

Features - CommCell Management

TABLE OF CONTENTS

OVERVIEW

SYSTEM REQUIREMENTS - COMMSERVE

PRE-INSTALLATION

- Network Requirements
- Firewall

INSTALLATION

- Install the CommServe
- Install the CommServe and Database Engine on Separate Computers
- Install/Upgrade the CommServe With an Existing Database
- Manually Installing the Software on a Passive Node
- Install the CommServe SNMP Enabler
- Silent Install - CommServe

ADMINISTRATION

- Scheduling
- Schedule Policy
- Custom Calendar
- Storage Policies
- Storage Policy Copies
- Alternate Data Paths (GridStor[®])
- Data Multiplexing
- User Administration and Security
- License Administration
- Data Encryption
- Disaster Recovery Backup
- Updates and Service Packs

JOB MANAGEMENT

- Operation Window
- Activity Control
- Job Management
- Job Priorities and Priority Precedence
- Job History
 - Admin Job History
 - Backup Job History
 - Client Job History
 - Recovery/Retrieve Job History
 - Restore Job History
 - Recovery Point Creation History
 - Recovery Point Copyback History
 - QR Volume Creation History
 - QR Volume Recovery History

STORAGE MANAGEMENT

- Auxiliary Copy
- Data Aging
- Data verification

- Media Refresh

CONFIGURATION

- Client Computer Groups
- Data Interface Pairs
- Firewall
- Robust Network Layer
- Datapipe Configuration
- Fault Tolerance

MONITORING

- Alerts
- SNMP Enablers
- Event Viewer
- Reports
- Services
- Audit Trail
- Log Files

OPERATIONS

- Name Management
- CommCell Migration
- Global Repository Cell (GRC)
- Space Check
- Separate the CommServe from a CommServe-MediaAgent Computer
- Web Administration

COMMAND LINE INTERFACE

BEST PRACTICES

- When WAN Links Cannot Support the Transfer of Data for Full Backups
 - Grandfather-Father-Son (GFS) Tape Rotation
-

Overview - CommServe® Storage Manager

Introduction

Controlling Activity from the CommCell® Console

- Job Manager
- Scheduler
- Event Manager and Alert Subsystem
- Reports and Job History
- User Security
- Disaster Recovery
- CommCell® Console

CommServe® Properties

- General
- Version
- Security
- Activity Control

CommServe® Operations

- Disaster Recovery Backup
- Restore DR Data to Disk
- Data Aging
- Auxiliary Copy
- Download Automatic Updates
- Install Updates
- Send Log Files
- Event Search
- View Schedules
- View Admin Job History
- View Log Files
- View Users Logged In

Control Panel

INTRODUCTION

The CommServe® StorageManager is the command and control center of the CommCell® architecture. It is responsible for managing the administrative functions. It handles all activity between agents, and communicates with MediaAgents when the media subsystem requires management. The CommServe manager contains the database that stores all of the information pertinent to the CommCell component.

The CommServe® server ties the elements of the CommCell configuration together; it is the coordinator and administrator of the CommCell component. The CommServe server communicates with all agents in the CommCell component to initiate data protection, management and recovery operations. Similarly, it communicates with MediaAgents when the media subsystem requires management. The CommServe server maintains a database containing all the information relating to the CommCell component. In addition, it provides several tools to administer and manage the CommCell component.

The software supports CommServe components on several Operating Systems, including support for CommServe server in a clustered environment. (See System Requirements - CommServe for a list of supported CommServe components and their requirements. See Support Information - Installation for information on cluster support for CommServes components).

See CommServe Deployment for information on installing the CommServe software. Once installed, the CommServe server is displayed in the CommCell Browser as the top node in the CommCell Browser. You can have only one CommServe server in a CommCell component. You can perform several operations from the CommServe component level and modify the properties associated with a CommServe server. These are described in CommServe Operations.

CONTROLLING ACTIVITY FROM THE COMMCELL® CONSOLE

The CommServe controls activity in the CommCell group through the following elements:

JOB MANAGER

The Job Manager manages and monitors immediate or scheduled operations throughout the CommCell group. The Job Manager communicates with agents in order to initiate and monitor data protection and data recovery operations. The Job Manager communicates with MediaAgents to monitor the resources necessary to complete these operations. The Job Manager starts, suspends, and resumes operations based on these resources.

All of this activity is displayed in the Job Controller of the CommCell Console. An authorized CommCell user can also perform actions on active operations from the Job Controller.

SCHEDULER

The scheduler allows users to schedule tasks so that these tasks can be initiated by the software.

EVENT MANAGER AND ALERT SUBSYSTEM

The CommServe® server controls the Event Manager and Alert subsystems. The Event Manager monitors the events occurring throughout the CommCell, and reports them through the Event Viewer in the CommCell® Console. This information can also be viewed through log files. Events can also be reported to CommCell users through the use of configured alert notifications, through the alert subsystem.

REPORTS AND JOB HISTORY

Users can obtain filtered data through the use of reports generated from the CommCell® Console. Users can also obtain information on non-active operations by viewing job history information.

USER SECURITY

The CommServe® server controls all user security within the CommCell® component. The CommServe software grants CommCell users permission to perform CommCell actions based on the assigned capabilities and CommCell object association of a CommCell user's member user group.

DISASTER RECOVERY

The CommServe® software is responsible for storing a metadata SQL database which contains all the information for the CommCell component. The software provides the facility to retrieve this data in the event of a disaster or system failure.

COMMCELL® CONSOLE

The CommCell® Console is the graphical user interface through which CommCell users can manage and administer the CommCell component.

COMMSERVE® PROPERTIES

GENERAL

From the CommCell® Browser, you can view information and modify the status of the CommServe® server.

CommServe® server properties can be viewed from the **General** tab of the CommServe **Properties** dialog box.

COMMCELL NAME

The CommCell name is the name that was given to this CommServe® server at the time of installation.

COMMCELL HOST NAME

The name of the computer on which the CommServe® software is installed.

VERSION

The **Version** tab of the CommServe **Properties** dialog box displays the version number of the CommServe® software that is installed on the CommServe computer. It also displays all post-release Service Packs and Updates that may have been installed on the CommServe computer.

For a detailed explanation of the version information, see **Version**.

SECURITY

The **Security** tab allows you to associate one or more user groups to the CommServe Server. Once associated, members of the associated user group(s) can perform all functions within a CommCell group.

For a detailed explanation of security, see **User Administration and Security**.

ACTIVITY CONTROL

The **Activity Control** tab allows you enable or disable administrative, data protection, data recovery, and scheduler activity for the entire CommCell® element.

For a detailed explanation of activity control, see [Activity Control](#).

COMMSERVE® OPERATIONS

DISASTER RECOVERY BACKUP

Disaster Recovery backups perform regular backups of the CommServe® database. It is critical to be able to retrieve this information in the case of a disaster or system failure. For comprehensive information on Disaster Recovery backups, see [Disaster Recovery Backup](#).

RESTORE DR DATA TO DISK

The **Restore by Jobs** feature can be used to restore Disaster Recovery backup data. For an overview, see [Restore by Jobs](#).

DATA AGING

You can run a **Data Aging** operation to remove the data that has exceeded its user-defined retention rule. For more information on **Data Aging**, see [Data Aging](#).

AUXILIARY COPY

An auxiliary copy operation allows you to create secondary copies of data associated with data protection operations, independent of the original copy. For more information on **Auxiliary Copy**, see [Auxiliary Copy](#),

DOWNLOAD AUTOMATIC UPDATES

This option allows you to download updates from the FTP site for downloading updates. For comprehensive information on updates, see [Automatic Updates](#).

INSTALL UPDATES

This options allows you to install updates from the CommServe® Cache. See [Install Updates to Specific Clients/MediaAgents](#) for step-by-step instructions to install updates. See [Automatic Updates](#) for comprehensive information on updates.

SEND LOG FILES

You can view and send the log files of the operations that have occurred on your system from a CommServe® computer. For more information on log files, see [Log Files](#).

EVENT SEARCH

You can perform a search for specific events that have occurred within your CommCell® configuration. For more information about events, see [Event Viewer](#).

VIEW SCHEDULES

From the CommCell® Browser, you can view and modify all the jobs that are scheduled to run on a CommServe® server using the **Scheduled Jobs** window. The **Scheduled Jobs** window allows you to review the jobs that are scheduled and the identity of the client computers for which they are run. For an overview, see [Scheduling](#).

VIEW ADMIN JOB HISTORY

You can view the job history of all of the administration jobs that have run. For an overview, see [Admin Job History](#).

VIEW LOG FILES

You can view the log files generated by a MediaAgent. The files that reside on a given computer may differ depending on the role of the computer in the CommCell® architecture (CommServe® Server, MediaAgent, Client). A CommServe computer contains only the CommServe log files. A computer that is both a CommServe Server and a MediaAgent contains the log files of both entities. For a detailed explanation of log files, see [Log Files](#).

VIEW USERS LOGGED IN

You can view the users currently logged on to the CommCell® Console. See [Users Logged In](#) for an overview.

CONTROL PANEL

The Control Panel allows you to launch a wide variety of administrative tasks. See Control Panel for more information.

[Back to Top](#)

System Requirements - CommServe

Enterprise Version | Express Version

The following requirements are for the Enterprise version of the CommServe:

OPERATING SYSTEM		PROCESSOR
WINDOWS	WINDOWS 2012	
	Microsoft Windows Server 2012 Editions See Considerations for Microsoft Windows Server 2012, 2012 R2, and Windows 8 for more information.	Dual 1 GHz minimum required
	WINDOWS 2008	
	Microsoft Windows Server 2008 R2 Editions	Dual 1 GHz minimum required
	Microsoft Windows Server 2008 32-bit and x64 Editions* *Core and Web Server Editions not supported	Dual 1 GHz minimum required
	WINDOWS 2003	
	Microsoft Windows Server 2003 32-bit and x64 Editions* with a minimum of Service Pack 2 *Web Server Editions not supported	Dual 1 GHz minimum required

CLUSTER - SUPPORT

The software can be installed on a Cluster if clustering is supported by the above-mentioned operating systems.

For information on supported cluster types, see Clustering - Support.

HARD DRIVE

2.1 GB of local disk space for the CommServe software, including database and log file growth, and the Microsoft SQL Server application and database. (The SQL software is embedded in the CommServe software installation.)

500 MB of temp space on the drive on which the Operating System and `temp` directory resides. (This space is used for temporary files copied during the installation or upgrade of the Microsoft SQL Server and CommServe software.)

1.5 GB of permanently available disk space on a local or mapped network drive for CommServe Disaster Recovery. (CommServe Disaster Recovery is a feature that secures the metadata of the CommServe.)

In time, you may need to provide additional space (several GB) to allow for growth in the CommServe metadata. The size of the metadata depends on the number of computers in the CommCell and the quantity of data stored.

MEMORY

16 GB RAM minimum required

To achieve higher scalability, it is recommended to deploy the CommServe on a physical server with 32 GB memory and Solid-state-disk (SSD). Refer to CommCell Scalability Guide for additional details.

DATABASE ENGINE

Calypso includes a license for Microsoft SQL Server 2008 (Enterprise Edition). Microsoft SQL Server 2008 database instance with Service Pack 1 will be automatically installed while installing the CommServe. Later SQL Server service packs and updates must be installed manually. We recommend to maintain the SQL Server up-to-date with any important updates released by Microsoft.

Microsoft SQL Server 2008 R2 Editions and SQL Server 2012 (SP1) are also supported. If using SQL Server 2012, it is required that you install the Cumulative Update Package 3 and review the recommendations listed in Considerations for SQL Server 2012.

The Microsoft SQL Server application that is installed on the computer must be dedicated to support the software and cannot be shared by other applications.

In a clustered environment, Microsoft SQL Server 2008 (Enterprise Edition) with the appropriate service pack must be installed and clustered prior to installing the CommServe software. The CommServe software automatically uses the default or the named instance created during the SQL installation.

RECOMMENDED SQL SERVER SETTINGS

The database instance used by the software requires specific SQL server settings. Using the SQL Management Studio, verify the SQL properties listed below.

SQL MEMORY SIZE

Access the server properties and navigate to the **Memory** page. The maximum server memory should be 50% of the physical memory available in the computer on which the software is installed.

SERVER COLLATION

Run the `sp_helpsort` system stored procedure, and verify that the server default collation has the following properties:

- Character Set is `1252/ISO` (default)
- Sort Order is `Dictionary order, and case is Insensitive`
- Unicode Collation includes `General Unicode, case Insensitive, width Insensitive`

TEMP DATABASE PROPERTIES

Navigate to the `tempdb` database (under the **Databases | System Databases** node), and access its properties to verify the following:

- The `tempdb` database has at least 100 MB of disk space. Depending on the components that you decide to install later, additional space may be needed.
- Click the **Files** page to check the autogrowth properties of the database files. The **Enable Autogrowth** option must be selected, and the file growth should be set to 20%

SERVICE ACCOUNTS

For Service Accounts, use the same Local System account for each service and enable auto-start for SQL services.

On clustered environments, use an account with administrator privileges (such as, a member of the Administrator local group of the computer or domain).

HARDWARE VALIDATION FOR COMMSERVE DATABASE

The CommServe database needs to be on a fast disk for optimal backup performance. Before setting up the CommServe, the storage volumes must be validated for high performance. This can be done using IO meter tool which measures the IOPs (Input Output Operations per second). For more information, see IOPs for CommServe Database Volumes.

PERIPHERALS

DVD-ROM drive

Network Interface Card

MISCELLANEOUS

INTERNET EXPLORER

Microsoft Internet Explorer (IE) version 8.0, 9.0

JAVA SUPPORT

The software supports Java 7 or higher*.

Java 7 versions are supported with Calypso Service Pack 8 or higher. Previous service pack versions do not fully support this version.

If a JRE version 1.7.0_17 or higher is available, the software will use the existing JRE software.

If a JRE version lower than 1.7.0_17 is available, or no JRE version is available at all, you will be prompted to install JRE version 1.7.0_17

*The Backup Time selection in the Advanced Options area of the Find dialog box is not compatible with Java 7 or higher.

COMMSERVE DATABASE ON CIFS

The CommServe's SQL database is not supported on a CIFS share.

RECOMMENDATION FOR USING VIRTUAL MACHINES

MEMORY

- Allocate multiple virtual CPUs to a virtual machine, if the anticipated SQL Server workload can take advantage of all the virtual CPUs.
- Memory page sharing and memory ballooning must be enabled on the virtual machine.

STORAGE

SQL Data files and log files must reside on different disks (different VMFS). It is recommended to place the log files on RAID 1+0 or RAID 1 disks.

NETWORK

Make sure to use the VMXNET virtual network adapter and separate virtual switches, each connected to its own physical network adapter.

NOTES ON COMMSERVE INSTALLATION

The CommServe is a resource intensive application and should be installed on a dedicated server. Therefore, it is recommended that the CommServe not be installed on a computer running other applications, such as Microsoft Exchange Server, an Oracle database, etc. Additionally, CommServe installed on virtual machines generally perform at about 60% capacity compared to physical machines with similar configurations.

The software should not be installed on a compressed drive.

The Enterprise version of the CommServe is not supported on Microsoft Windows Small Business Server platforms. If you wish to install the CommServe on Microsoft Windows Small Business Server platform, you must install the Express version of the CommServe. See the System Requirements for the Express version of the CommServe for more information.

The computer on which the software is installed must have a static IP address. The software does not support Dynamic Host Configuration Protocol (DHCP).

INSTALLING ON A VMWARE ENVIRONMENT

If installing the CommServe on a VMware virtual machine, consider the following recommendations for optimal performance:

- The ESX Server hosting the virtual machine should be vSphere (4.0) or above.
- Disable vMotion for the virtual machine and the storage.
- The virtual machine on which the CommServe will be installed should have:
 - Minimum 2 64-bit vCPUs
 - Minimum 16 GB RAM
 - A Windows Server 2008 x64 Edition operating system
 - All VMware tools and utilities installed
- Minimum bandwidth of 1 Gbps for data transfer.
- The CommServe's SQL database should be configured on shared storage (such as a SAN or FAST disk).

INSTALLING ON A HYPER-V ENVIRONMENT

If installing the CommServe on a Hyper-V virtual machine, consider the following recommendations for optimal performance:

- Hyper-V Server 2008 R2 with Service Pack 1 (or higher) should be used to host the virtual machine.
- The virtual machine on which the CommServe will be installed should have:
 - Minimum 4 64-bit vCPUs
 - Minimum 16 GB RAM
 - A Windows Server 2008 x64 Edition operating system
 - All Hyper-V Integration tools installed using the latest versions
- A fast and dedicated storage as well as network interfaces for optimal performance of the CommServe SQL database.

NOTES ON COMBINED INSTALLATIONS

You will often install more than one module (For example, CommServe, MediaAgent, Client) on a single computer so that it can perform two or more functions. For example, you may want to back up the file system of a MediaAgent; hence, you would install both the MediaAgent and client software on that computer.

When you combine two or more functions on a single computer, the storage resources required to support the software for that computer are not essentially cumulative. This is because modules share some of the same software. As a result, combined installations require about 30 MB less disk space than installations where the software resides on separate computers.

DISCLAIMER

Minor revisions and/or service packs that are released by application and operating system vendors are supported by our software but may not be individually listed in our System Requirements. We will provide information on any known caveat for the revisions and/or service packs. In some cases, these revisions and/or service packs affect the working of our software. Changes to the behavior of our software resulting from an application or operating system revision/service pack may be beyond our control. The older releases of our software may not support the platforms supported in the current release. However, we will make every effort to correct the behavior in the current or future releases when necessary. Please contact your Software Provider for any problem with a specific application or operating system.

Additional considerations regarding minimum requirements and End of Life policies from application and operating system vendors are also applicable

Network Requirements

TABLE OF CONTENTS

Overview

Domain Name Server (DNS) environment

Multi-Homed CommCell® Computers

WINS or other Non-DNS Environment

Reverse Lookup

Enabling Reverse Lookup

Internet Protocols

Important Considerations

OVERVIEW

All CommCell® computers (i.e., CommServe, MediaAgent, and Client computers) must be connected via a network configured with TCP/IP protocol. To ensure each computer can resolve the names of other CommCell computer members and therefore communicate, we offer the following guidelines.

DOMAIN NAME SERVER (DNS) ENVIRONMENT

A DNS environment provides a centralized means of resolving computer names with their corresponding IP addresses. Refer to your operating system documentation for information on how to establish and manage DNS.

MULTI-HOMED COMMCELL® COMPUTERS

A multi-homed computer is one that has two or more network interface cards (NICs). To ensure proper name/IP address resolution within the CommCell computer, it is necessary to uniquely name each NIC in the DNS. For example, assume there is a computer whose computer name is `amber` and fully qualified host names are `amber1.company.com` and `amber2.company.com` respectively. This computer has two NICs with the following IP addresses:

- First NIC: 150.128.4.78
- Second NIC: 150.128.6.32

To ensure that both interfaces can be resolved, define unique names within DNS, such as:

- `amber1.company.com 150.128.4.78`
- `amber2.company.com 150.128 6.32`

If a computer name resolves to multiple IP addresses, the software will automatically use the first IP address resolved. However, if that first IP address becomes unreachable, the software will not be able to reach the computer using the other IP addresses in the list. In such scenarios, it is recommended that a hosts file be created with all the computer's reachable IP addresses included.

WINS OR OTHER NON-DNS ENVIRONMENT

If your network does not have DNS lookup or some other name resolution facility, the CommServe® manager will provide the names and IP addresses of all the members in the CommCell® group. The fully qualified computer name and IP address of the CommServe manager is stored in the hosts file of each CommCell member. The hosts file in the CommServe computer, in turn, stores the fully qualified computer name and IP addresses of all the members in the CommCell, thereby providing the lookup facility to all the members in the CommCell group. Depending on the operating system on your computer, the hosts file is located in one of the following directories:

- On a Windows computer, the `hosts` file is located in `%SystemRoot%\system32\drivers\etc` directory. (`%SystemRoot%` is the Windows installation directory on your system.)
- On a computer with a Unix operating system, the `hosts` file is located in the `/etc/inet` directory.

During installation of each CommCell member, the install program attempts to resolve the name of the CommServe manager to an IP address. If the resolution fails, the installation prompts you to enter the IP address of the CommServe computer.

Proper name/IP address resolution is essential to reliable network communications.

REVERSE LOOKUP

Prior to performing any installation, ensure that the hostname and the fully qualified domain name are reachable from the CommCell network, and the IP Addresses/Host Names are resolved correctly using the DNS System.

Computers in a network use the Domain Name System to determine the IP address associated with a host/domain name. This process is also known as forward DNS resolution. Reverse DNS lookup is the inverse process, the resolution of an IP address to its designated host/domain name. For a proper network

communication, the IP Address to Host Name resolution and Host Name to IP address resolutions are essential.

If reverse DNS lookup is not enabled on a client computer, it will not be able to communicate with the remote computer by using the host name.

Use the following steps to perform a reverse lookup on an IP address:

1. Logon to the client computer as an Administrator.
2. Click **Start**, and then click **Run**.
3. In the **Open** box, type **cmd**, and then click **OK**.
4. From the command prompt, run the following command:

```
nslookup <remote_computer_ip_address>
```

Example:

```
C:\administrator.idclab\nslookup 172.xxx.xxx.244
```

```
Server: ingpdc01.gp.cv.company.com
```

```
Address: 172.16.xxx.xxx
```

```
Name: faraday.gp.cv.company.com
```

```
Address: 172.xxx.xxx.244
```

In the above example, the first section specifies the server and the IP address of that server that provided you with the domain name, and the second section shows the host name associated with the IP address that you typed with **nslookup** command.

If the DNS service is not running on the setup, the above command returns one of the following error messages:

```
No Response from Server
```

```
Timed Out
```

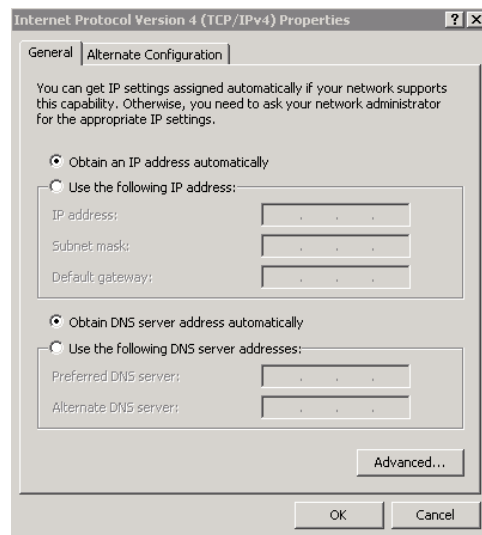
```
No Records
```

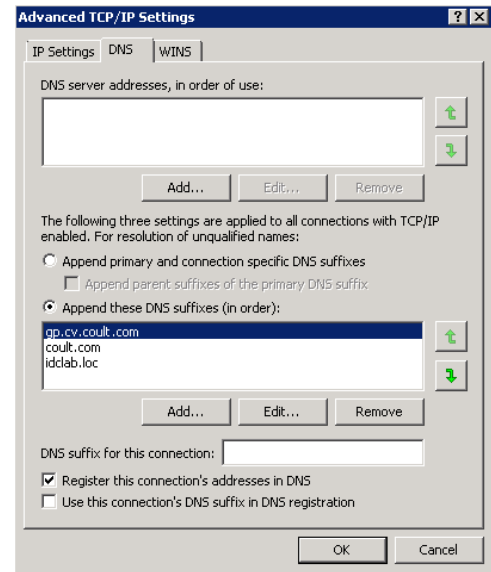
```
Server Failure
```

ENABLING REVERSE LOOKUP

Use the following steps to enable Reverse DNS lookup on a client computer:

1.
 - Logon to the computer as an Administrator.
 - Click **Start**, click **Control Panel** and then select **Network and Internet**.
 - Click **Network and Sharing Center**.
 - Under **Tasks**, Select **Manage network connections**.
 - Right-click the **Local Area Connection** icon, and then click **Properties**.
 - On the **Local Area Connection Properties** dialog box, select **Internet Protocol Version4 (TCP/IPv4)**, and then click **Properties**.
 - If you have a DHCP Server in your network environment, then select **Obtain DNS server address automatically**. Else, select **Use the following DNS server addresses** and follow the below steps:
 - In the **Preferred DNS server** box, type the IP Address of the DNS server.
 - In the **Alternate DNS server** box, type the IP Address of the alternate DNS server.
2.
 - Click **Advanced**.
 - On the **Advanced TCP/IP Settings** dialog box, click the **DNS** tab.
 - Click **Append these DNS suffixes (in order)**.
 - Click **Add**, in the **Domain suffix** box, type the Domain suffix, and then click **Add**. Repeat this step to add all the DNS suffixes in order.
 - Click **OK**, and then click **OK**.
 - Click **OK**.





In case the DNS is not configured or not supported, then the client computer will not be able to perform IP/Name resolution and will not be able to communicate with the remote computers by using the host names. You can overcome this temporarily by adding the IP addresses and the fully qualified domain names in the host file of the client computer. It is not recommended to add Hosts file entries as these create communications control points that may impact other server operations and are difficult to maintain and manage. These should be used only as temporary solutions until the larger network or DNS issues can be resolved. You can use the following steps to add entries to the host file of the client computer with Windows operating system:

1. Logon to the computer as an Administrator.
2. Click **Start**, and then click **Run**.
3. In the **Open** box, type **drivers**, and then click **OK**.
4. Double-click **etc** folder, open **hosts** file with Notepad, and then type the IP address, the fully qualified domain name and the host name of the remote computer. You can add additional entries on separate lines. Save the `hosts` file after adding the entries.

Example:

```
172.32.xxx.xxx dbwin1.idclab.loc dbwin1
172.14.xxx.xxx dbwin2.idclab.loc dbwin2
```

Similarly, to enable reverse lookup on a remote computer, repeat step 1 through step 3 for adding IP address of the client computer in the `hosts` file of the remote computer.

For more information, see: [http://technet.microsoft.com/en-us/library/cc780585\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc780585(WS.10).aspx)

For a Unix computer, the entries should be added in the `host` file located under `etc` folder.

INTERNET PROTOCOLS

CommCell® computers can operate on the following Internet Protocol (IP) versions:

- IPv4 on all Windows, Unix, and Novell client computers.
- IPv6 on the following Windows and Unix computers (See Support below for more information.)

IMPORTANT CONSIDERATIONS

The CommServe® computer requires IPv4 to obtain permanent licenses. However, the CommServe® computer can have both IPv4 and IPv6 enabled using multiple NIC cards. If the client computers in the CommCell® use the IPv6 protocol, the CommServe and MediaAgent must also use the IPv6 protocol.

CONFIGURATION

To enable CommCell® functionality for Windows computers on an IPv6 network, you must use the following registry keys:

- `nOverridePreferredIPFamily` - This key provides the capability to install CommCell components on computers in an IPv6 environment. This key must be manually created on each computer in the CommCell group prior to installing any software components.

Note that this key only provides IPv6 support for the duration of the software installation.

- `nPreferredIPFamily` - This key is provided with the software and allows you to operate CommCell components in an IPv6 environment beyond the software installation process. This key must be configured on each computer in the CommCell group after the software has been installed.

To enable CommCell functionality for Unix computers on an IPv6 network, you must perform the following:

- Add the following to the `cvpkgadd` command:

```
-display-interface-family [nPreferredIPFamily]
```

For example, if you wish to apply both IPv4 and IPv6 support, you would add the following to the `cvpkgadd` command:

```
-display-interface-family 0
```

Note that this key only provides IPv6 support for the duration of the software installation.

- `nPreferredIPFamily` - This key is provided with the software and allows you to operate CommCell components in an IPv6 environment beyond the software installation process. This key must be configured on each computer in the CommCell group after the software has been installed.

COMMCELL CONSOLE CONSIDERATIONS

- If a CommServe server has both IPv4 and IPv6 protocols enabled, the CommCell® Console will always obtain an IPv4 address. If you wish to obtain and connect with an IPv6 address, the following parameter must be added to the `java/javaw` command:

```
-Djava.net.preferIPv6Addresses=true
```

For example:

```
"C:\Program Files\Java\jre1.6.0\bin\javaw.exe" -jar cv.jar cranberry 8401 -oemid=1 -Djava.net.preferIPv6Addresses=true
```

Note that this configuration is supported for the CommCell Console as a stand-alone application only. If you are running the CommCell Console as a remote web-based application, you will always obtain an IPv4 address.

- To run the CommCell Console as a Remote Web-Based Application in an IPv6 environment, the web alias must include either the IPv6 address or a host name that resolves to the IPv6 address.

MACINTOSH FILE SYSTEM CONSIDERATIONS

- By default, the software installation program will not display IP addresses that are not reverse-resolvable to the a host name in the interface list. To display such IP addresses, create the following empty file:

```
/tmp/cvpkgadd_unlock_ipaddress
```

OUTLOOK ADD-IN CONSIDERATIONS

- To perform stub recalls using the Outlook Add-In in an IPv6 environment, the `ipfamilypref` registry key must be configured to accept the IPv6 protocol. This key must be configured on each computer on which Outlook Add-In is installed.

FILE ARCHIVER CONSIDERATIONS

- It has been seen that a Windows computer may crash with a blue screen when accessing a file under the following conditions:
 - the file resides on a Celerra file server
 - the file has offline attributes set
 - the services handling offline file restores is disabled or shut down
 - the client Windows computer has IPv6 installed and enabled

Therefore, it is recommended that the services handling stub file restores are running before accessing offline stub files on a Celerra file server from a Windows computer with IPv6 enabled.

- FPolicy with NetApp ONTAP is not supported with IPv6 on Microsoft Windows Server 2008 platforms.
- If the File Archiver Agent is installed on a computer using the IPv4 protocol and the client computer is using the IPv6 protocol, it is recommended that the `nPreferredIPFamily` registry key be created on the client computer with the value set to 1. This will ensure connections between the two computers are not disrupted during stub recalls.

SUPPORT

IPv6 is not supported for the following:

- 1-Touch client recoveries
- Command Line Interface
- Content Indexing and Search
- Data Classification on Unix platforms
- NDMP Remote Server (when backup up a file server that does not support NDMP IPv6)
- NetWare MediaAgent
- NetWare File System *iDataAgent*
- Novell Directory Services (NDS) *iDataAgent*
- Novell GroupWise *iDataAgent*

- Unix computers running HP-UX 11.00

Additionally, consider the following:

- IPv6 support for AIX 5.3 and above may require use the of `/etc/hosts` for IPv6 name resolution.
- IPv6 support for Tru64 OSF1 Release 5.1A requires the use of `/etc/ipnodes` for IPv6 name resolution.
- IPv6 support for HP-UX 11.11 requires the installation of the Transport Optional Upgrade Release (TOUR) 2.5 and OS patch PHCO29328.
- For Linux computers, only varieties with a glibc of 2.3 or 2.4 are supported with IPv6.
- For Solaris computers, only Solaris 9 and above are supported with IPv6.
- For Windows computers, only Microsoft Windows Server 2003 varieties and above are supported with IPv6.
- The **Optimize for Concurrent LAN Backups** option is not supported for AIX MediaAgents using the IPv6 protocol.

[Back to Top](#)

Firewall

Setup	Advanced	Troubleshooting	Best Practices
-------	----------	-----------------	----------------

Overview

Operating Using Direct Connections

- Client Connects to the CommServe (One-Way Firewall)
- CommServe Connects to the Client (One-Way Firewall)
- Client and CommServe Connect to Each Other (Two-Way Firewall)

Operating Through a Port-Forwarding Gateway

- Configure the Port-Forwarding Gateway
- Setup connection to the CommServe
- Install the Client
- Configure the CommServe, MediaAgent and Client
- Security Considerations

Operating Through a DMZ Using Calypso Proxy

- Set up the Calypso Proxy
- Install the Client
- Configure the CommServe, MediaAgent and Client

Operating Using Public WiFi Connections

- Install the Client
- Configure the Client to Operate across HTTP Proxy

Configuring Windows Firewall to Allow CommCell Communication

OVERVIEW

When CommCell components are separated by a firewall, the components must be configured with the connection route to reach each other across the firewall. Once configured, the components seamlessly communicate across the firewall for all data management operations such as backup, browse, restore, etc.

CommCell components can be configured to operate across the following:

- Port-forwarding gateways
- HTTP proxies
- DMZ
- NAT configurations
- Combinations of the above firewall scenarios.

In addition, you can also create your own Calypso proxy by designating a CommCell component as the proxy and defining the connections rules on the component. Components can communicate using HTTP or HTTPS protocol.

The following sections explain in detail the configuration required to install and operate CommCell components across different types of firewalls.

KEY FEATURES

The software offers the following key features in communication across firewall:

- Centralized configuration from the CommCell Console. Firewall settings can be configured at the individual client or client group levels.
- Lesser port requirements. Having port number 8400 is no longer a requirement to operate across firewalls. Backup and restore operations can be performed through a single open port. However, it is recommended that you open additional ports to enable faster data traffic.
- Support for port-forwarding routers. Multiple CommCell components on the internal network can be exposed to the outside world via a single gateway IP address with necessary port forwarding configured on the gateway. Roaming clients can reach specific internal machines by opening tunnel or data connections to specific ports on the port-forwarding gateway.
- Support for Calypso proxy configurations. For maximum security, the software now supports a special proxy configuration where you can place a Calypso agent in a DMZ, and configure the firewall to allow connections from inside and outside networks into the DMZ only.
- HTTPS encryption in the tunnels. The software now uses HTTPS encapsulation in all tunnel connections. This provides SSL/TLS encryption protecting all data in transit and allows for better compatibility with traffic filtering firewalls.
- Tunnel authentication using CommCell-specific certificate. Due to the use of HTTPS, all tunnel connections are not only encrypted, but also authenticated. For high levels of security, CommCells can be locked down to use CommCell-specific certificates for SSL/TSL authentication which is unique for every CommCell deployment.

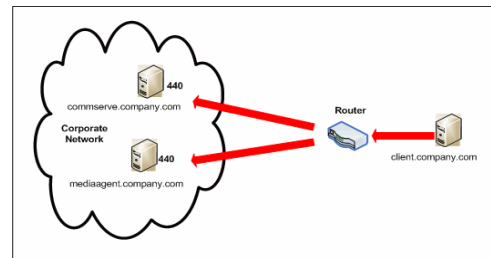
OPERATING USING DIRECT CONNECTIONS

Direct connection with port restrictions is a setup where at least one of any two communicating computers can establish a one-to-one connection towards the other on specific ports. The connection could also be routed if the routing does not include a proxy or an intermediate port-forwarding gateway. This configuration was supported as One-Way Firewall and Two-Way Firewall in previous releases.

CLIENT CONNECTS TO THE COMMSERVE (ONE-WAY FIREWALL)

Consider the diagram that illustrates a direct connection setup where the client opens tunnel connection towards the CommServe and the MediaAgent.

The following sections explain the configuration required on the CommServe, MediaAgent, and the client to operate in this scenario.



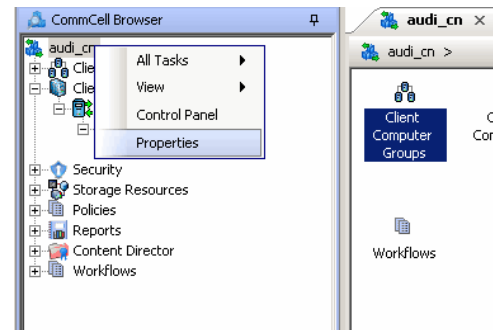
Review the following considerations before you begin.

- Make a note of the port configurations on your firewall and substitute them appropriately in the following instructions.
- Microsoft Internet Information Services (IIS) uses port number 443 by default. So if you have IIS running on a computer, then you will not be able to use port 443 for firewall configuration on that computer.

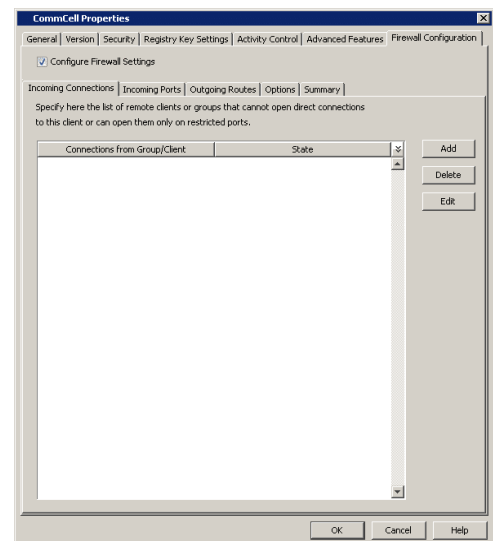
SETUP CONNECTION TO THE COMMSERVE

Before installing the client, you will have to provide an incoming port number on which the CommServe will receive tunnel connections from the client. The following steps explain the configurations required for this purpose.

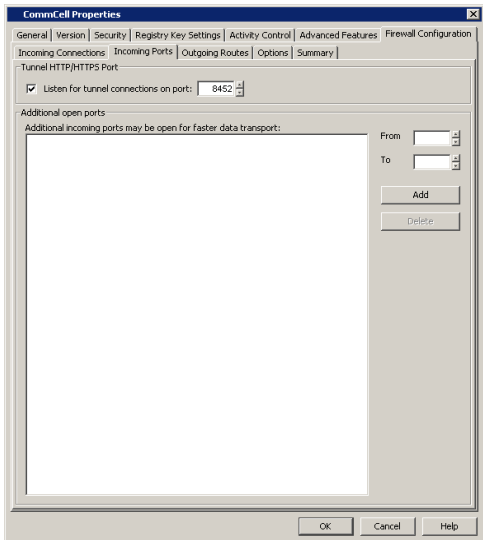
1. From the CommCell Console, right-click the CommServe computer and click **Properties**.



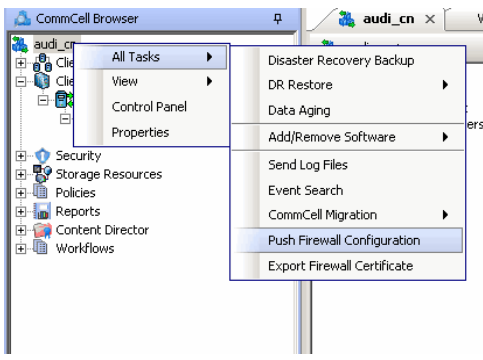
2. Click the **Firewall Configuration** tab.



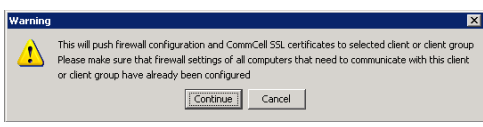
3.
 - Click the **Incoming Ports** tab.
 - Select **Listen for tunnel connections on port** and specify the port number on which the incoming tunnel connection is received.
 - Click **OK**.



- From the CommCell Console, right-click the CommServe computer and click **All Tasks | Push Firewall Configuration**.



- Click **Continue**.
The specified configuration is saved.
Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.



INSTALL THE CLIENT

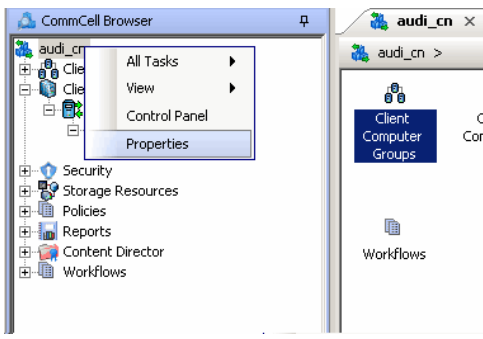
In this configuration the client establishes connection with the CommServe using one or more ports. To install the client across a firewall in this setup, you will have to specify the path to reach the CommServe computer. During installation of the client, use one of the following firewall configuration sequence.

- Client/MediaAgent can reach the CommServe (Windows clients)
- Client/MediaAgent can reach the CommServe (Unix clients)

CONFIGURE THE COMMSERVE, MEDIAAGENT AND CLIENT

Use the following steps to establish incoming and outgoing connectivity details between the CommServe, MediaAgent, and the client computer.

- To configure the CommServe, right-click the CommServe computer from the CommCell Console and click **Properties**.



- Click the **Firewall Configuration** tab.
- From the **Incoming Connections** tab, click **Add**.

4.
 - In the **From** field, select the name of the client you just installed.
 - In the **State** field, specify the status of the connection from the client. Since in this case the client can reach the CommServe, assuming that the firewall is restricting connections to a specific port, select **Restricted**.

Note that if the firewall allowed any connection from the client to the CommServe, then this entry is not required.

- Click **OK**.

5.
 - Click the **Incoming Ports** tab. You will see the tunnel port already specified on the CommServe.
 - **Additional Open Ports:** For components that handle data transfer (for example, MediaAgent, File System iDataAgent, etc.), you can speed up the data transfer by opening additional ports on the firewall and recording them as open in this screen. Specify the range of ports in the **Additional open ports** area, **From** and **To** fields. Click **Add** to add the ports. To remove a port from the listing, select the port and click **Delete**. The ports must be within the range of 1024 - 65000. Ensure that the ports specified here are not used by other applications.

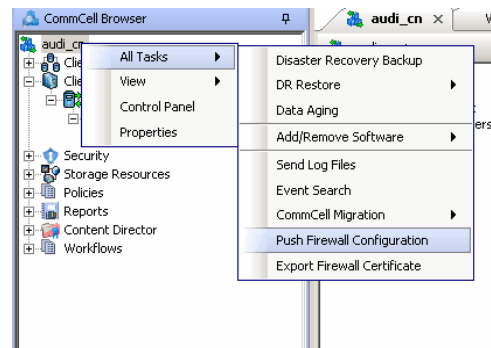
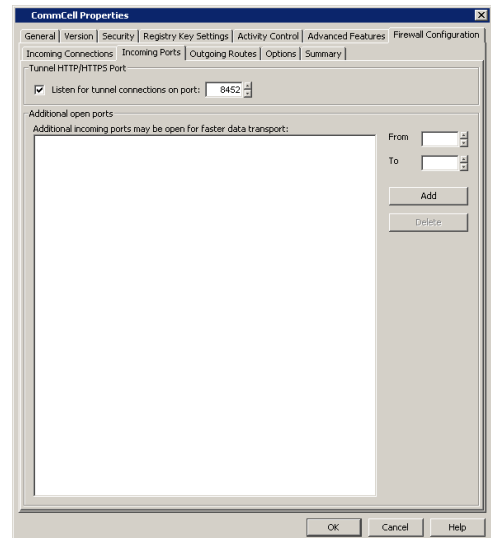
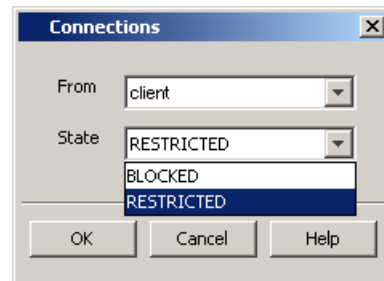
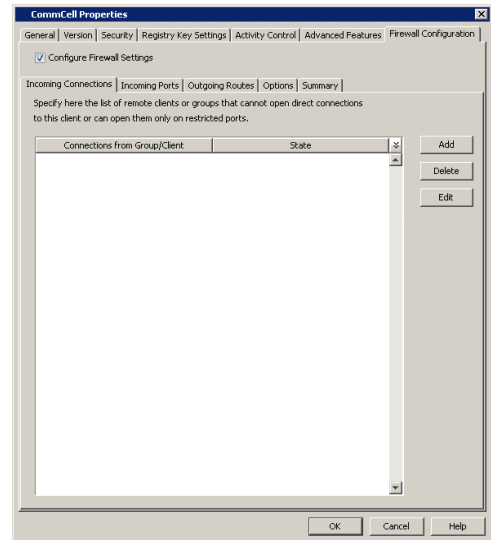
Review the following recommendations.

- For MediaAgents involving multi-stream restores, opening additional ports increases the restore performance. The number of open ports should correspond to the number of simultaneously running restore streams.
- For MediaAgents with **Optimize for concurrent LAN backups** option enabled, opening the incoming port of the Bull Calypso Communications Service improves the backup performance.
- For MediaAgents performing SnapProtect operations with Data Replicator snap engine, opening additional ports increases the backup performance.
- For ContinuousDataReplicator and Workstation Backup destination computers, opening additional incoming ports improves the replication performance.

- Click **OK**.

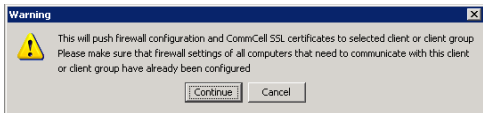
6. From the CommCell Console, right-click the CommServe computer and click **All Tasks | Push Firewall Configuration**. This updates the firewall configuration on the CommServe and client computer.

7. Click **Continue**.

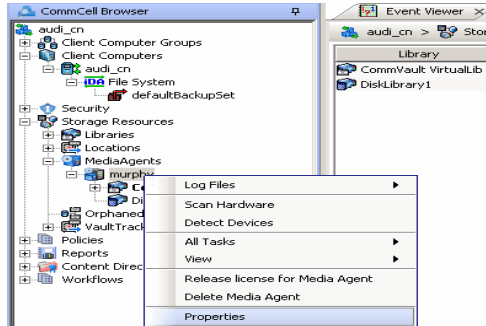


The CommServe is configured to receive communication from the client.

Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.

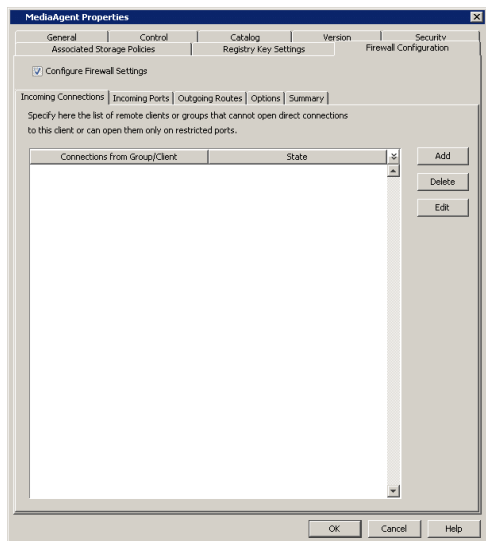


- 8. To configure the MediaAgent, right-click the MediaAgent computer from the CommCell Console and click **Properties**.



- 9. Click the **Firewall Configuration** tab.

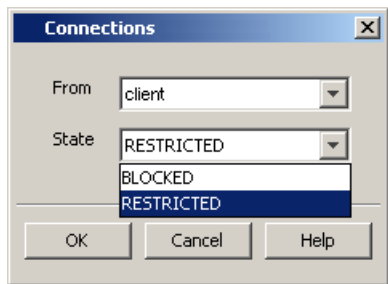
- 10. From the **Incoming Connections** tab, click **Add**.



- 11.
 - In the **From** field, select the name of the client you just installed.
 - In the **State** field, specify the status of the connection from the client. Since in this case the client can reach the MediaAgent, assuming that the firewall is restricting connections to a specific port, select **Restricted**.

Note that if the firewall allowed any connection from the client to the MediaAgent, then this entry is not required.

- Click **OK**.



- 12.
 - Click the **Incoming Ports** tab.
 - Select the **Listen for tunnel connections on port** option and specify the tunnel port through which connections from the client are received on the MediaAgent computer.
 - **Additional Open Ports:** For components that handle data transfer (for example, MediaAgent, File System iDataAgent, etc.), you can speed up the data transfer by opening additional ports on the firewall and recording them as open in this screen. Specify the range of ports in the **Additional open ports** area, **From** and **To** fields. Click **Add** to add the ports. To remove a port from the listing, select the port and click **Delete**. The ports must be within the range of 1024 - 65000. Ensure that the ports specified here are not used by other applications.

Review the following recommendations.

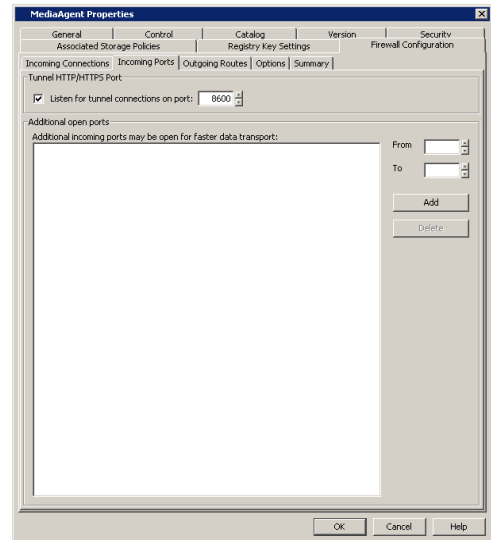
- For MediaAgents involving multi-stream restores, opening additional ports increases the restore performance. The number of open ports should correspond to the number of simultaneously running restore streams.
- For MediaAgents with **Optimize for concurrent LAN backups** option enabled, opening the incoming port of the Bull Calypso Communications Service

improves the backup performance.

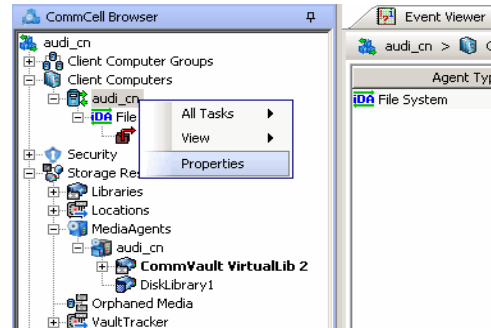
- For MediaAgents performing SnapProtect operations with Data Replicator snap engine, opening additional ports increases the backup performance.
- For ContinuousDataReplicator and Workstation Backup destination computers, opening additional incoming ports improves the replication performance.

- Click **OK**.

The MediaAgent is now configured to receive communication from the client.

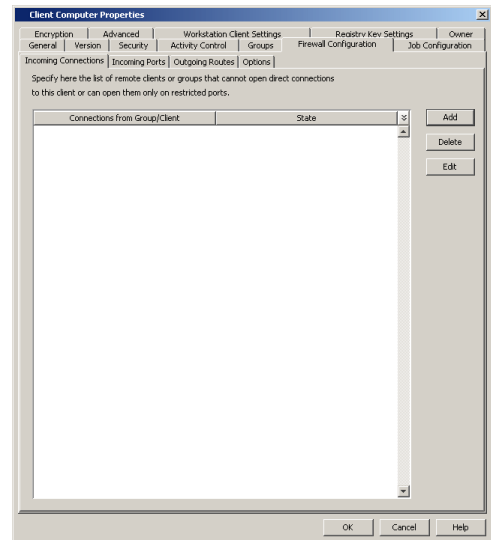


13. To configure the Client, right-click the client computer from the CommCell Console and click **Properties**.

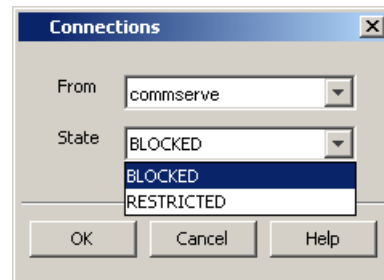


14. Click the **Firewall Configuration** tab.

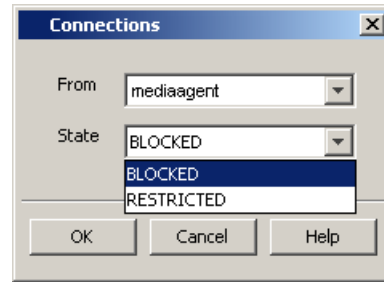
15. From the **Incoming Connections** tab, click **Add**.



16.
 - In the **From** field, specify the name of the CommServe computer.
 - In the **State** field, select **Blocked**, since the CommServe cannot open connections to the Client.
 - Click **OK**.



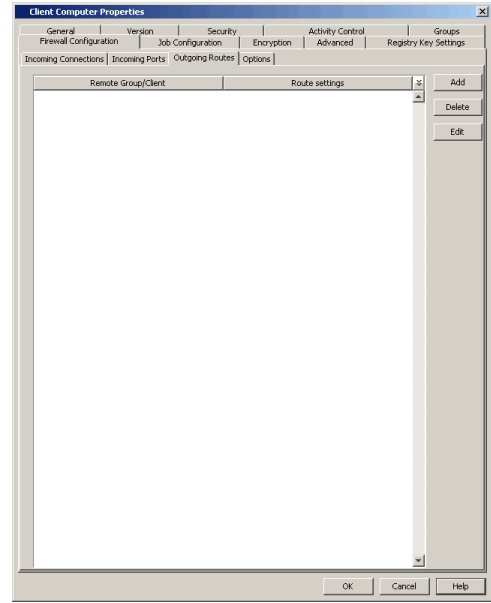
17.
 - Click **Add** again to specify the MediaAgent connection details.
 - In the **From** field, specify the name of the MediaAgent computer.
 - In the **State** field, select **Blocked**, since the MediaAgent cannot open connections to the Client.
 - Click **OK**.



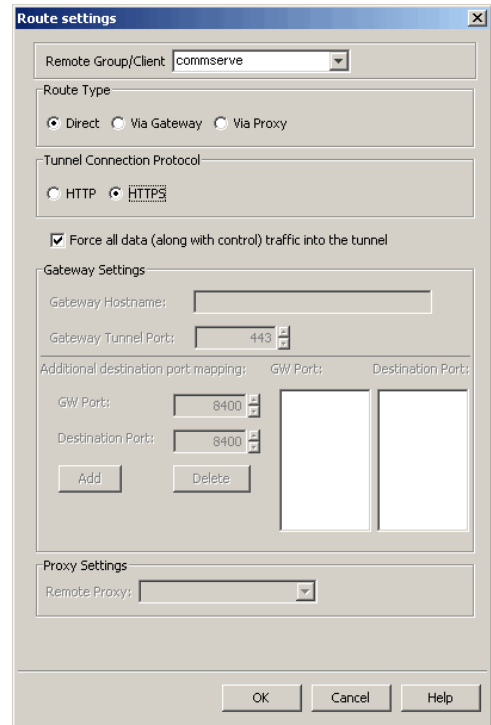
18.
 - Click the **Outgoing Routes** tab.
 - Click **Add**.

Outgoing routes are automatically created in the direct connectivity setup — manual entry is not required. However, you might want to create an entry if you wish to achieve one of the following.

 - Enable HTTPS encryption for the tunnel or data traffic.
 - Encrypt the data connections by forcing the connections into the tunnel. However, consider the following before using this option.
 - Direct connections always work faster. Forcing data connections into the tunnel might degrade performance of data protection operations.
 - If you wish to encrypt your backup data, you must rather configure encryption at the client level which offers more control and stores the data in encrypted form on the backup media as well.



19.
 - Select the CommServe name in **Remote Group/Client**.
 - Select **Direct**.
 - Select **HTTPS** protocol. This will enable authentication and encryption for tunnel connections.
 - **Force all data (along with control) traffic into the tunnel** option is not required as this route is not toward MediaAgent.
 - Click **OK**.



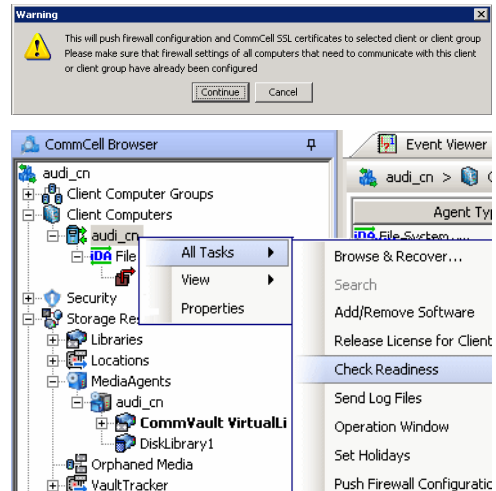
20. From the CommCell Console, right-click the client computer and click **All Tasks | Push Firewall Configuration**. This updates the firewall configuration files on the client computer.

21. Click **Continue**.

The client is configured to communicate with the CommServe and MediaAgent.

Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.

- From the CommCell Console, right-click the client computer and click **All Tasks | Check Readiness**. The results are displayed in **Client Connectivity** dialog box. If the client computer is not ready, verify your settings with the above recommendations and revise the settings if required.

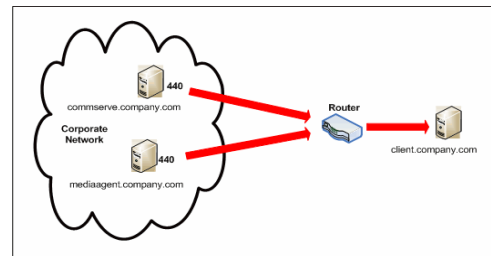


Connectivity between CommServe, MediaAgent, and the client is now established.

COMMSERVE CONNECTS TO THE CLIENT (ONE-WAY FIREWALL)

Consider the diagram that illustrates a direct connection setup where the CommServe opens tunnel connection towards the client.

The following sections explain the configuration required on the CommServe, MediaAgent, and the client to operate in this scenario.



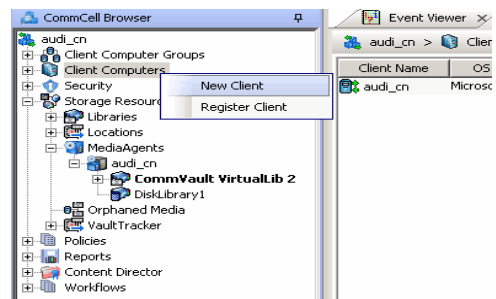
Review the following considerations before you begin.

- Make a note of the port configurations on your firewall and substitute them appropriately in the following instructions.
- Microsoft Internet Information Services (IIS) uses port number 443 by default. So if you have IIS running on a computer, then you will not be able to use port 443 for firewall configuration on that computer.

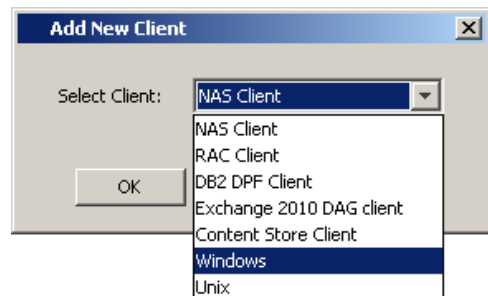
SETUP CONNECTION TO THE COMMSERVE

In this configuration, CommServe establishes tunnel connection with the client. Since the client is not yet available in the CommCell, follow the steps below to create a placeholder client and configure the firewall settings before installing the client.

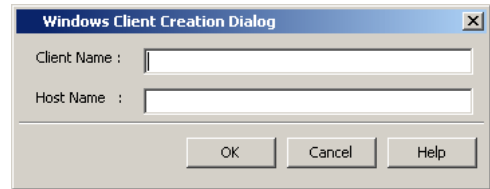
- From the CommCell Console, right-click on the client computer node, and click **New Client**.



- Select **Windows** or **Unix** as applicable.



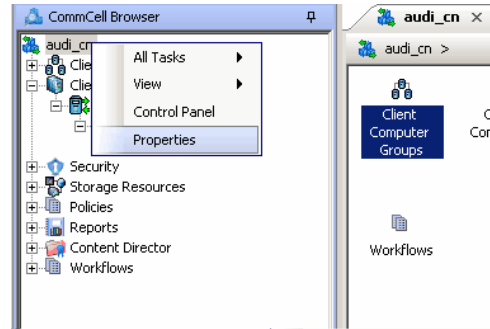
3. Provide the **Client Name** and the **Host Name** of the client computer to be installed.
 - The Client Name must be the same client name that you will provide during the client installation — the name by which the client will be identified in the CommCell Browser after installation. Ensure to provide the correct client name as the firewall program uses it to establish communication.
 - The Host Name must be either the fully qualified domain name of the client or the IP address that the CommServe should use to open tunnel connection to the client. If there is a NAT router between the client and the CommServe, provide the NAT IP address.



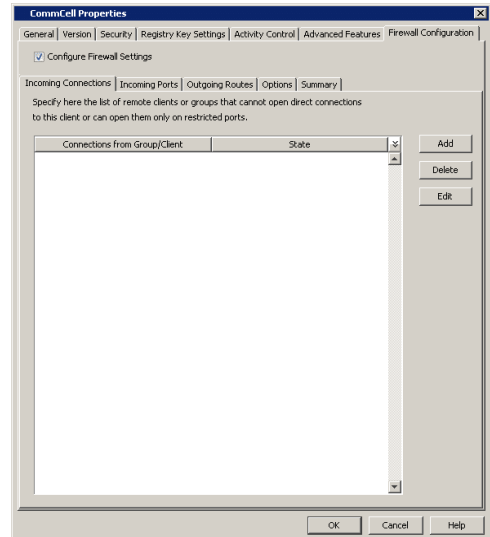
Click **OK**.

A placeholder client is created for firewall configuration use.

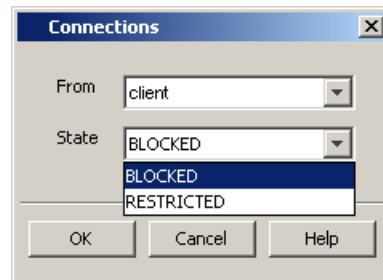
4. From the CommCell Console, right-click the CommServe computer and click **Properties**.



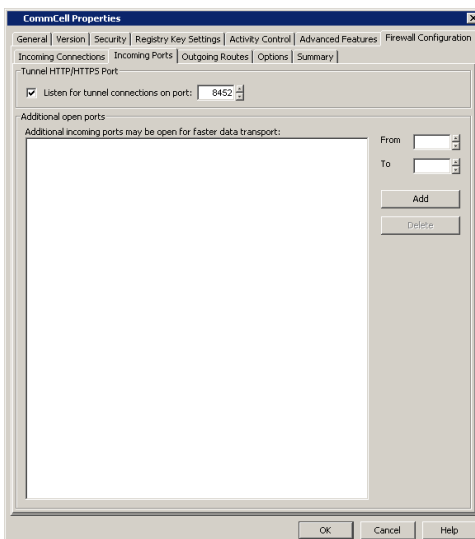
5. Click the **Firewall Configuration** tab.
6.
 - Click the **Incoming Connections** tab.
 - Click **Add**.



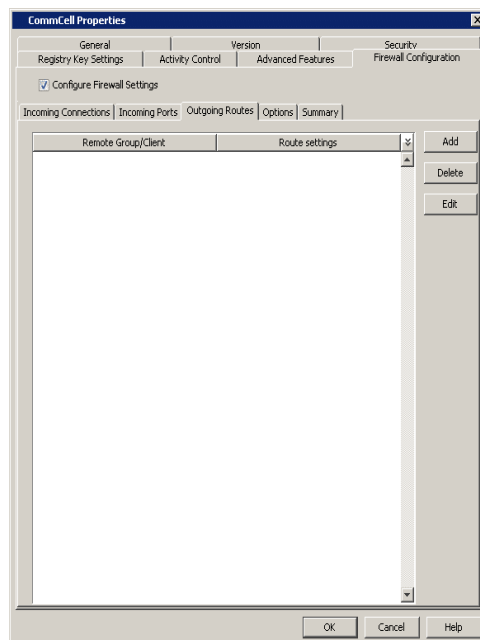
7.
 - In the **From** field, select the name of the placeholder client you just added.
 - In the **State** field, select **Blocked**, since the CommServe does not open tunnel connection to the client.
 - Click **OK**.



8.
 - Click the **Incoming Ports** tab.
 - As the CommServe does not receive connections from the client, not need to select **Listen for tunnel connections on port**.



- 9.
- Click the **Outgoing Routes** tab.
 - Click **Add** to specify the outgoing route toward the proxy.
- Outgoing routes are automatically created in the direct connectivity setup — manual entry is not required. However, you might want to create an entry if you wish to achieve one of the following.
- Enable HTTPS encryption for the tunnel or data traffic.
 - Encrypt the data connections by forcing the connections into the tunnel. However, consider the following before using this option.
 - Direct connections always work faster. Forcing data connections into the tunnel might degrade performance of data protection operations.
 - If you wish to encrypt your backup data, you must rather configure encryption at the client level which offers more control and stores the data in encrypted form on the backup media as well.



- 10.
- Select the name of the placeholder client in **Remote Group/Client**.
 - Select **Direct**.
 - Select **HTTP**.
 - **Force all data (along with control) traffic into the tunnel** option is not required as this route is not toward MediaAgent.
 - Click **OK**.

- From the CommCell Console right-click the CommServe computer, click **All Tasks**, and click **Push Firewall Configuration**.

- Click **Continue**.

The CommServe is configured to open tunnel connections with the client.

Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.

INSTALL THE CLIENT

See Installation for step-by-step installation procedures to install the client.

During installation of the client, use one of the following firewall configuration sequence.

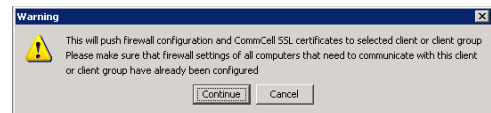
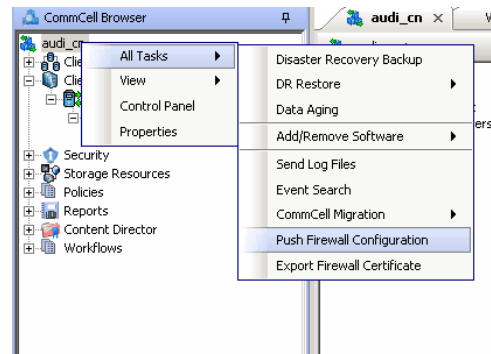
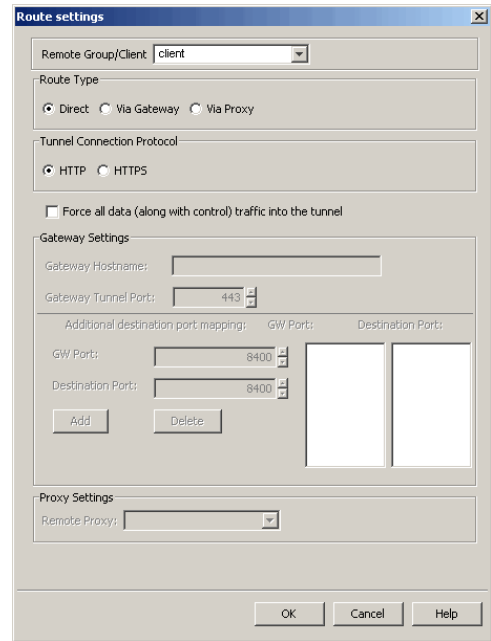
- CommServe can reach the Client/MediaAgent (Windows clients)
- CommServe can reach the Client/MediaAgent (Unix clients)

CONFIGURE THE COMMSERVE, MEDIAAGENT AND CLIENT

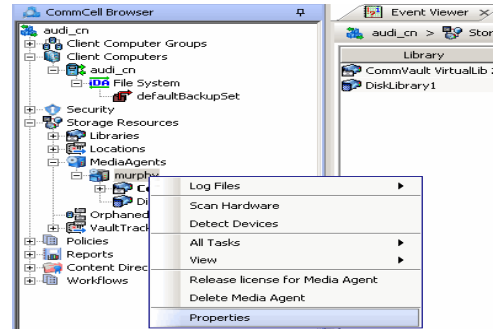
Use the following steps to establish incoming and outgoing connectivity details between the CommServe, MediaAgent, and the client computer.

The configuration required for the CommServe to connect to the client was done prior to installing the client. No additional configuration is required.

- To configure the MediaAgent, right-click the MediaAgent computer from the CommCell Console and click **Properties**.



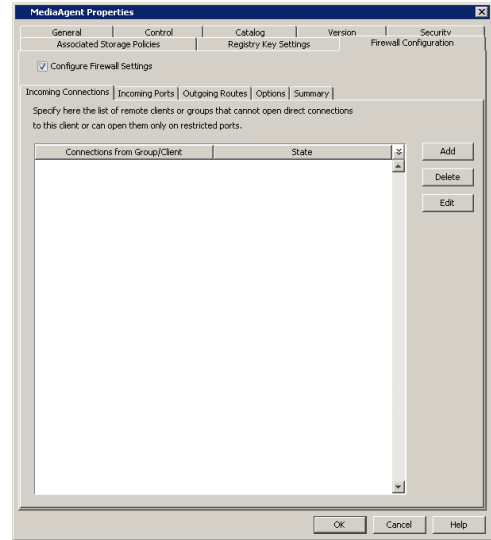
2. Click the **Firewall Configuration** tab.
3. From the **Incoming Connections** tab, click **Add**.



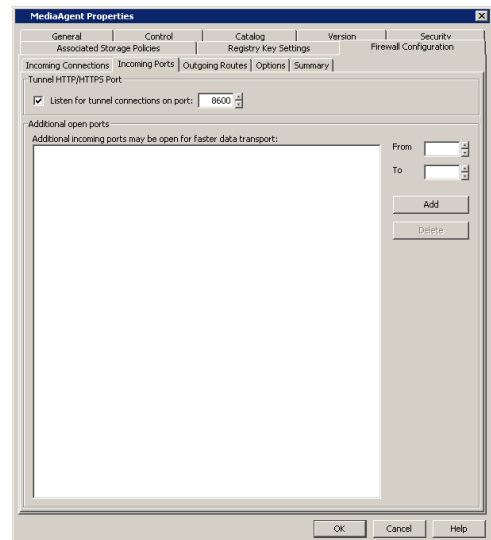
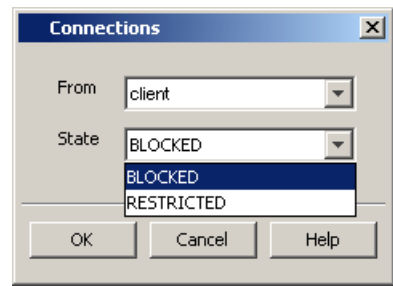
4.
 - In the **From** field, select the name of the client you just installed.
 - In the **State** field, select **Blocked**, since the MediaAgent does not open tunnel connection to the client.

Note that if the firewall allowed any connection from the client to the MediaAgent, then this entry is not required.

 - Click **OK** to continue.



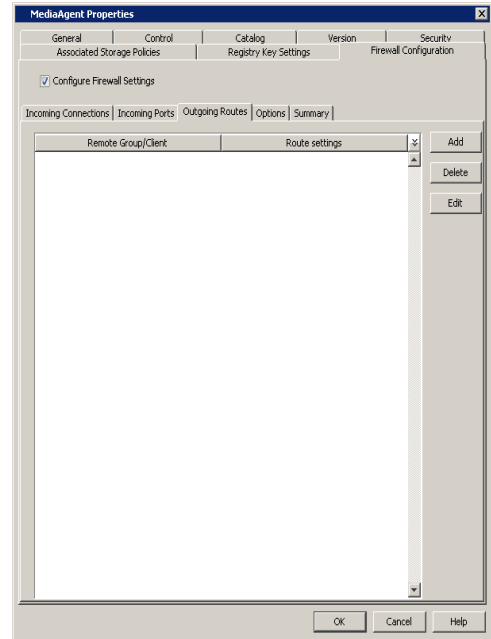
5.
 - Click the **Incoming Ports** tab.
 - Assuming that the MediaAgent opens tunnel connection to the client, there is no need to select **Listen for tunnel connections on port**.
 - Click **OK**.



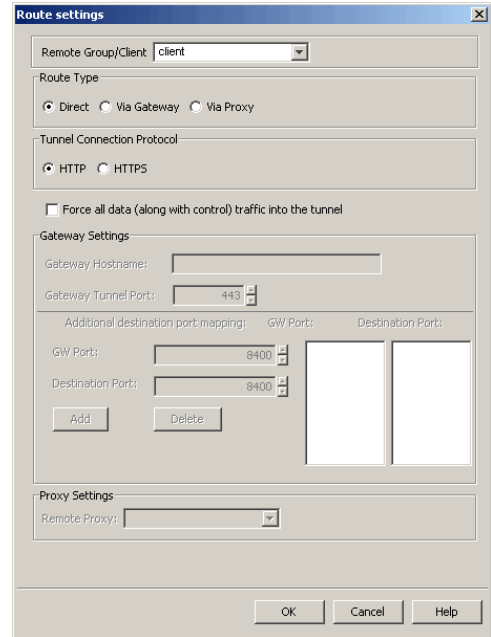
6.
 - Click the **Outgoing Routes** tab.
 - Click **Add** to specify the outgoing route toward the proxy.

Outgoing routes are automatically created in the direct connectivity setup — manual entry is not required. However, you might want to create an entry if you wish to achieve one of the following.

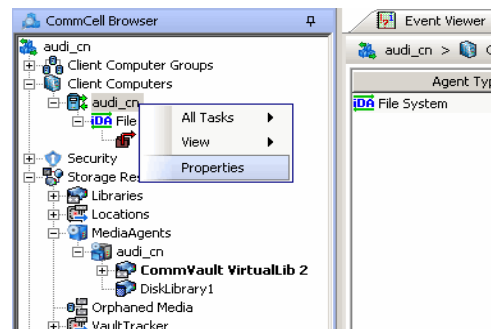
 - Enable HTTPS encryption for the tunnel or data traffic.
 - Encrypt the data connections by forcing the connections into the tunnel. However, consider the following before using this option.
 - Direct connections always work faster. Forcing data connections into the tunnel might degrade performance of data protection operations.
 - If you wish to encrypt your backup data, you must rather configure encryption at the client level which offers more control and stores the data in encrypted form on the backup media as well.



7.
 - Select the client name in the **Remote Group/Client** field.
 - Select **Direct**.
 - Select **HTTP**.
 - Select **Force all data (along with the control) traffic into the tunnel** to force the data traffic into the control tunnel. This automatically encrypts the data connection.
 - Click **OK**.

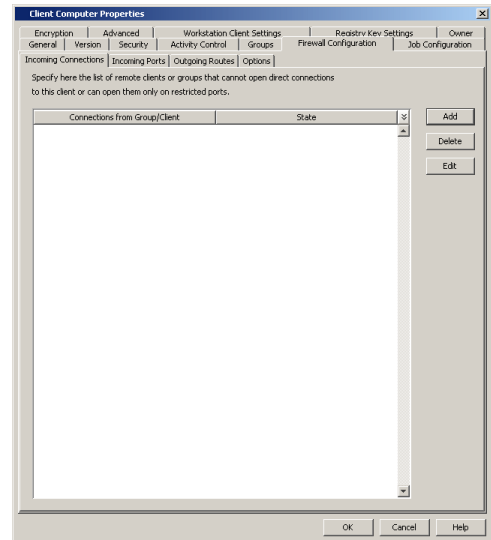


8. From the **Outgoing Routes** tab, click **OK**.
The MediaAgent is now configured to communicate with the client.
9. To configure the Client, right-click the client computer from the CommCell Console and click **Properties**.

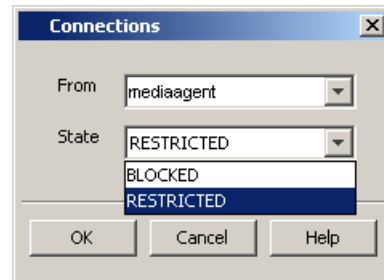
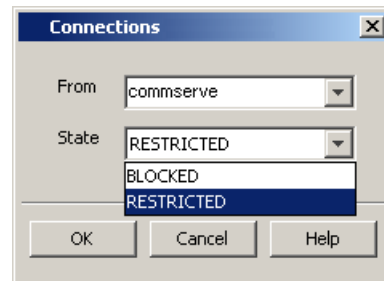


10. Click the **Firewall Configuration** tab.
11. From the **Incoming Connections** tab, click **Add**.

12.
 - In the **From** field, select the name of the CommServe computer.
 - In the **State** field, select **Restricted**, since the CommServe will connect to the Client through a port.
 - Click **OK**.



13.
 - Click **Add** again to specify the MediaAgent connection details.
 - In the **From** field, select the name of the MediaAgent computer.
 - In the **State** field, select **Restricted**, since the MediaAgent will connect to the Client through a port.
 - Click **OK**.

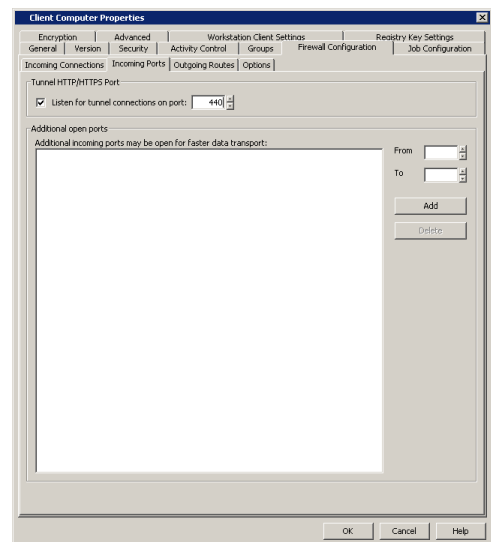


14.
 - Click the **Incoming Ports** tab.
 - Select **Listen for tunnel connections on port** and specify the incoming port number on which the firewall will allow connections from the CommServe and the MediaAgent.
 - **Additional Open Ports:** You can speed up the data transfer by opening additional ports towards the client on the firewall and recording them as open in this screen. Specify the range of ports in the **Additional open ports** area, **From** and **To** fields. Click **Add** to add the ports. To remove a port from the listing, select the port and click **Delete**. The ports must be within the range of 1024 - 65000. Ensure that the ports specified here are not used by other applications.

Review the following recommendations.

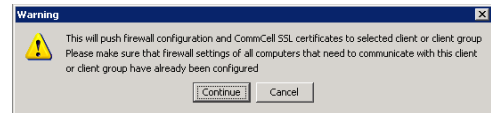
- For backups to MediaAgents with **Optimize for concurrent LAN backups** option unchecked, opening additional incoming ports improves the backup performance. The number of open ports should correspond to the number of simultaneously running backup streams.
- For ContinuousDataReplicator and Workstation Backup destination computers, opening additional incoming ports improves the replication performance.

- Click **OK**.



15. From the CommCell Console, right-click the client computer and click **All Tasks | Push Firewall Configuration**. This updates the firewall configuration files on the client computer.

16. Click **Continue**.
The client is configured to communicate with the CommServe and MediaAgent.
Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.
17. From the CommCell Console, right-click the client computer and click **All Tasks | Check Readiness**. The results are displayed in **Client Connectivity** dialog box.
If the client computer is not ready, verify your settings with the above recommendations and revise the settings if required.

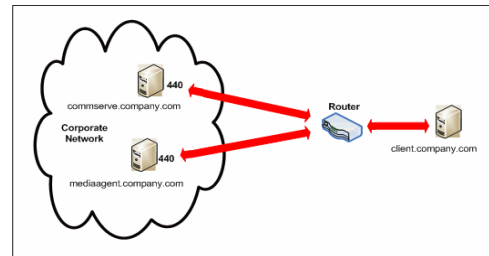


Connectivity between CommServe, MediaAgent, and the client is now established.

CLIENT AND COMMSERVE CONNECT TO EACH OTHER (TWO-WAY FIREWALL)

Consider the diagram that illustrates a direct connection setup where the client, CommServe and MediaAgent open tunnel connection between them.

The following sections explain the configuration required on the CommServe, MediaAgent, and the client to operate in this scenario.



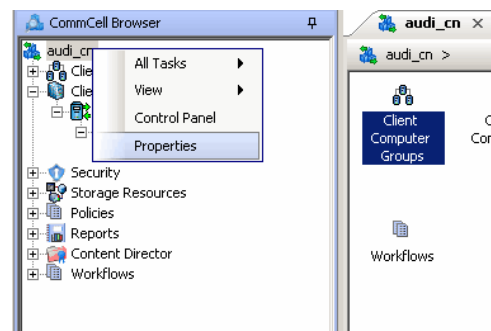
Review the following considerations before you begin.

- Make a note of the port configurations on your firewall and substitute them appropriately in the following instructions.
- Microsoft Internet Information Services (IIS) uses port number 443 by default. So if you have IIS running on a computer, then you will not be able to use port 443 for firewall configuration on that computer.

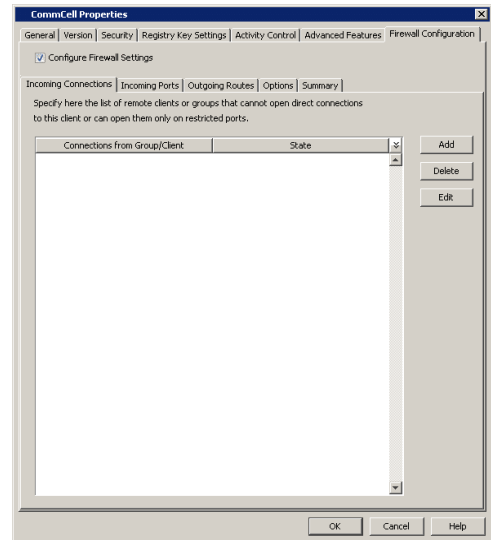
SETUP CONNECTION TO THE COMMSERVE

Before installing the client, you will have to provide an incoming port number on which the CommServe will receive tunnel connections from the client. The following steps explain the configurations required for this purpose.

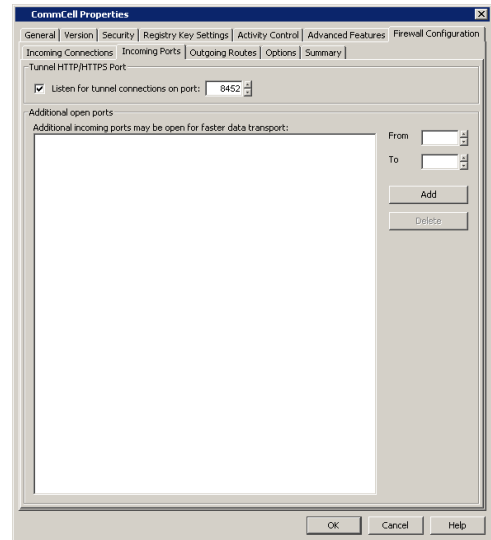
1. From the CommCell Console, right-click the CommServe computer and click **Properties**.
2. Click the **Firewall Configuration** tab.



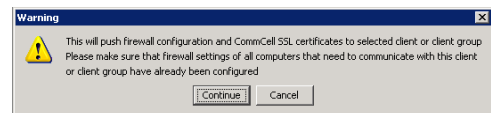
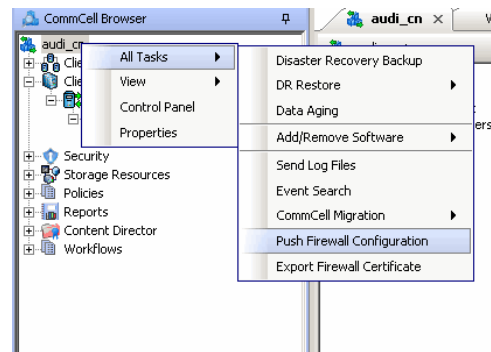
3.
 - Click the **Incoming Ports** tab.
 - Select **Listen for tunnel connections on port** and specify the port number on which the incoming tunnel connection is received.
 - Click **OK**.



4. From the CommCell Console, right-click the CommServe computer and click **All Tasks | Push Firewall Configuration**.



5. Click **Continue**.
The specified configuration is saved.
Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.



INSTALL THE CLIENT

In this configuration the client and the CommServe establish connection between them using one or more ports. To install the client across a firewall in this setup, you will have to specify the path to reach the CommServe computer. During installation of the client, use one of the following firewall configuration sequence.

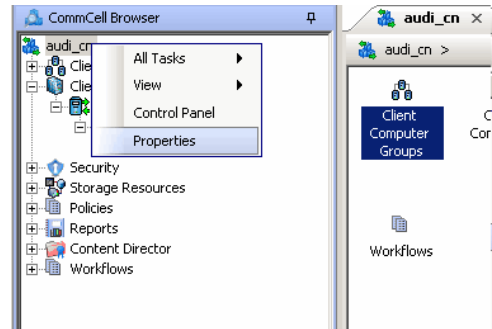
- Client/MediaAgent and CommServe can reach each other (Windows clients)

- Client/MediaAgent and CommServe can reach each other (Unix clients)

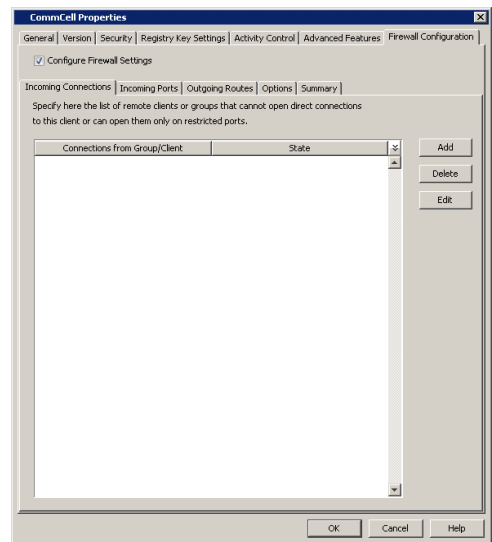
CONFIGURE THE COMMSERVE, MEDIAAGENT AND CLIENT

Use the following steps to establish incoming and outgoing connectivity details between the CommServe, MediaAgent, and the client computer.

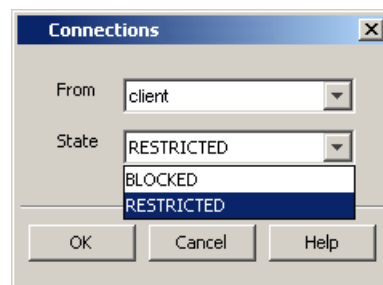
1. To configure the CommServe, right-click the CommServe computer from the CommCell Console and click **Properties**.



2. Click the **Firewall Configuration** tab.
3. From the **Incoming Connections** tab, click **Add**.



4.
 - In the **From** field, select the name of the client you just installed.
 - In the **State** field, select **Restricted**, since the client can reach the CommServe.
 - Click **OK**.



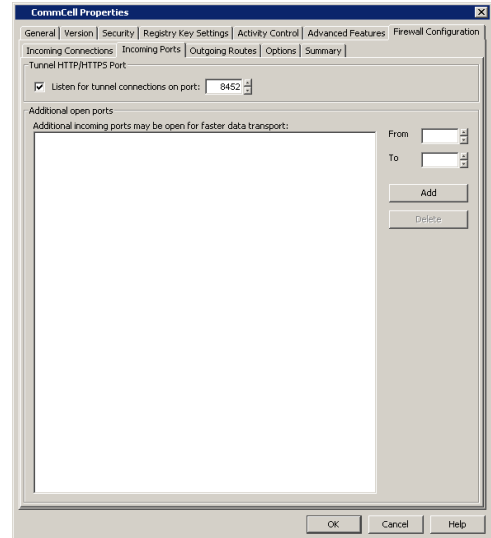
5.
 - Click the **Incoming Ports** tab. You will see the tunnel port already specified on the CommServe.
 - **Additional Open Ports:** For components that handle data transfer (for example, MediaAgent, File System iDataAgent, etc.), you can speed up the data transfer by opening additional ports on the firewall and recording them as open in this screen. Specify the range of ports in the **Additional open ports** area, **From** and **To** fields. Click **Add** to add the ports. To remove a port from the listing, select the port and click **Delete**. The ports must be within the range of 1024 - 65000. Ensure that the ports specified here are not used by other applications.

Review the following recommendations.

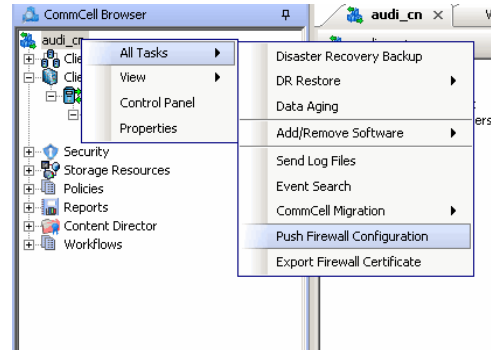
- For MediaAgents involving multi-stream restores, opening additional ports increases the restore performance. The number of open ports should correspond to the number of simultaneously running restore streams.
- For MediaAgents with **Optimize for concurrent LAN backups** option enabled, opening the incoming port of the Bull Calypso Communications Service improves the backup performance.

- For MediaAgents performing SnapProtect operations with Data Replicator snap engine, opening additional ports increases the backup performance.
- For ContinuousDataReplicator and Workstation Backup destination computers, opening additional incoming ports improves the replication performance.

- Click **OK**.



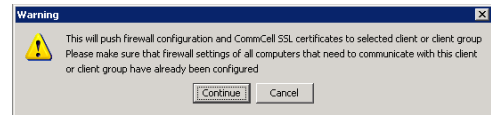
6. From the CommCell Console, right-click the CommServe computer and click **All Tasks | Push Firewall Configuration**.



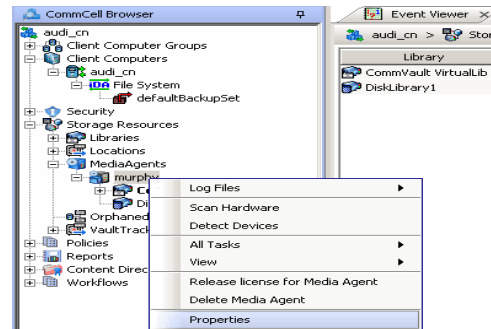
7. Click **Continue**.

The CommServe is configured to receive communication from the client.

Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.



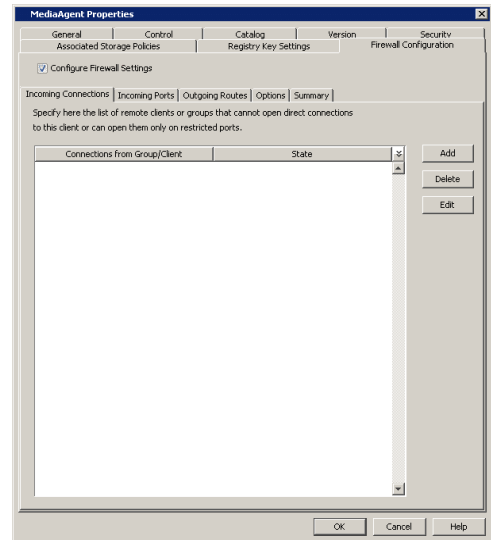
8. To configure the MediaAgent, right-click the MediaAgent computer from the CommCell Console and click **Properties**.



9. Click the **Firewall Configuration** tab.

10. From the **Incoming Connections** tab, click **Add**.

11.
 - In the **From** field, specify the name of the client you just installed.
 - In the **State** field, select **Restricted**, since the client can reach the MediaAgent.
 - Click **OK**.



12.
 - Click the **Incoming Ports** tab.
 - Select the **Listen for tunnel connections on port** option and specify the tunnel port through which connections from the client are received on the MediaAgent computer.
 - **Additional Open Ports:** For components that handle data transfer (for example, MediaAgent, File System iDataAgent, etc.), you can speed up the data transfer by opening additional ports on the firewall and recording them as open in this screen. Specify the range of ports in the **Additional open ports** area, **From** and **To** fields. Click **Add** to add the ports. To remove a port from the listing, select the port and click **Delete**. The ports must be within the range of 1024 - 65000. Ensure that the ports specified here are not used by other applications.

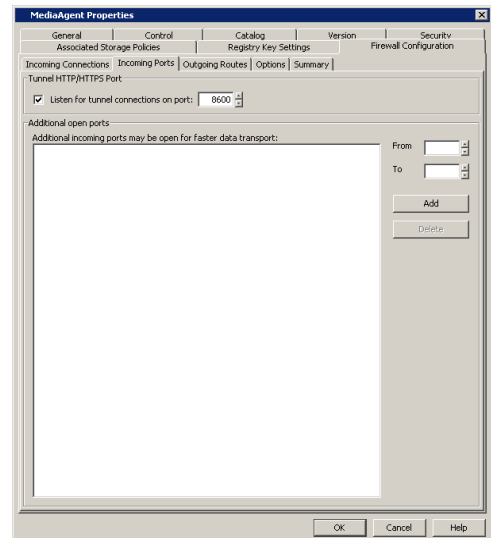
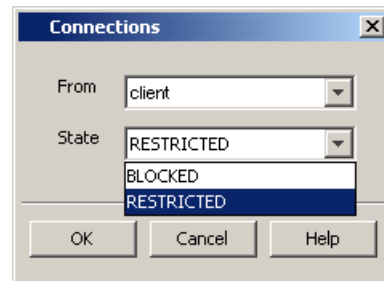
Review the following recommendations.

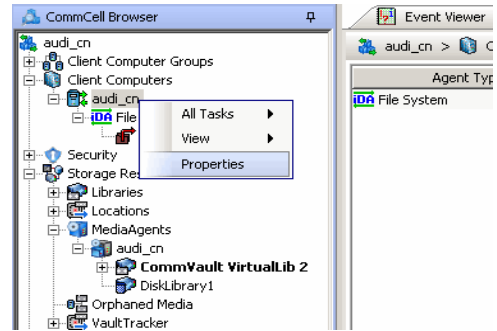
- For MediaAgents involving multi-stream restores, opening additional ports increases the restore performance. The number of open ports should correspond to the number of simultaneously running restore streams.
- For MediaAgents with **Optimize for concurrent LAN backups** option enabled, opening the incoming port of the Bull Calypso Communications Service improves the backup performance.
- For MediaAgents performing SnapProtect operations with Data Replicator snap engine, opening additional ports increases the backup performance.
- For ContinuousDataReplicator and Workstation Backup destination computers, opening additional incoming ports improves the replication performance.

- Click **OK**.

The MediaAgent is now configured to receive communication from the client.

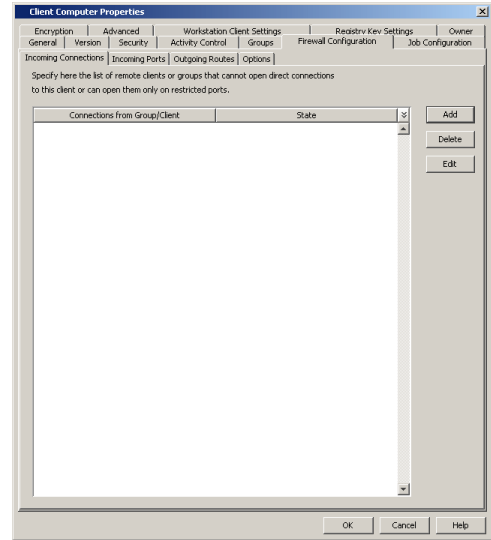
13. To configure the Client, right-click the client computer from the CommCell Console and click **Properties**.



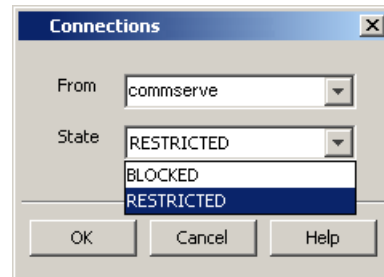


14. Click the **Firewall Configuration** tab.

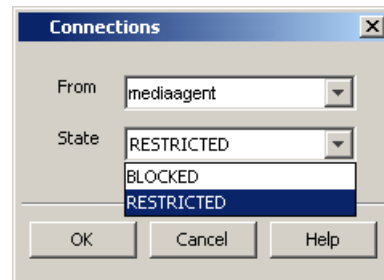
15. From the **Incoming Connections** tab, click **Add**.



- 16.
 - In the **From** field, specify the name of the CommServe computer.
 - In the **State** field, select **Restricted**, since the Client can connect to the CommServe.
 - Click **OK**.



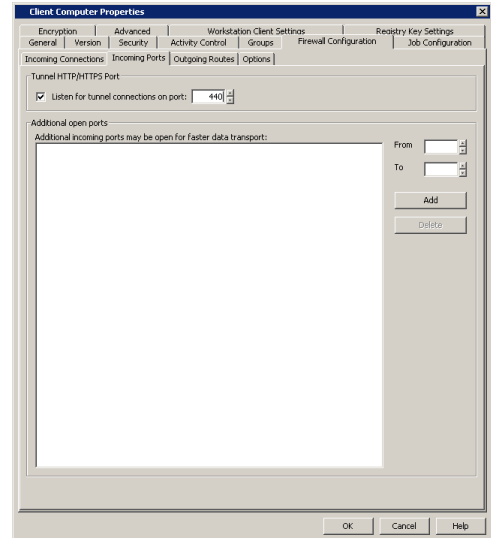
- 17.
 - Click **Add** again to specify the MediaAgent connection details.
 - In the **From** field, specify the name of the MediaAgent computer.
 - In the **State** field, select **Restricted**, since the Client can connect to the MediaAgent.
 - Click **OK**.



- 18.
 - Click the **Incoming Ports** tab.
 - Select the **Listen for tunnel connections on port** option and specify the incoming port number on which the firewall will allow connections from the CommServe and the MediaAgent. The client will listen for incoming tunnel connections on this port.
 - **Additional Open Ports:** You can speed up the data transfer by opening additional ports towards the client on the firewall and recording them as open in this screen. Specify the range of ports in the **Additional open ports** area, **From** and **To** fields. Click **Add** to add the ports. To remove a port from the listing, select the port and click **Delete**. The ports must be within the range of 1024 - 65000. Ensure that the ports specified here are not used by other applications.

Review the following recommendations.

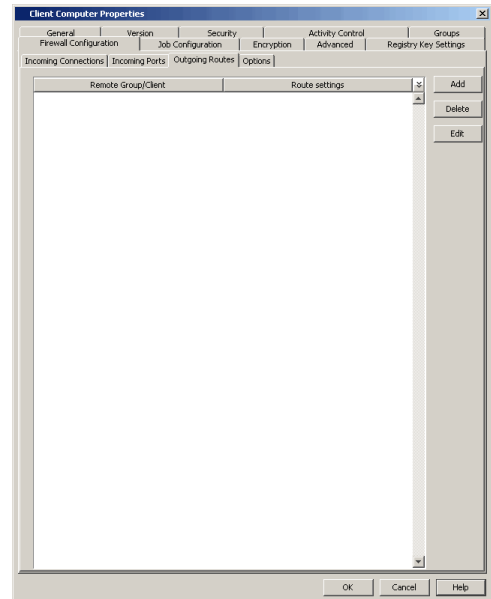
- For backups to MediaAgents with **Optimize for concurrent LAN backups** option unchecked, opening additional incoming ports improves the backup performance. The number of open ports should correspond to the number of simultaneously running backup streams.
- For ContinuousDataReplicator and Workstation Backup destination computers, opening additional incoming ports improves the replication performance.
- Click **OK**.



- 19.
- Click the **Outgoing Routes** tab.
 - Click **Add**.

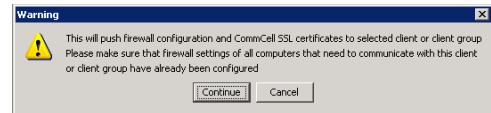
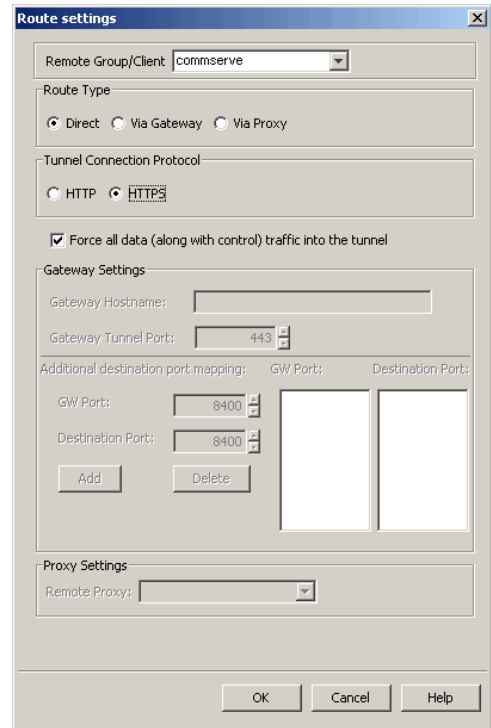
Outgoing routes are automatically created in the direct connectivity setup — manual entry is not required. However, you might want to create an entry if you wish to achieve one of the following.

- Enable HTTPS encryption for the tunnel or data traffic.
- Encrypt the data connections by forcing the connections into the tunnel. However, consider the following before using this option.
 - Direct connections always work faster. Forcing data connections into the tunnel might degrade performance of data protection operations.
 - If you wish to encrypt your backup data, you must rather configure encryption at the client level which offers more control and stores the data in encrypted form on the backup media as well.



- 20.
- Select the CommServe name in **Remote Group/Client**.
 - Select **Direct**.
 - Select **HTTPS** protocol. This will enable authentication and encryption for tunnel connections.
 - **Force all data (along with control) traffic into the tunnel** option is not required as this route is not toward MediaAgent.
 - Click **OK**.

21. From the CommCell Console, right-click the client computer and click **All Tasks | Push Firewall Configuration**. This updates the firewall configuration files on the client computer.
22. Click **Continue**.
The client is configured to communicate with the CommServe and MediaAgent.
Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.
23. From the CommCell Console, right-click the client computer and click **All Tasks | Check Readiness**. The results are displayed in **Client Connectivity** dialog box.
If the client computer is not ready, verify your settings with the above recommendations and revise the settings if required.



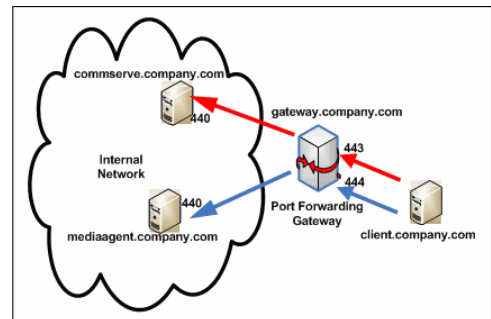
Connectivity between CommServe, MediaAgent, and the client is now established.

OPERATING THROUGH A PORT-FORWARDING GATEWAY

There are cases where direct connectivity setups do not work. Imagine a situation where the CommServe and MediaAgent are located inside a company's internal network, and the entire network is exposed to the outside world through a single IP address. Typically this IP address belongs to a firewall/gateway that works as a NAT device for connections from the internal network to the outside.

In scenarios like this, you can establish a port-forwarding at the gateway to forward incoming connections on specific ports to certain machines on the internal network (on specific ports). You can then configure the client to open a direct connection to the port-forwarder's IP on a specific port to reach a particular internal server. This creates a custom route from client towards the internally running server(s).

Consider the diagram on the right that illustrates the setup. The following sections explain how to configure the software to operate in this setup.



Review the following considerations before you begin.

- Make a note of the port configurations in your setup and substitute them in the following instructions.
- Microsoft Internet Information Services (IIS) uses port number 443 by default. So if you have IIS running on a computer, then you will not be able to use port 443 for firewall configuration on that computer.
- Any additional destination port specified in the outgoing connection routes of the client must also be defined in the incoming port list of the remote client (CommServe or MediaAgent).

CONFIGURE THE PORT-FORWARDING GATEWAY

A port-forwarding gateway sends incoming connections to specific machines on the internal network based on the incoming connection's destination port number. With reference to our illustration above, the following port-forwarding must be configured on the gateway.

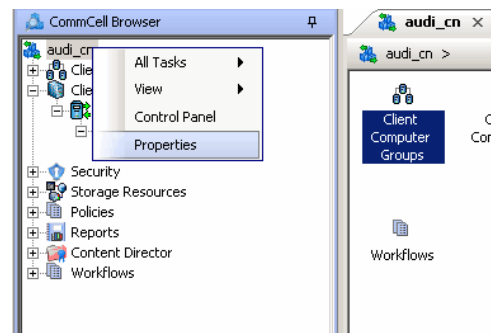
- Connections to gateway.company.com on port 443 must be forwarded to the internally running commserve.company.com on port 440.
- Connections to gateway.company.com on port 444 must be forwarded to the internally running mediaagent.company.com on port 440.

Note that there is no restriction on the internal port numbers. They need not be the same as shown in the illustration. Also, for machines in the internal network, neither the IP addresses nor the names have to be reachable or resolvable from outside.

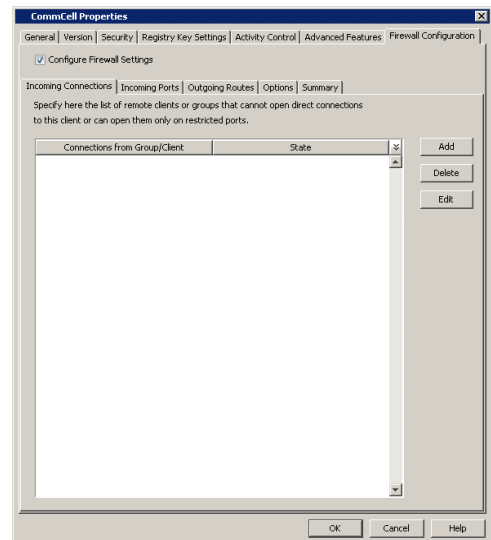
SETUP CONNECTION TO THE COMMSERVE

This procedure assumes that the CommServe is installed and available behind the gateway. The following steps explain the configurations required to connect to the CommServe before installing the client.

1. From the CommCell Console, right-click the CommServe computer and click **Properties**.

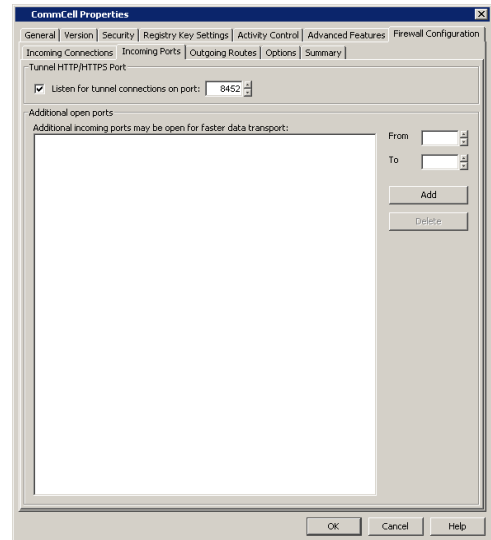


2. Click the **Firewall Configuration** tab.

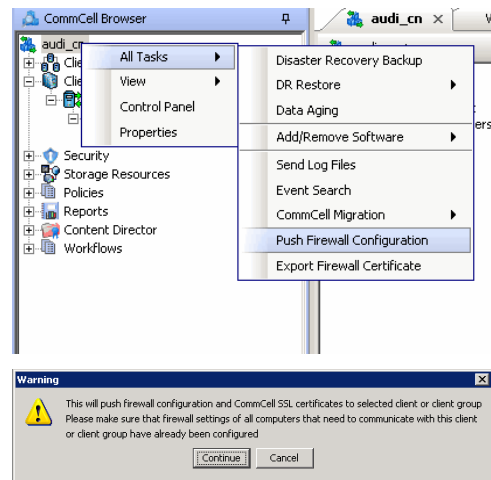


3.
 - Click the **Incoming Ports** tab.
 - Select **Listen for tunnel connections on port** and enter **440** as the port number. The gateway will forward connections to commserve.company.com:440 when the gateway receives them from outside on port 443.
 - Click **OK**.

- From the CommCell Console, right-click the CommServe computer and click **All Tasks | Push Firewall Configuration**.



- Click **Continue**.
The specified configuration is saved.
Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.



INSTALL THE CLIENT

See Installation for step-by-step installation procedures to install the client.

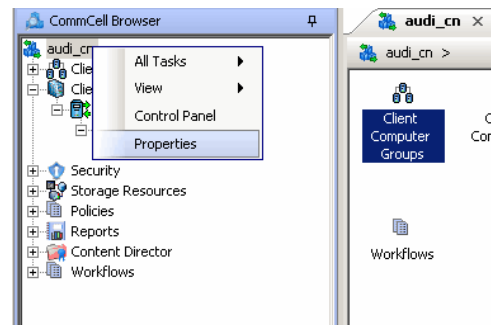
During installation, provide the gateway information through which the CommServe computer can be reached. The install program communicates to the CommServe using this information. Use one of the following firewall configuration sequence.

- CommServe can be Reached through a Port Forwarding Gateway (Windows clients)
- CommServe can be Reached through a Port Forwarding Gateway (Unix clients)

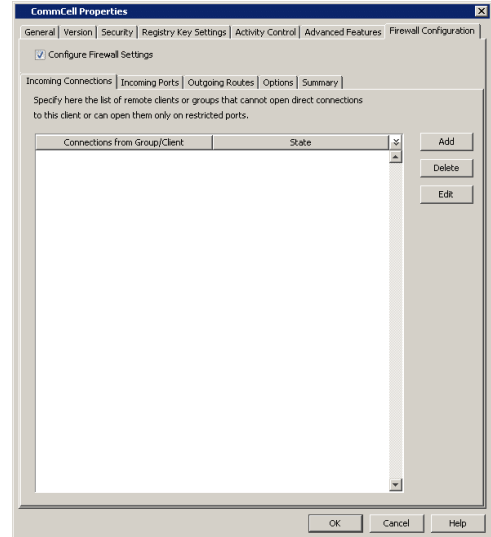
CONFIGURE THE COMMSERVE, MEDIAAGENT AND CLIENT

The previous configurations provided a path to reach the CommServe for installation purposes. To enable data protection operations between the two computers, you will have to establish the communication path between them. Perform the following steps to establish the communication route.

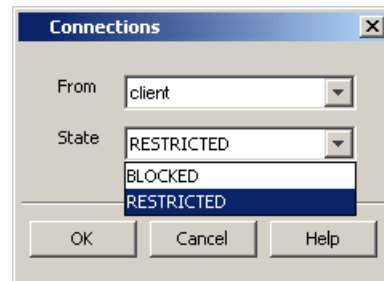
- To configure the CommServe, right-click the CommServe computer from the CommCell Console and click **Properties**.



2. Click the **Firewall Configuration** tab.
3.
 - Click the **Incoming Connections** tab.
 - Click **Add**.



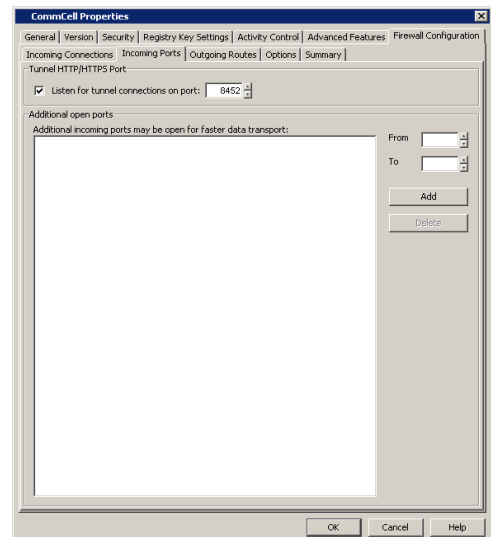
4.
 - In the **From** field, specify the name of the client outside the gateway you just installed.
 - In the **State** field, specify the status of the connection from the client. Since the connection is restricted through a gateway, select **Restricted**.
 - Click **OK**.



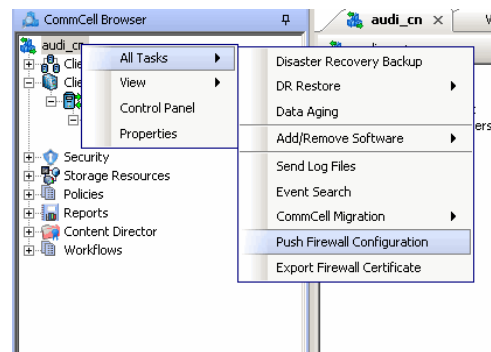
5.
 - Click the **Incoming Ports** tab.

You will see the tunnel port already specified on the CommServe with port number 440.

 - Click **OK**.



6. From the CommCell Console right-click the CommServe computer and click **All Tasks** | **Push Firewall Configuration**.



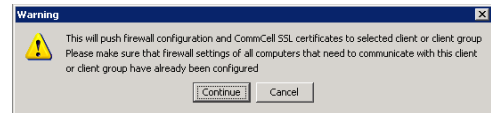
7. Click **Continue**.

The CommServe is configured to receive communication from the client.

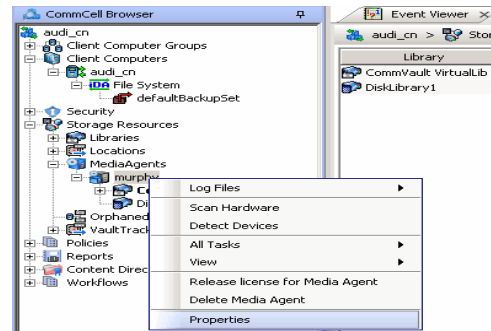
Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.

8. From the CommCell Console, right-click the client computer and click **All Tasks | Check Readiness**. The results are displayed in **Client Connectivity** dialog box.

If the client computer is not ready, verify your settings with the above recommendations and revise the settings if required.

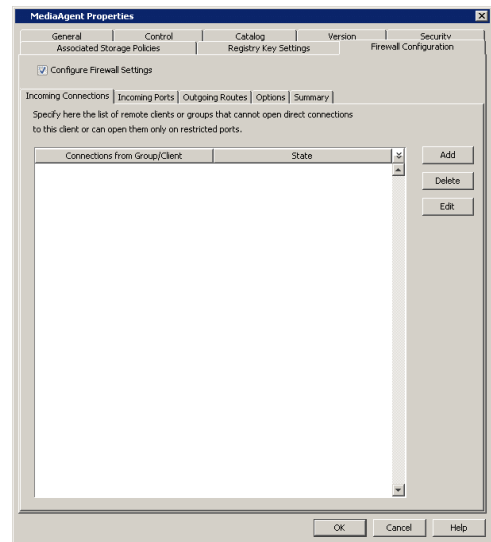


9. To configure the MediaAgent, right-click the MediaAgent computer from the CommCell Console and click **Properties**.

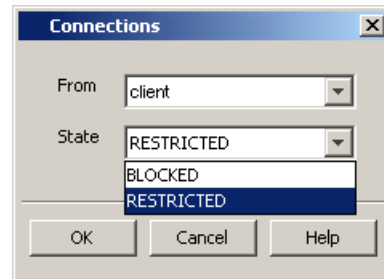


10. Click the **Firewall Configuration** tab.

11. From the **Incoming Connections** tab, click **Add**.



- 12.
 - In the **From** field, specify the name of the client outside the gateway you just installed.
 - In the **State** field, specify the status of the connection from the client. Since the connection is restricted through a gateway, select **Restricted**.
 - Click **OK**.



13.

- Click the **Incoming Ports** tab.

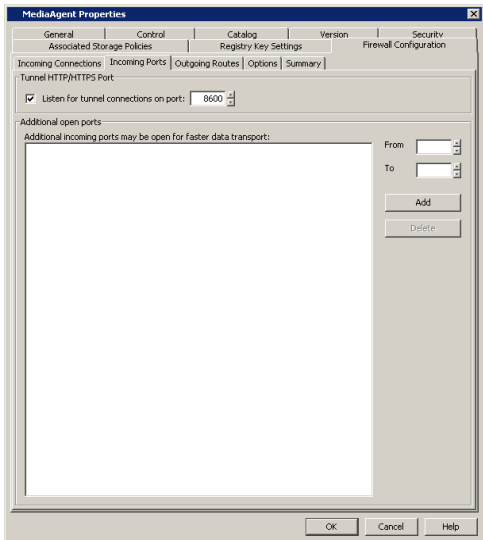
- Select **Listen for tunnel connections on port** and enter **440** as the port number. The gateway will forward connections to **mediaagent.company.com:440** when the gateway receives them from outside on port 444.
- **Additional Open Ports:** For components that handle data transfer (for example, MediaAgent, File System iDataAgent, etc.), you can open and port-forward additional ports on the gateway to speed up the data transport. Note that the additional ports may be the same on the MediaAgent and on the gateway since the gateway has the ability to translate externally visible port numbers to the actual port numbers on the MediaAgent.

In this screen you need to configure the range of ports used for listening to additional incoming connections from the clients. The mapping on how these ports are exported by the gateway must be defined in the outgoing route from the client towards the MediaAgent. (See Step 21) Specify the range of ports in the **Additional open ports** area, **From** and **To** fields. Click **Add** to add the ports. To remove a port from the listing, select the port and click **Delete**. The ports must be within the range of 1024 - 65000. Ensure that the ports specified here are not used by other applications.

Review the following recommendations:

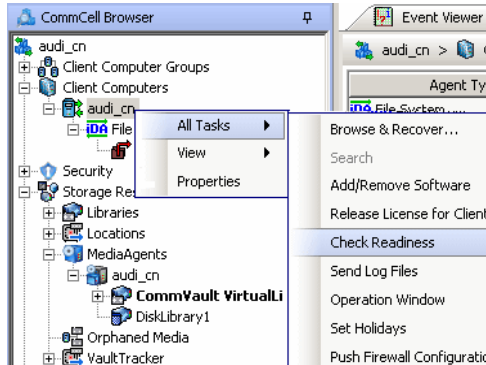
- For MediaAgents involving multi-stream restores, opening additional ports increases the restore performance. The number of open ports should correspond to the number of simultaneously running restore streams.
 - For MediaAgents with **Optimize for concurrent LAN backups** option enabled, opening the incoming port of the Bull Calypso Communications Service improves the backup performance.
 - For MediaAgents performing SnapProtect operations with Data Replicator snap engine, opening additional ports increases the backup performance.
 - For ContinuousDataReplicator and Workstation Backup destination computers, opening additional incoming ports improves the replication performance.
- Click **OK**.

The MediaAgent is now configured to receive communication from the client.

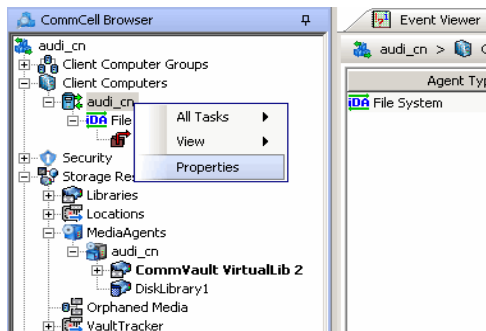


14. From the CommCell Console, right-click the client computer and click **All Tasks | Check Readiness**. The results are displayed in **Client Connectivity** dialog box.

If the client computer is not ready, verify your settings with the above recommendations and revise the settings if required.



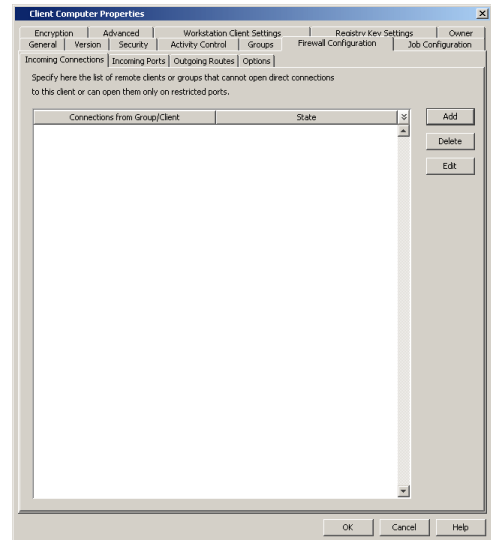
15. To configure the Client, right-click the client computer from the CommCell Console and click **Properties**.



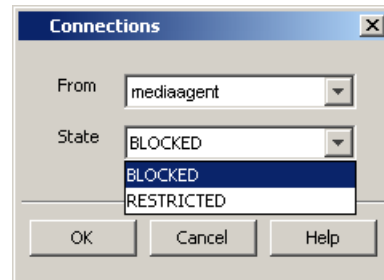
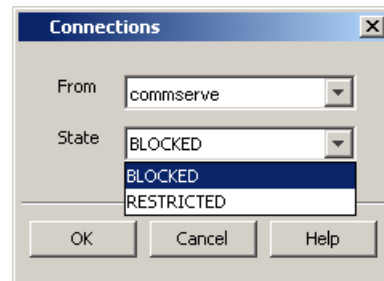
16. Click the **Firewall Configuration** tab.

17. From the **Incoming Connections** tab, click **Add**.

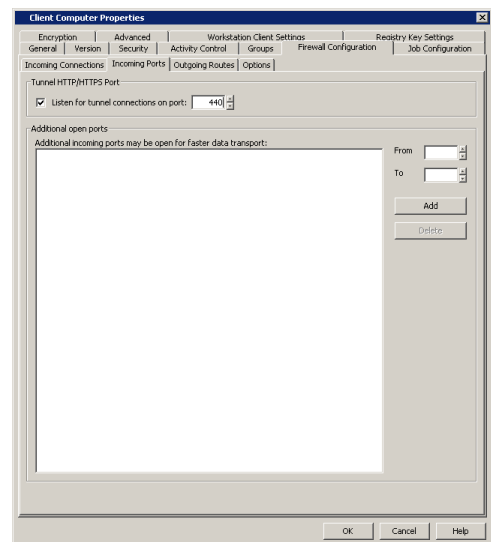
18.
 - In the **From** field, specify the name of the CommServe computer behind the gateway.
 - In the **State** field, specify the status of the connection from the CommServe. Since CommServe does not open connections towards the client, select **Blocked**.
 - Click **OK**.



19.
 - Click **Add** again to specify the MediaAgent connection details.
 - In the **From** field, specify the name of the MediaAgent computer behind the gateway.
 - In the **State** field, specify the status of the connection from the CommServe. Since MediaAgent does not open connections towards the client, select **Blocked**.
 - Click **OK**.

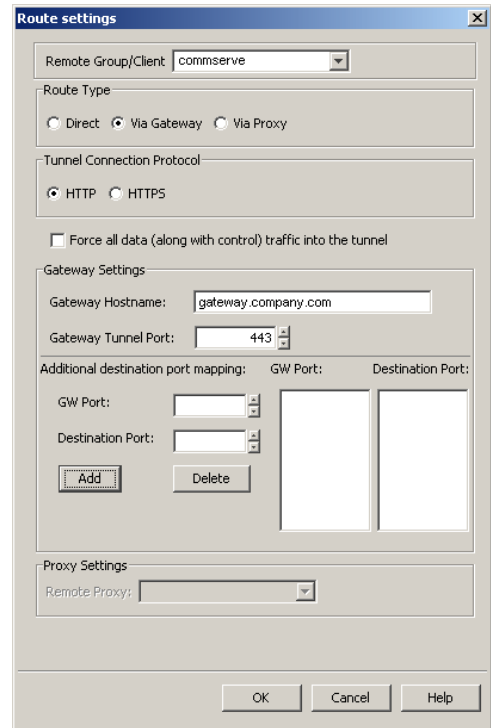
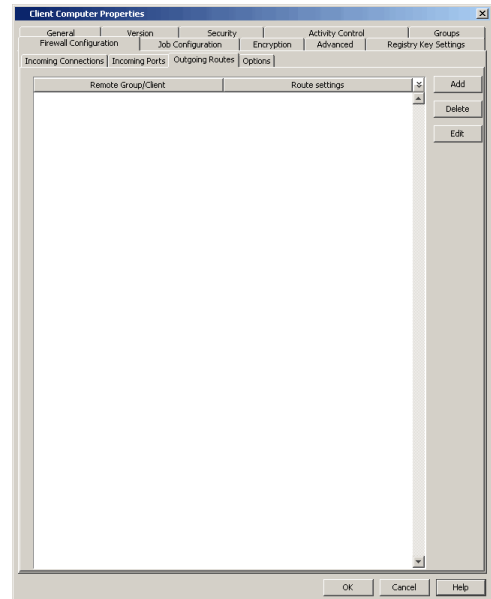


20.
 - Click the **Incoming Ports** tab.
 - As the client does not receive incoming connections from the CommServe or MediaAgent, there is no need to select **Listen for tunnel connections on port**.
 - Click **OK**.



21.
 - Click the **Outgoing Routes** tab.
 - Click **Add** to specify the outgoing connection route from this client towards the CommServe.

- 22.
- Select the CommServe name in **Remote Group/Client**.
 - Select **Via Gateway**.
 - **Force all data (along with control) traffic into the tunnel** option is not required as this route is not toward MediaAgent.
 - Enter the **Gateway Hostname** through which you can reach the CommServe. Referring to our diagram, it is gateway.company.com.
 - Enter the **Gateway Tunnel Port** through which the CommServe can be reached. Referring to the diagram above, this is port number 443.
 - **Additional destination port mapping:** If you want to configure additional destination ports, make sure that these ports are also defined on the CommServe, then you can establish mappings between those ports on the CommServe and the ports on the gateway which the client will connect to.
- To add destination port mapping, specify the incoming gateway port in **GW Port** and the mapping destination port in **Destination Port**. Click **Add** to add the port mapping. To remove a port from the listing, select the port and click **Delete**. The ports must be within the range of 1024 - 65000. Ensure that the ports specified here are not used by other applications.
- Click **OK**.

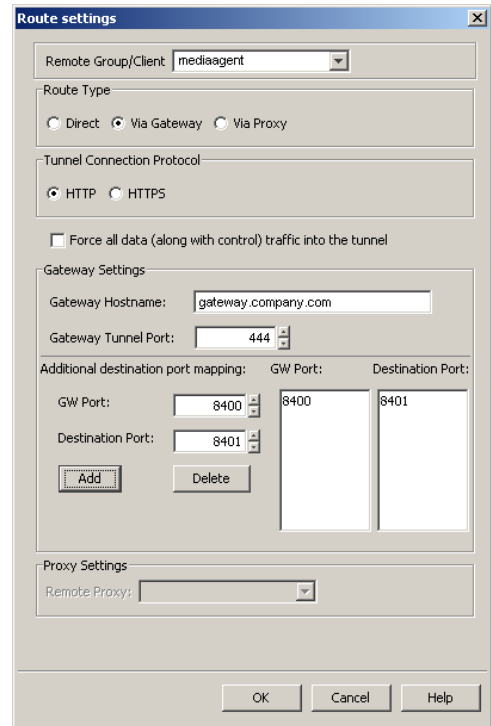


- 23.
- Click **Add** again to specify the outgoing connection route from this client towards the MediaAgent.
 - Select the MediaAgent in **Remote Group/Client**.
 - Select **Via Gateway**.
 - Select **Force all data (along with the control) traffic into the tunnel** to force the data traffic into the control tunnel. This automatically encrypts the data connection.
 - Enter the **Gateway Hostname** through which you can reach the CommServe. Referring to our diagram, it is gateway.company.com.
 - Enter the **Gateway Tunnel Port** through which the MediaAgent can be reached. Referring to the diagram above, this is port number 444.
 - **Additional destination port mapping:** If you want to configure additional destination ports, make sure that these ports are also defined on the MediaAgent (see Step 13), then you can establish mappings between those ports on the MediaAgent and the ports on the gateway which the client will connect to.

To add destination port mapping, specify the incoming gateway port in **GW Port**

and the mapping destination port in **Destination Port**. Click **Add** to add the port mapping. To remove a port from the listing, select the port and click **Delete**. The ports must be within the range of 1024 - 65000. Ensure that the ports specified here are not used by other applications.

- Click **OK**.



24. From the CommCell Console, right-click the client computer and click **All Tasks | Push Firewall Configuration**.

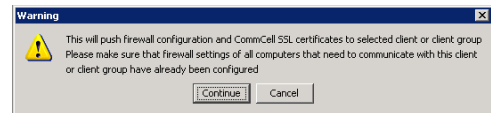
25. Click **Continue**.

The client is configured to communicate with the CommServe and MediaAgent computers behind the gateway.

Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.

26. From the CommCell Console, right-click the client computer and click **All Tasks | Check Readiness**. The results are displayed in **Client Connectivity** dialog box.

If the client computer is not ready, verify your settings with the above recommendations and revise the settings if required.



Connectivity between CommServe, MediaAgent, and the client is now established.

SECURITY CONSIDERATIONS

Since both MediaAgent and CommServe computers are in a way exposed to the outside world through port-forwarded connections, you might want to enable encryption and authentication for the tunnel connections. This can be done in one of the following ways.

- Select **HTTPS** for the **Tunnel Connection Protocol** in the **Outgoing Routes tab** on all outgoing routes.
- Select **Allow only HTTPS** for the **Incoming Tunnel Protocol** in the **Options tab** of the CommServe and MediaAgent. Once HTTPS has been enabled, the client and CommServe/MediaAgent will authenticate each other and set up tunnel encryption in accordance with the HTTPS standard.

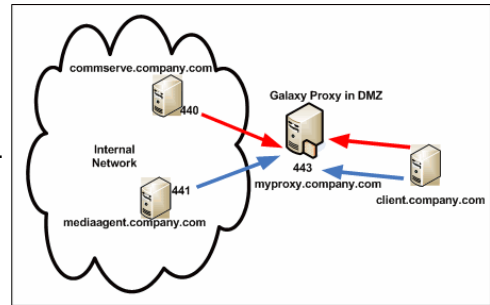
OPERATING THROUGH A DMZ USING CALYPSO PROXY

Calypso proxy is a special proxy configuration where a dedicated *iDataAgent* is placed in a Demilitarized Zone (DMZ) and the firewall(s) is configured to allow connections (from inside and outside networks) into the DMZ. The proxy, which is the agent running in the DMZ, authenticates, encrypts, and proxies accepted tunnel connections to connect the clients operating outside to clients operating inside. In effect, the Calypso proxy acts like a Private

Branch Exchange (PBX) that sets up secure conferences between dial-in client calls. With this setup, firewalls can be configured to disallow straight connections between inside and outside networks.

The diagram on right illustrates this setup where a client from outside communicates to the CommServe and MediaAgent operating in an internal network through the Calypso proxy.

The following sections describe the configuration required to operate the software in this setup.



Review the following considerations before you begin.

- The instructions given below are tailored to the component names and port numbers presented in the illustration. Make a note of the details in your setup and substitute them appropriately.
- Microsoft Internet Information Services (IIS) uses port number 443 by default. So if you have IIS running on a computer, then you will not be able to use port 443 for firewall configuration on that computer.

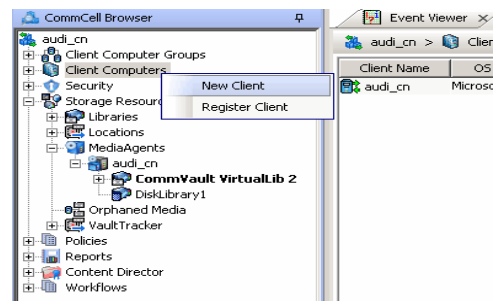
SET UP THE CALYPSO PROXY

The following sections explain the steps involved in creating the Calypso proxy.

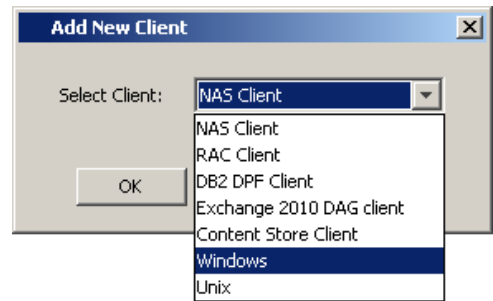
PRECONFIGURE THE CALYPSO PROXY

Follow the steps below to create and configure a placeholder for the Calypso proxy on your CommServe computer before installing it.

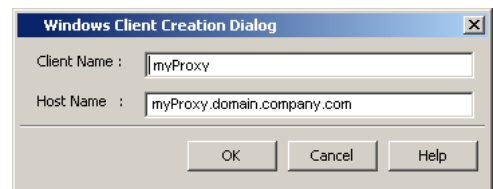
1. From the CommCell Console, right-click on the client computer node, and click **New Client**.



2. Select **Windows** or **Unix** as applicable.

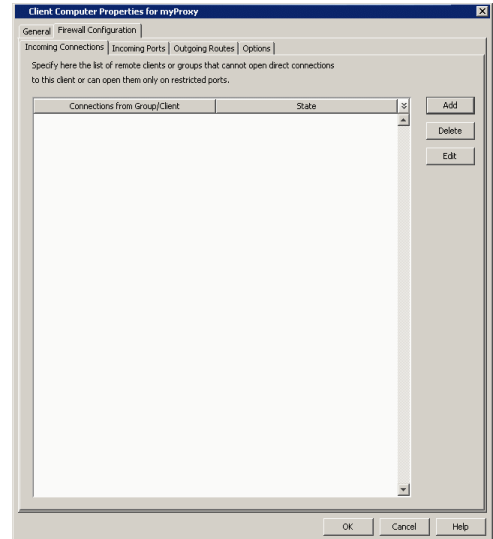
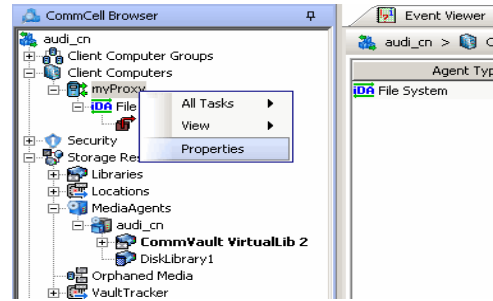


3.
 - Provide the **Client Name** and the **Host Name** you will use during your Calypso proxy installation.
 - Click **OK**.

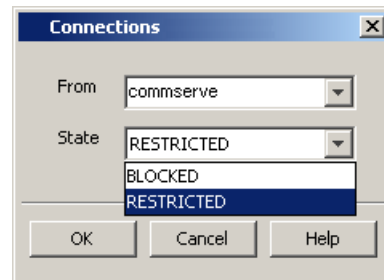


4. From the CommCell Console, right-click the client you just created, and click **Properties**.

5.
 - Click the **Firewall Configuration** tab.
 - Click **Add**.

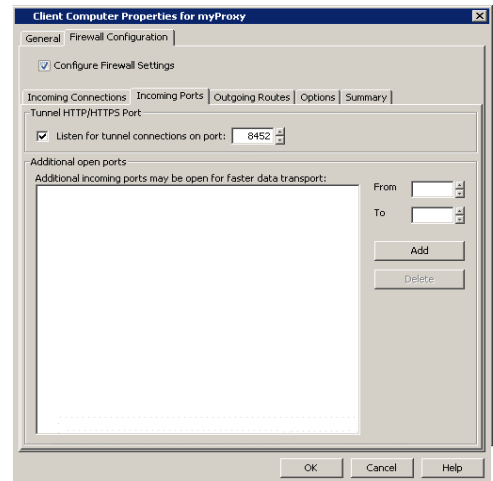


6.
 - In the **From** field, select the CommServe name.
 - In the **State** field, select **Restricted**.
 - Click **OK**.
 - If you have a MediaAgent, repeat this step providing the MediaAgent computer name.



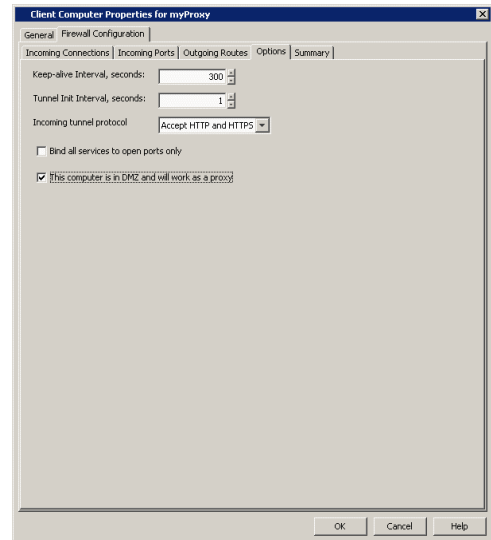
7.
 - Click the **Incoming Ports** tab.
 - Select **Listen for tunnel connections on port** and enter port number on which the Calypso proxy will listen from the CommServe.

Write down the port number used as it will be needed during the Calypso proxy installation.

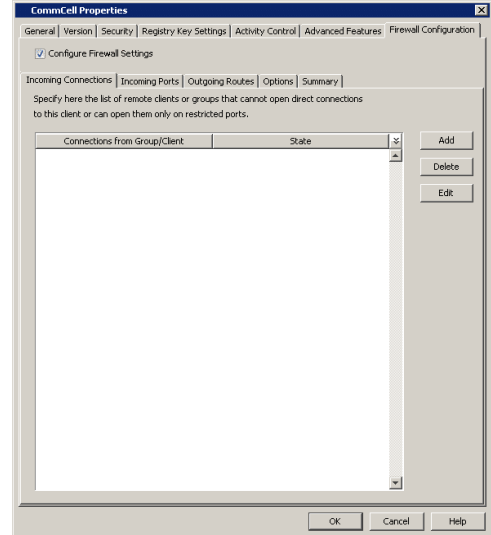
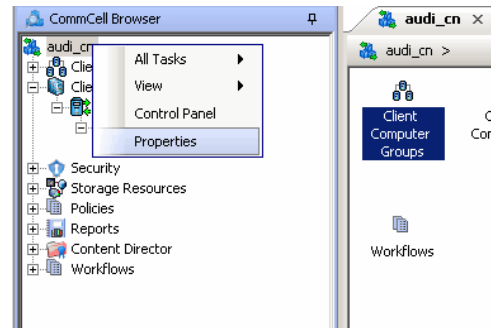


8.
 - Click the **Options** tab.
 - Select **This computer is in DMZ and will work as a proxy**.
 - Click **OK**.

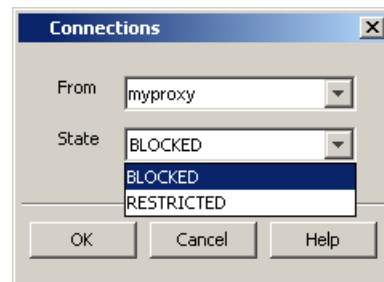
9. From the CommCell Console, right-click the CommServe computer and click **Properties**.



10.
 - Click the **Firewall Configuration** tab.
 - From the **Incoming Connections** tab, click **Add**.

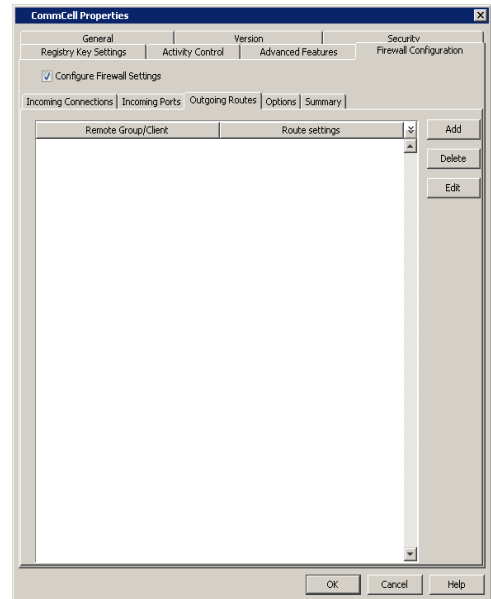


11.
 - In the **From** field, select the Calypso proxy computer.
 - In the **State** field, select **Blocked**.
 - Click **OK**.

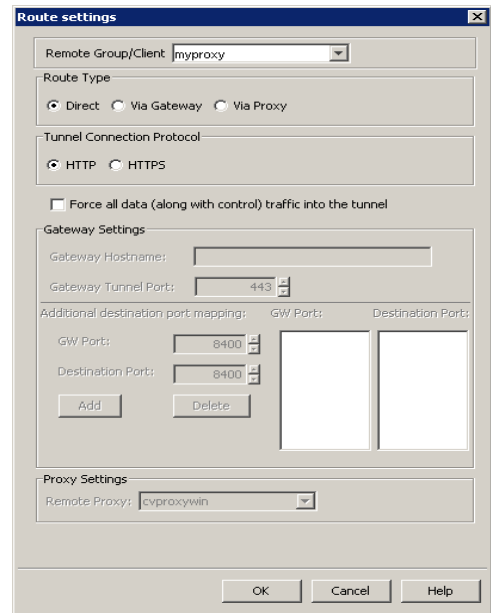


12.
 - Click the **Outgoing Routes** tab.

- Click **Add**.

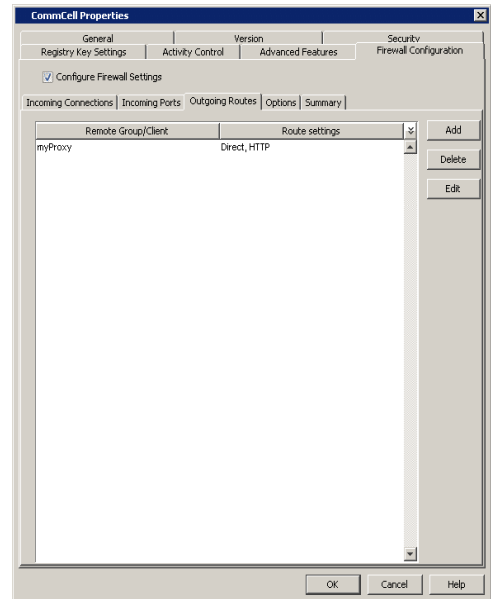


- 13.
- Select the Calypso proxy in **Remote Group/Client**.
 - Select **Direct**.
 - Click **OK**.

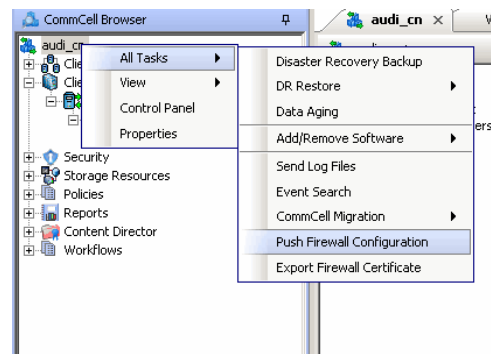


14. Click **OK**.

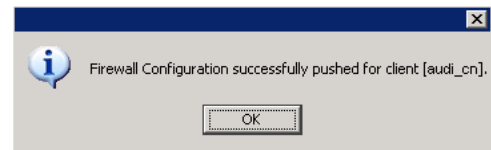
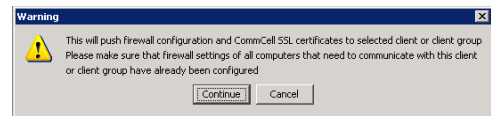
- From the CommCell Console right-click the CommServe computer, click **All Tasks**, and click **Push Firewall Configuration**.



- Click **Continue**.



- Click **OK**.
You are now ready to install the Calypso proxy.
Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.



INSTALL THE CALYPSO PROXY

Install a CommCell client (e.g., File System iDataAgent) in the DMZ. This will operate as the Calypso proxy. Since DMZ always receives connections from outside, the Calypso proxy in DMZ must communicate to the CommServe through tunnel connections initiated by the CommServe.

If firewall is enabled on the computer where the Calypso proxy will be installed, ensure there are open connections for the CommServe and client computers.

During the installation, use one of the following firewall configuration sequences:

- CommServe can reach the Client/MediaAgent (Windows clients)
- CommServe can reach the Client/MediaAgent (Unix clients)

After the installation is completed, open the CommCell Console, right-click the Calypso proxy computer and click **All Tasks | Push Firewall Configuration**.

INSTALL THE CLIENT

To install the client across the Calypso proxy, you will have to specify the path to reach the CommServe computer. The install program communicates to the CommServe using this information.

See Installation for step-by-step installation procedures to install the client. During installation, use one of the following firewall configuration sequences:

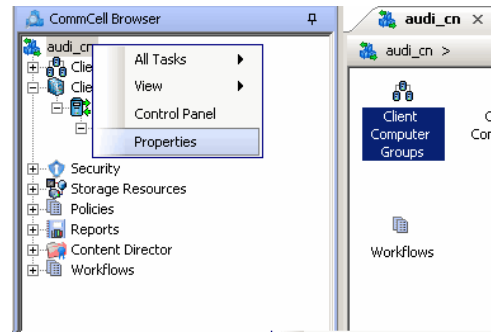
- CommServe can be Reached through a Proxy (Windows clients)

- CommServe can be Reached through a Proxy (Unix clients)

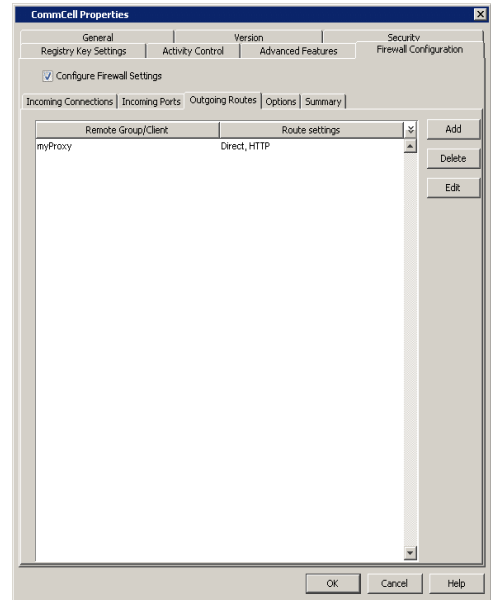
CONFIGURE THE COMMSERVE, MEDIAAGENT AND CLIENT

The following steps explain the actions required to configure routes between CommServe, MediaAgent and the new client through the Calypso proxy.

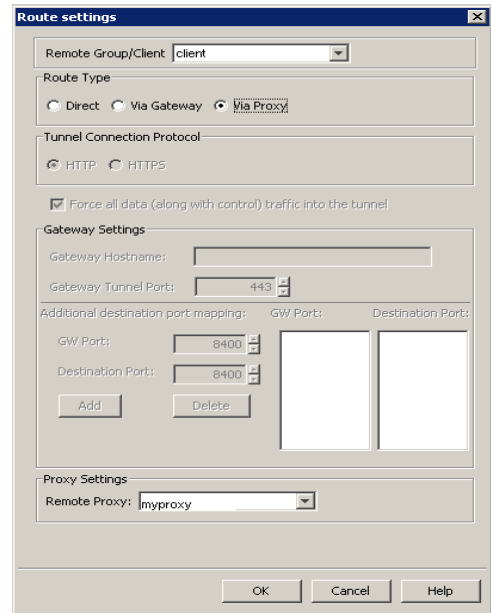
1. To configure the CommServe, right-click the CommServe computer from the CommCell Console and click **Properties**.



2.
 - Click the **Firewall Configuration** tab.
 - Click the **Outgoing Routes** tab.
 - Click **Add** to specify the outgoing connection route from the CommServe to the Client through the Calypso proxy.



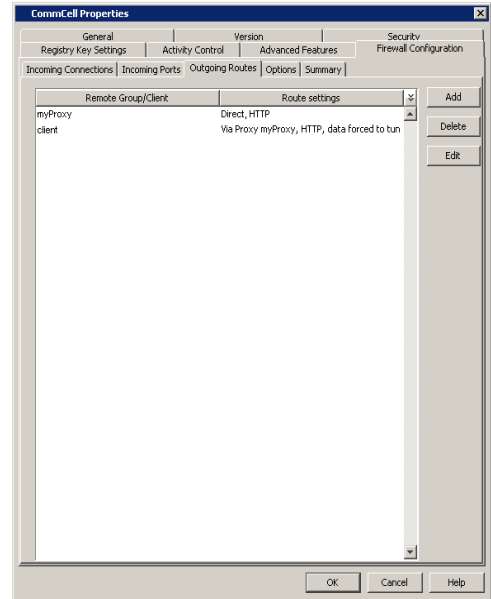
3.
 - Select the client computer in **Remote Group/Client**.
 - Select **Via Proxy**.
 - Select the Calypso proxy in **Remote Proxy**.
 - Click **OK**.



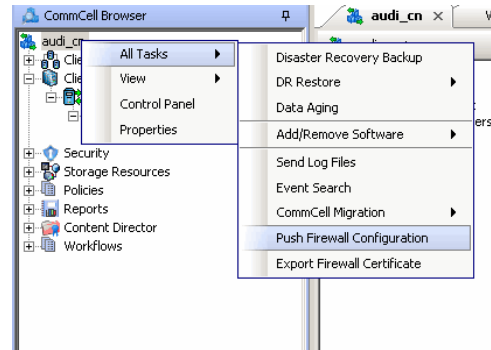
4. Click **OK**.

The **Outgoing Routes** tab should display two routes — the route from CommServe to the proxy and the route from CommServe to the client through the proxy.

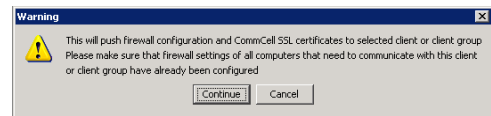
Note that when two computers are communicating with each other through a proxy, two routes need to be configured in each computer's Firewall preferences: one route to describe the connectivity of the computer with the proxy, and another route to describe the connectivity of the computer with the remote computer via proxy.



- From the CommCell Console, right-click the CommServe computer and click **All Tasks | Push Firewall Configuration**.

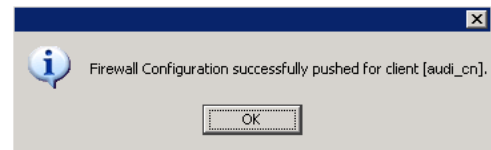


- Click **Continue**.



- Click **OK**.
The CommServe is configured to receive communication from the client through the Calypso proxy.

Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.



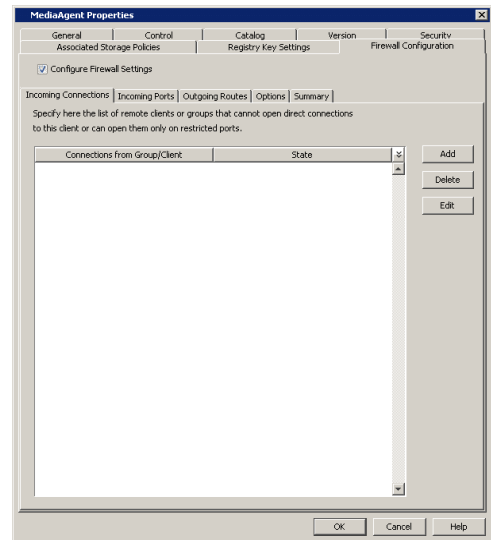
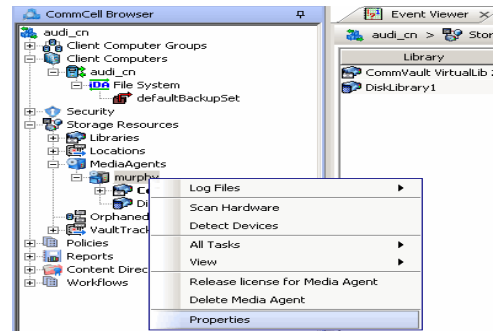
- From the CommCell Console, right-click the client computer and click **All Tasks | Check Readiness**. The results are displayed in **Client Connectivity** dialog box.

If the client computer is not ready, verify your settings with the above recommendations and revise the settings if required.

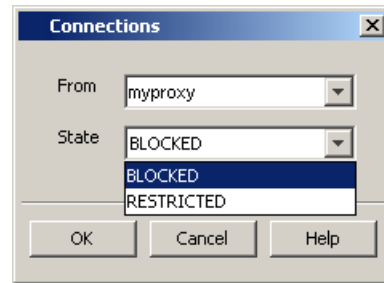


- To configure the MediaAgent, right-click the MediaAgent computer from the CommCell Console and click **Properties**.

- 10.
- Click the **Firewall Configuration** tab.
 - From the **Incoming Connections** tab, click **Add**.

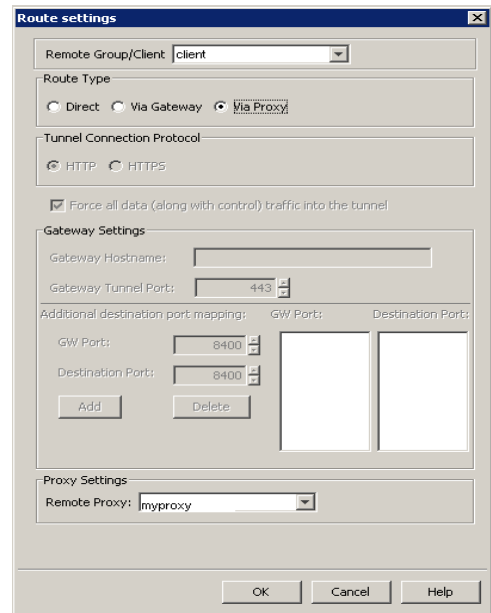
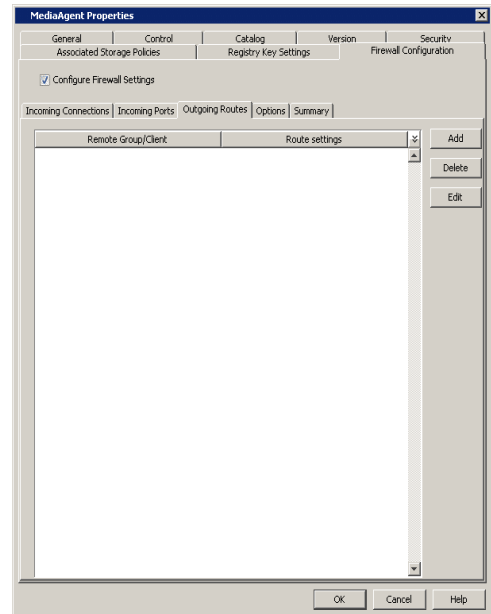


- 11.
- In the **From** field, select the Calypso proxy computer.
 - In the **State** field, select **Blocked**.
 - Click **OK**.

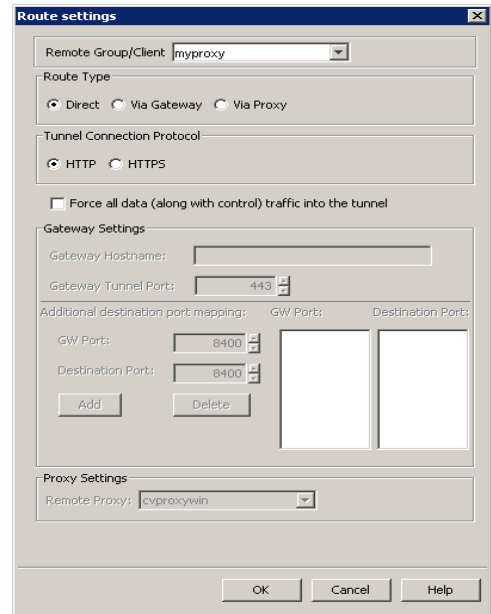


- 12.
- Click the **Outgoing Routes** tab.
 - Click **Add** to specify the outgoing connection route from the MediaAgent to the Client through the Calypso proxy.

- 13.
- Select the client computer in **Remote Group/Client**.
 - Select **Via Proxy**.
 - Select the Calypso proxy in **Remote Proxy**.
 - Click **OK**.



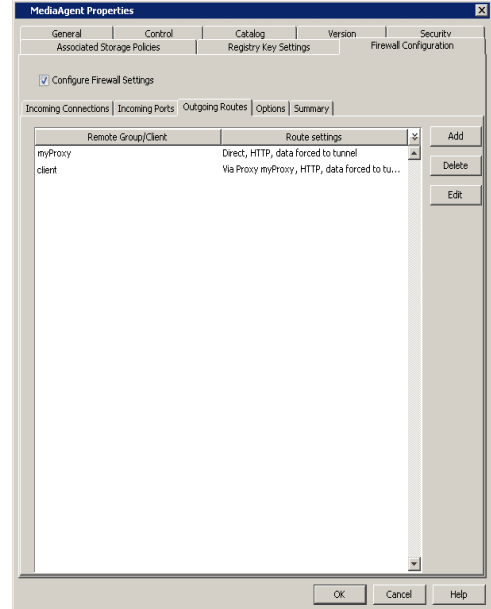
- 14.
- Click **Add** again to specify the route from MediaAgent to the Calypso proxy.
 - Select the name of the CommServe in **Remote Group/Client**.
 - Select **Force all data (along with the control) traffic into the tunnel**.
 - Click **OK**.



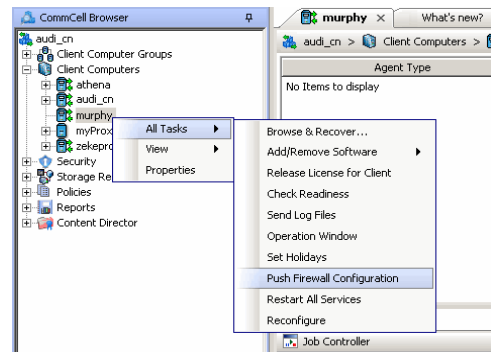
15. Click **OK**.

The **Outgoing Routes** tab must display two routes: the route from MediaAgent to the proxy and the route from MediaAgent to the client through the proxy.

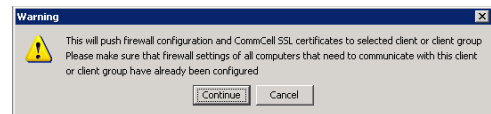
The MediaAgent is configured to receive communication from the client through the Calypso proxy.



16. From the CommCell Console, right-click the MediaAgent computer and click **All Tasks | Push Firewall Configuration**.



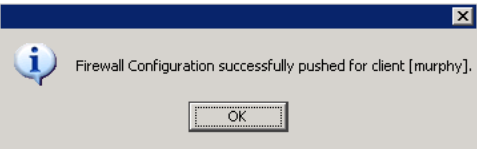
17. Click **Continue**.



18. Click **OK**.

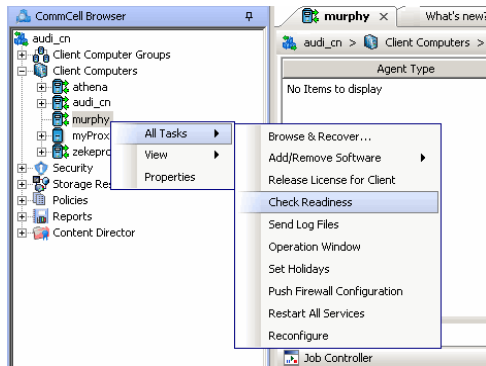
The MediaAgent is configured to receive communication from the client through the Calypso proxy.

Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.

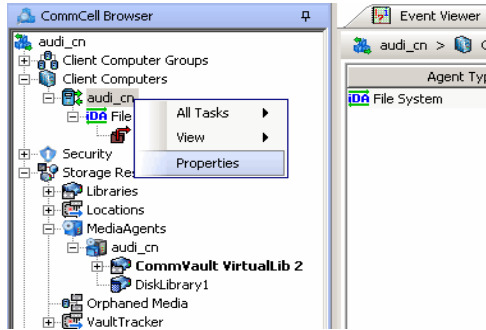


- 19. From the CommCell Console, right-click the MediaAgent computer and click **All Tasks | Check Readiness**. The results are displayed in **Client Connectivity** dialog box.

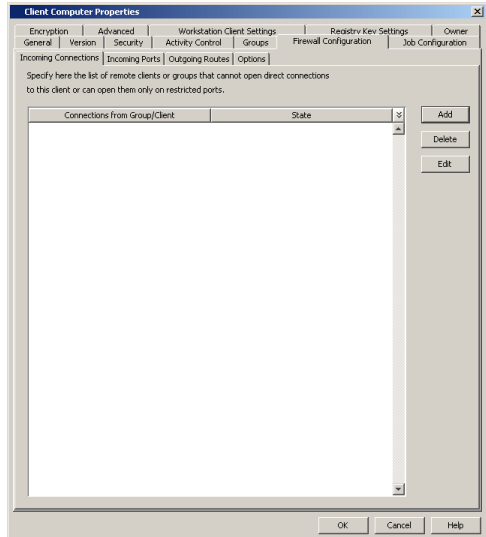
If the MediaAgent computer is not ready, verify your settings with the above recommendations and revise the settings if required.



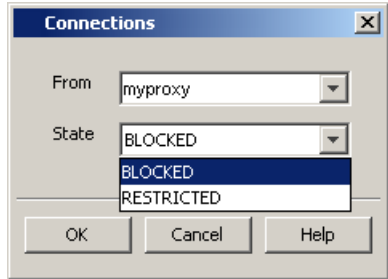
- 20. To configure the Client, right-click the client computer from the CommCell Console and click **Properties**.



- 21.
 - Click the **Firewall Configuration** tab.
 - From the **Incoming Connections** tab, click **Add**.

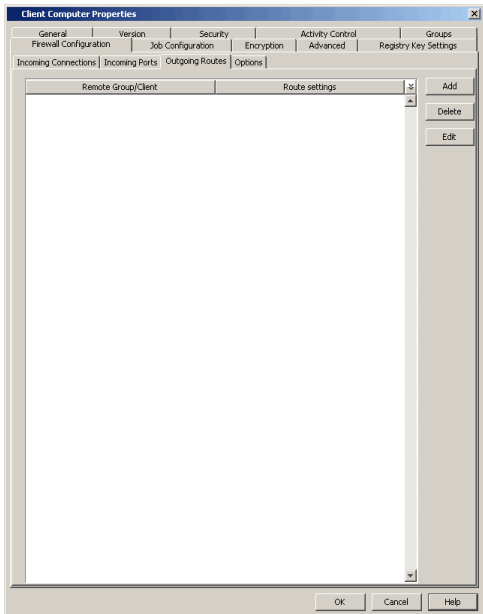


- 22.
 - In the **From** field, select the Calypso proxy computer.
 - In the **State** field, select **Blocked**. Since there are no incoming connections from the proxy to the client, the connection status is **Blocked**.
 - Click **OK**.



- 23.
 - Click the **Outgoing Routes** tab.

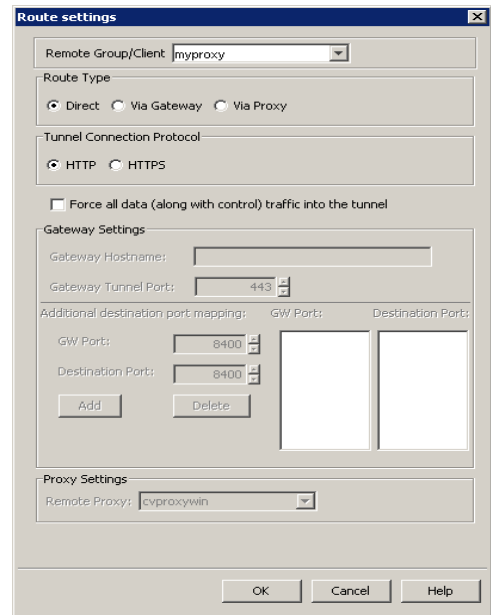
- Click **Add** to specify the route for outgoing connection from the client to the Calypso proxy.



- 24.
- Select the Calypso proxy in **Remote Group/Client**.
 - Select **Direct** for **Route Type**.

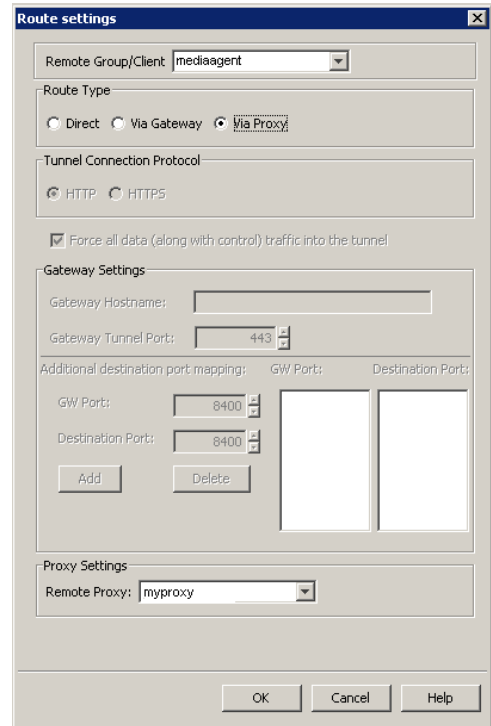
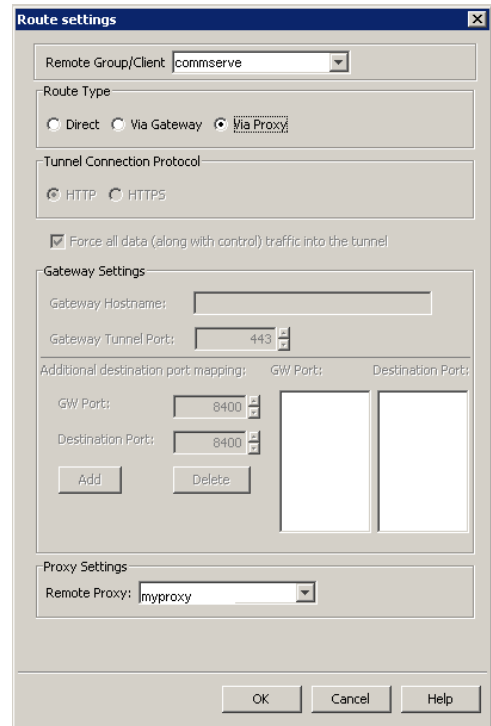
In case there is a port-forwarding gateway between the client and the Proxy, you will have to select **Via Gateway** and configure Gateway Settings.

- Select **Force all data (along with the control) traffic into the tunnel** to force the data traffic into the control tunnel. This automatically encrypts the data connection.
- Click **OK**.

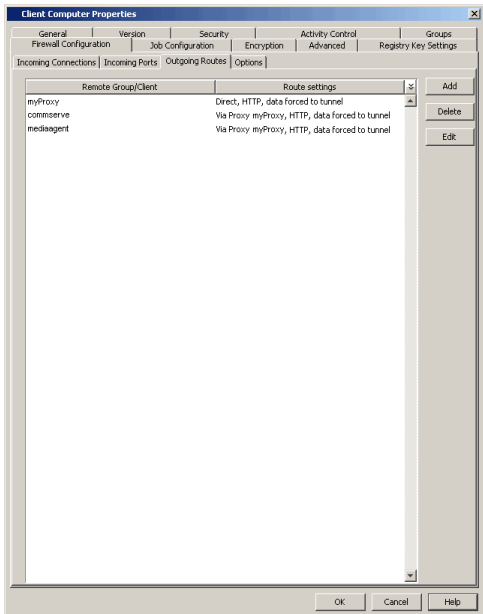


- 25.
- Click **Add** again to specify the route for outgoing connection from the client to the CommServe through the Calypso proxy.
 - Select the name of the CommServe in **Remote Group/Client**.
 - Select **Via Proxy**.
 - Select the Calypso proxy in **Remote Proxy**.
 - Click **OK**.

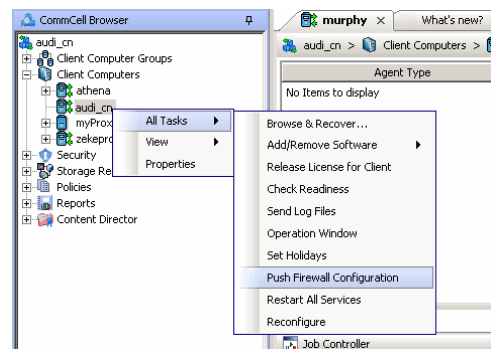
- 26.
- Click **Add** again to specify the route for outgoing connection from the client to the MediaAgent through the Calypso proxy.
 - Select the name of the MediaAgent in **Remote Group/Client**.
 - Select **Via Proxy**.
 - Select the Calypso proxy in **Remote Proxy**.
 - Click **OK**.



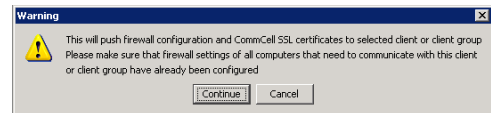
27. Click **OK**.
- The **Outgoing Routes** tab should display three routes: the routes from the client to the proxy, client to to the MediaAgent, and client to the CommServe.
- Please note that the image to the right assumes the route between the client and the proxy was configured using a **Direct** route. If you used a port-forwarding gateway, you will see **Via Gateway** as the route setting.



28. From the CommCell Console, right-click the client computer and click **All Tasks | Push Firewall Configuration**.



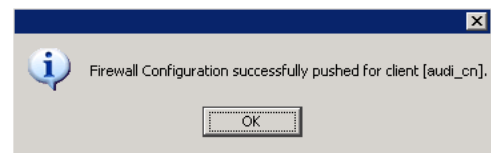
29. Click **Continue**.



30. Click **OK**.

The specified configurations are saved.

Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.



31. From the CommCell Console, right-click the client computer and click **All Tasks | Check Readiness**. The results are displayed in **Client Connectivity** dialog box.

If the client computer is not ready, verify your settings with the above recommendations and revise the settings if required.



Connectivity between the CommServe, MediaAgent, and the client through the Calypso proxy is established.

OPERATING USING PUBLIC WIFI CONNECTIONS

Consider the scenario where you are in a public location like a coffee shop, airport, hotel, or other such remote locations where internet access is using public WiFi through a HTTP proxy. If you are a roaming user who travels frequently, you might operate the software in this scenario. The following sections describe the configuration required to operate the software through HTTP proxy.

INSTALL THE CLIENT

We assume that your computer contains client components only. In most cases, the client software is already installed and ready for backup and recovery operations. You can however, install the software from behind a HTTP proxy. The following sections present the possible firewall scenarios that might protect the CommServe and the installer sequence to reach the CommServe in each scenario. Select the scenario that matches your deployment setup and follow the steps in sequence.

- Firewall Configuration - Windows
- Firewall Configuration - Unix

CONFIGURE THE CLIENT TO OPERATE ACROSS HTTP PROXY

To configure the client to operate across HTTP Proxy:

1. Locate the firewall configuration file `FWConfigLocal.txt` under `<software_installation>/Base` folder. This file contains the firewall configuration options provided during installation. Do not modify the `FWConfig.txt` file.

This file might not be available if the client software was installed within the internal network with no firewall separating the computer and the CommServe. In such case, contact your system administrator for details to create this file.

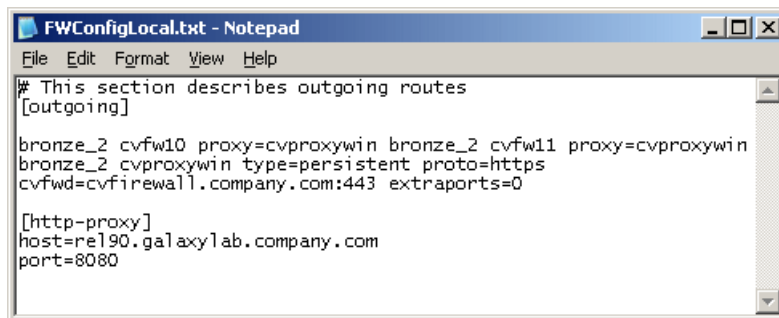
2. Locate the `[http-proxy]` section at the end of the file and remove the comment tag (`#`) from the section and its body. The section and its contents will appear as follows.

```
# [http-proxy]
# host= <host name of the proxy server>
# port= <HTTP proxy port number>
```

3. Provide the correct values for the host name and port number of the HTTP server. The software does not support HTTP proxies that require authentication.

If you are a roaming user frequently operating using public WiFi, you will have entries from your previous access. In such case, update the entries with the `host` and `port` information applicable to the current setup.

The following are sample entries for an outgoing route through HTTP Proxy.



```
FWConfigLocal.txt - Notepad
File Edit Format View Help
# This section describes outgoing routes
[outgoing]
bronze_2 cvfw10 proxy=cvproxywin bronze_2 cvfw11 proxy=cvproxywin
bronze_2 cvproxywin type=persistent proto=https
cvfwd=cvfirewall.company.com:443 extraports=0
[http-proxy]
host=re190.galaxy1ab.company.com
port=8080
```

CONFIGURING WINDOWS FIREWALL TO ALLOW COMMCELL COMMUNICATION

Windows Firewall, the built-in firewall included in Windows Operating Systems, can be configured to allow CommCell communication by adding CommCell programs and services to the Windows Firewall Exception list. Once the CommCell programs are added to the Exception list, the Windows Firewall will allow external network connections to the CommCell Console.

During installation of Windows components, the installer provides an option to add CommCell programs and services to Windows Firewall List. You can use this option to configure Windows Firewall during installation.

After installation, you can later configure Windows Firewall using `AddFWExclusions.bat` program. The `AddFWExclusions.bat` program should be run through the command prompt to prevent adding system32 executables to the firewall exception list as the default system environment variable may be triggered.

To add CommCell programs and services to Windows Firewall Exception List:

1. Open the command prompt.
2. Navigate to the `<Software_Installation_Path>/Base` folder.
3. Run the `AddFWExclusions.bat` file to execute the commands.

4. All applicable CommCell communication programs and services are added to Windows Firewall Exception List. Note that this must be done on all CommCell Computers.

If the firewall configuration is reset on a computer for any reason (this can happen, for example, when the computer is moved from a workgroup to a domain), then the firewall exclusions must be added again.

[Back To Top](#)

Install the CommServe Software

TABLE OF CONTENTS

Install Requirements

Install Procedure

- Cluster Selection
- Select Components for Installation
- Install Remaining Cluster Nodes
- Setup Complete

Post-Install Considerations

INSTALL REQUIREMENTS

The following procedure describes the steps involved in installing the CommServe on both clustered and non-clustered environment.

A Microsoft SQL Server 2008 database instance (Enterprise Edition) with the appropriate service pack will be automatically installed while installing the software.

Review the following Install Requirements before installing the software:

GENERAL

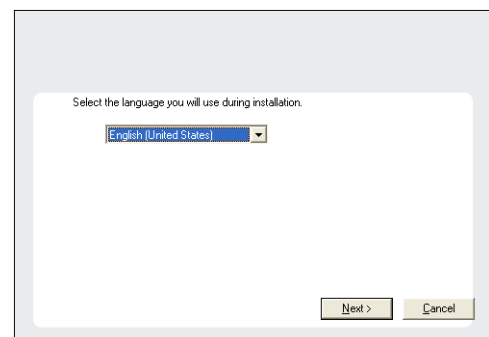
- Do not install the CommServe® on a computer that has Microsoft Exchange Server or an Oracle database.
- Make sure that you have the latest Software Installation Disc before you start to install the software. If you are not sure, contact your software provider.
- Close all applications and disable any programs that run automatically, including anti-virus, screen savers and operating system utilities. Some of the programs, including many anti-virus programs, may be running as a service. Stop and disable such services before you begin. You can re-enable them after the installation.

CLUSTER SPECIFIC

- In a clustered environment, Microsoft SQL Server 2008 (Enterprise Edition) with the appropriate service pack must be installed and clustered prior to installing the CommServe software. The CommServe software automatically uses the default or the named instance created during the SQL installation.
For more information, see Pre-Installing SQL Database for CommServe - Clustered Environment.
- SQL Server cannot be installed on a Cluster Quorum disk.

INSTALL PROCEDURE

1. Run **Setup.exe** from the **Software Installation Disc**.
2. Choose the language you want to use during installation. Click the down arrow and select the desired language from the drop-down list, and click **Next** to continue.

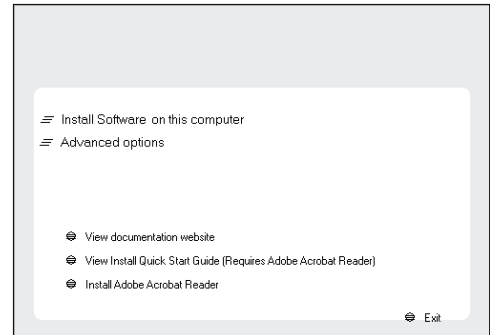


3. Select the option to install software on this computer.

NOTES

- The options that appear on this screen depend on the computer in which the software is being installed.

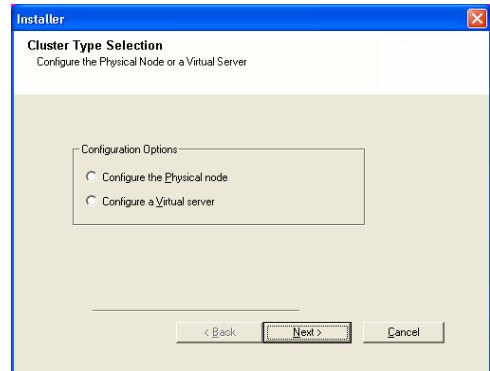
4. Select **I accept the terms in the license agreement**.
Click **Next**.



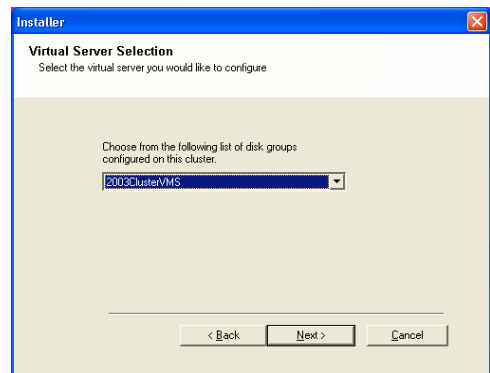
CLUSTER SELECTION

If you are installing in clustered environment, follow the steps below. For non-clustered environment, skip to Select Components for Installation.

5. Select **Configure a Virtual Server**.
Click **Next** to continue.



6. Select the disk group in which the cluster group resides.
Click **Next** to continue.



SELECT COMPONENTS FOR INSTALLATION

7. Select the following component(s) to install:
 - Expand **CommServe Modules** and click **CommServe**.
 - Clear **SRM Server**.

- Click **YES** to install Microsoft .NET Framework package.

NOTES

- This prompt is displayed only when Microsoft .NET Framework is not installed.
- Once the Microsoft .NET Framework is installed, the software automatically installs the Microsoft Visual J# 2.0 and Visual C++ redistributable package.

- Specify the SQL Server System Administrator password.

Click **Next**.

NOTES

- This is the password for the administrator's account created by SQL during the installation.

- Click **Yes** to set up a dedicated instance of Microsoft SQL Server for the CommServe Server.

- Verify the Installation Path for the Database Engine.

Click **Browse** to change the default location.

Click **Next**.

NOTES

- This is the location where you want to setup the Microsoft SQL Server System databases.
- If you plan to perform VSS enabled backups on the CommServe computer, it is recommended that the CommServe database is not installed on the system drive. VSS restores could cause system state restore issues.
- The install program installs the database instance.

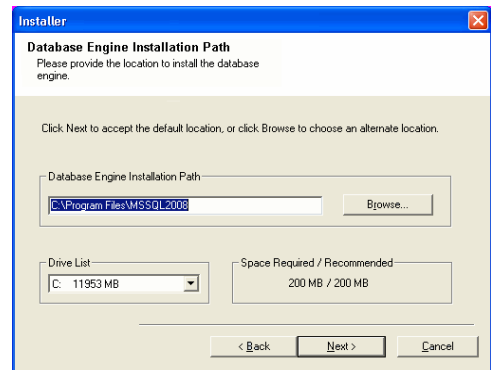
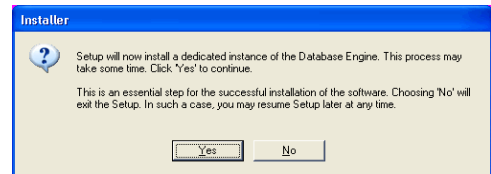
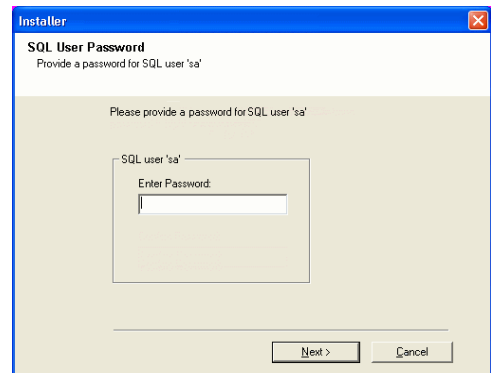
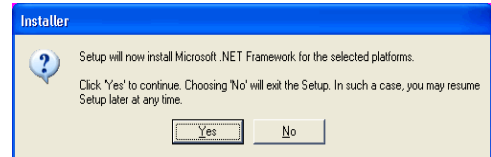
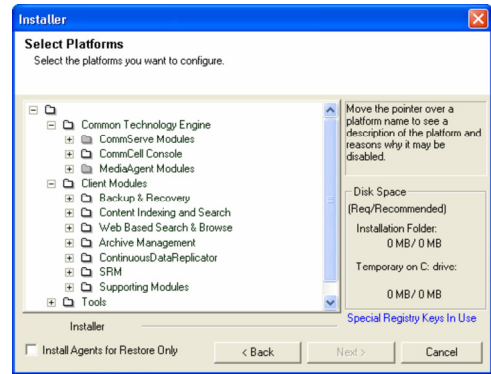
- Verify **MSSQL Database Installation Path**.

Click **Browse** to change the default location.

Click **Next**.

NOTES

- This is the location where you want to install Microsoft SQL Server.
- This step may take several minutes to complete.



13. If this message is displayed, click **Reboot Now** to continue. The install program will automatically resume from the point of failure after the reboot.

If the install program does not automatically resume after the reboot:

- Click the **Start** button on the Windows task bar, and then click **Run**.
- Browse to the installation disc drive, select **Setup.exe**, click **Open**, then click **OK**.

NOTES

- Click the **Skip Reboot** option if it is displayed and continue with the installation. You can reboot at a later time if the option is displayed.

14. Click **Next**.

NOTES

The **CommServe Client Name** and **CommServe Host Name** are automatically populated.

15. Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.

Click **Next**.

This option enables CommCell operations across Windows firewall by adding CommCell programs and services to Windows firewall exclusion list.

It is recommended to select this option even if Windows firewall is disabled. This will allow the CommCell programs and services to function if the Windows firewall is enabled at a later time.

16. Verify the default location for software installation.

Click **Browse** to change the default location.

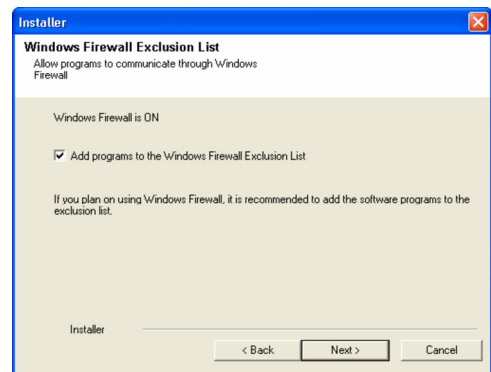
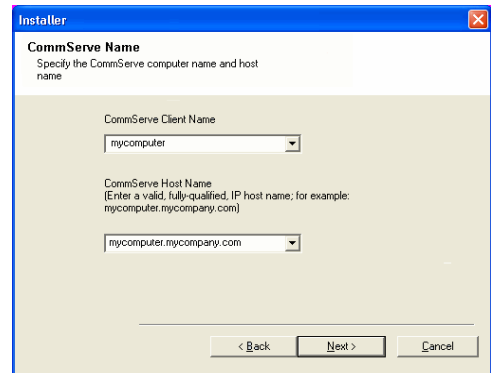
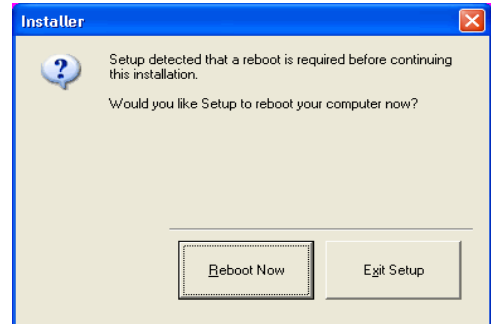
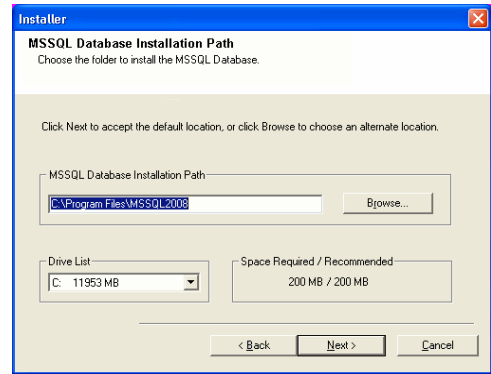
Click **Next**.

NOTES

- Do not install the software to a mapped network drive.
- Do not use the following characters when specifying the destination path:

/ : * ? " < > | #

It is recommended that you use alphanumeric characters only.



17. Verify the location of the database.
Click **Browse** to change the default location.
Click **Next**.

NOTES

- Do not specify a mapped network drive.
- Ensure that the drive has at least 1GB of free space.
- The directory file path selected should not be located on a FAT drive. A FAT drive cannot be supported as the location for this database because it does not allow a temporary sparse file to be generated when creating the database snapshot, which is required for data verification.

18. Select the **Create a New Database** option and click **Next** to continue.

NOTES

- This screen may look different from the example shown.

19. Enter the network or local path where Disaster Recovery Backup files should be stored.

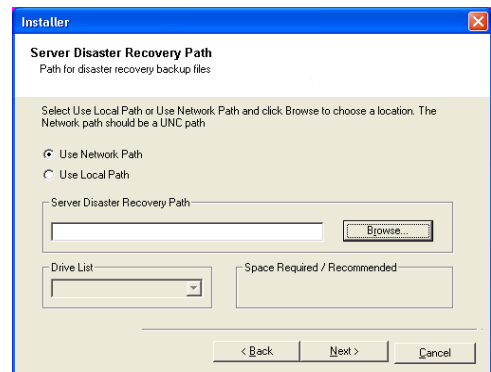
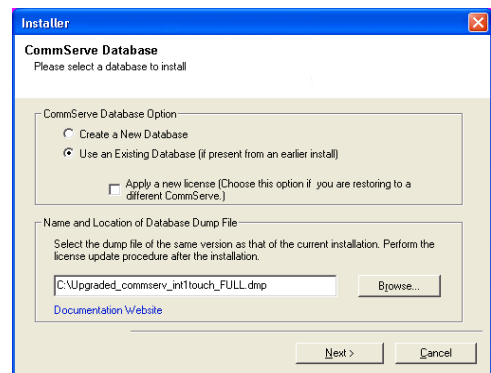
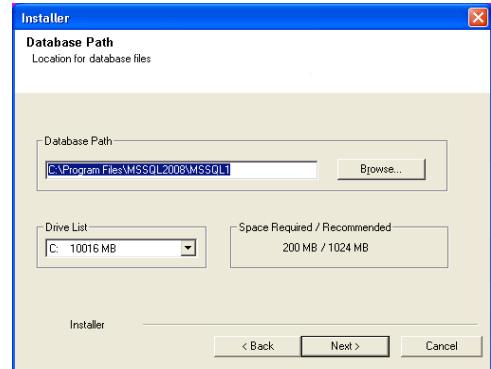
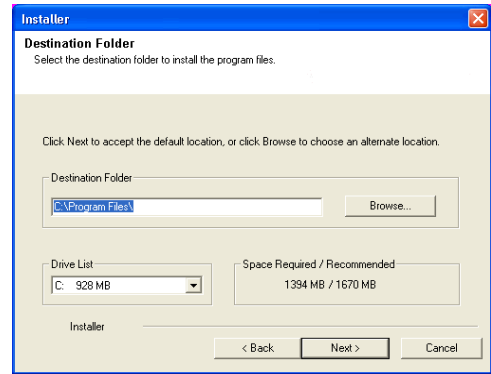
Click **Next**.

NOTES

- If you selected **Use Network Path**, you must enter the **Network share username** and the **Network share password**.
 - The Network share username is the domain\username of the user that has administrative rights to the Disaster Recovery Backup destination path.
 - The Network share password is the password of the network share username.

20. Enter the **CommCell Username** and **CommCell Password**.

Click **Next**.



21. Select **Setup Software Cache** option to download the software updates automatically.
 Select **Schedule FTP Download of Automatic Updates** option to schedule automatic FTP downloading of software updates.
 Click **Next**.

22. Specify the path where the update files from the FTP site should be stored.
 Click **Next**.

NOTES

- This prompt will be displayed if the **Setup Software Cache** option was enabled.

23. Click **Next**.

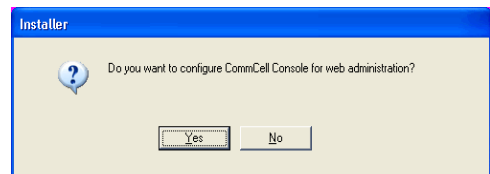
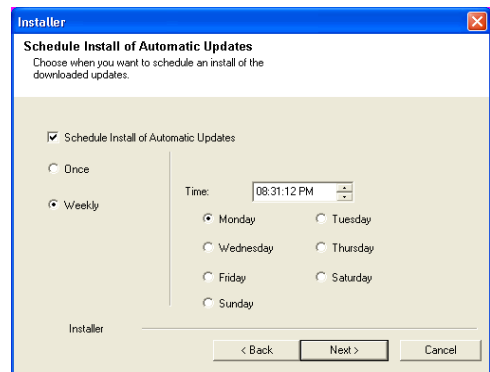
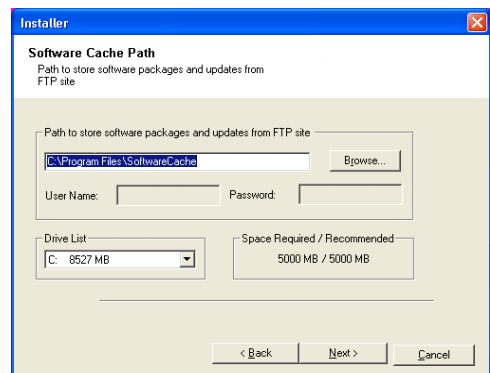
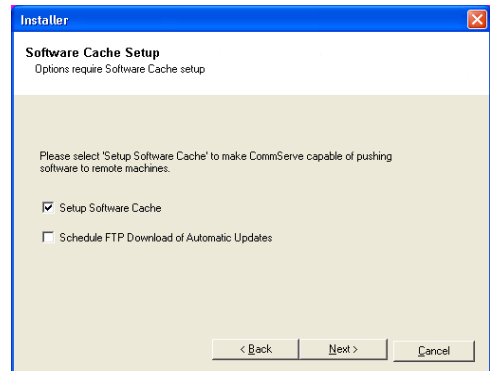
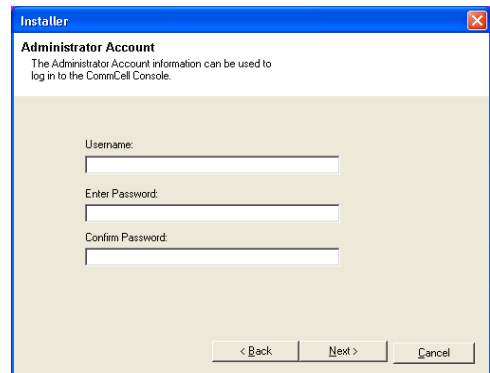
NOTES

- Schedule Install of Automatic Updates allows automatic installation of the necessary software updates on the computer on a single or weekly basis. If you do not select this option, you can schedule these updates later from the CommCell Console.

24. Click **Yes** to configure the CommCell Console for web administration, or Click **No** to continue without configuring the CommCell Console for web administration.

NOTES

- The Internet Information Server (IIS) must be installed on this computer in order to configure for web administration.
- Configuring this computer for web administration allows you to:
 - Access the CommCell Console and Books Online from a remote computer using a Web browser.
 - View CommCell reports via a Web browser.

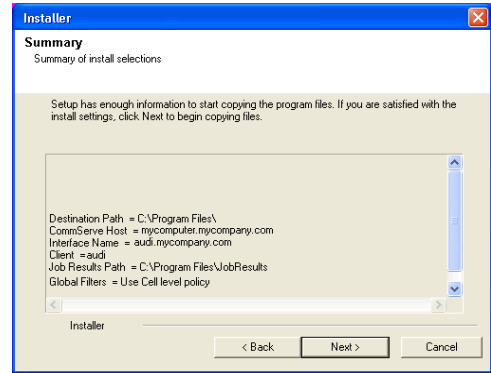


- o Access Books Online by clicking the Help button (the icon with a ?) in the CommCell Console.

25. Click **Next**.

NOTES

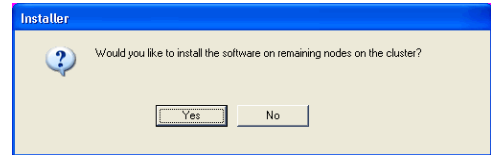
- The install program now starts copying the software to the computer. This step may take several minutes to complete.



INSTALL REMAINING CLUSTER NODES

If you are installing in clustered environment, follow the steps below to install on remaining nodes of the cluster. For non-clustered environment, skip to Setup Complete.

26. To install/upgrade the software on the remaining nodes of the cluster, click **Yes**.
To complete the install for this node only, click **No**.

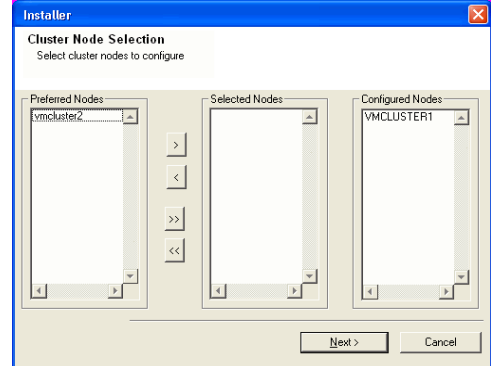


27. Select cluster nodes from the **Preferred Nodes** list and click the arrow button to move them to the **Selected Nodes** list.

NOTES

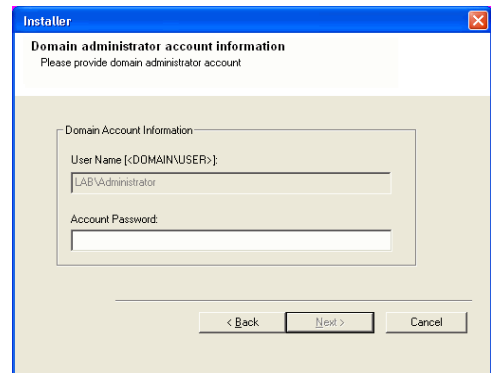
- The list of **Preferred Nodes** displays all the nodes found in the cluster; from this list you should only select cluster nodes configured to host this cluster group server.
- Do not select nodes that already have multiple instances installed. For more information, see Multi Instancing.

When you have completed your selections, click **Next** to continue.



28. Type the **User Name** and **Password** for the Domain Administrator account, so that the installer can perform the remote install/upgrade of the cluster nodes you selected in the previous step.

Click **Next** to continue.



29. The progress of the remote install for the cluster nodes is displayed; the install can be interrupted if necessary.

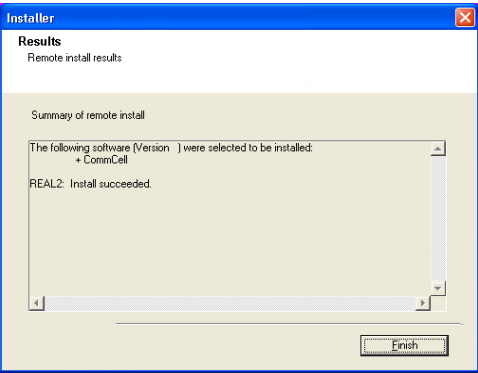
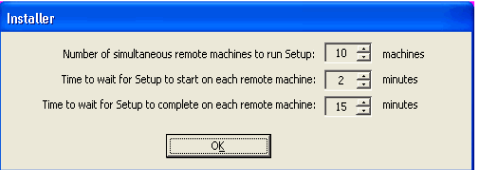
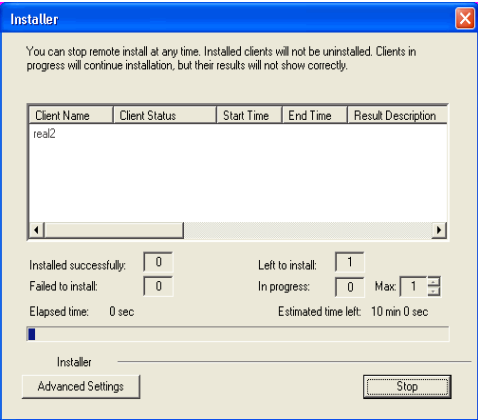
Click **Stop** to prevent installation to any nodes after the current ones complete.

Click **Advanced Settings** to specify any of the following:

- Maximum number of nodes on which Setup can run simultaneously.
- Time allocated for Setup to begin executing on each node, after which the install attempt will fail.
- Time allocated for Setup to complete on each node, after which the install attempt will fail.

NOTES

- If, during the remote install of a cluster node, setup fails to complete or is interrupted, you must perform a local install on that node. When you do, the install begins from where it left off, or from the beginning if necessary. For procedures, see Manually Installing the Software on a Passive Node.



30. Read the summary for remote installation to verify that all selected nodes were installed successfully.

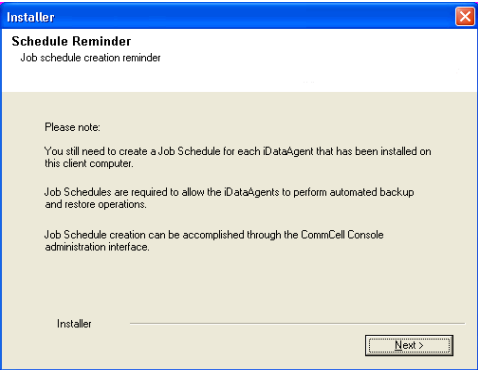
NOTES

- If any node installation fails, you must manually install the software on that node once the current installation is complete. (See Manually Installing the Software on a Passive Node for step-by-step instructions.)
- The message displayed on your screen will reflect the status of the selected nodes, and may look different from the example.

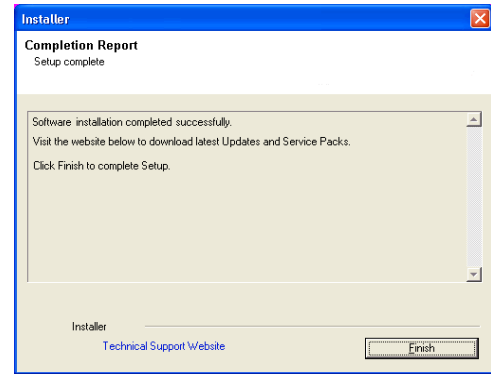
Click **Next** to continue.

SETUP COMPLETE

31. Click **Next**.



32. Click **Finish**.



33. Proceed as follows, based on your installation configuration:

- If you installed both the CommServe software and the CommServe database in the cluster group:
 - a. If the passive node was not available while installing the software, you must manually install the software on the passive node now. (See [Manually Installing the Software on a Passive Node](#) for step-by-step instructions.)
 - b. Fail over the disk group containing the CommServe to the passive nodes at least once, so that the configurations to the passive node occur. This must be done before installing any other software components. The install program updates the passive nodes on the cluster so that the virtual server can fail over. A program to create the CommServe Data Source Name (DSN) is launched automatically on each passive node.
 - c. Fail back the nodes, then continue on to the MediaAgent installation.
 - d. You must install the CommCell Console on a physical node of the cluster before proceeding. For instructions, see [Install the CommCell Console - Windows](#).
- If you installed the CommServe software on the active physical node, and the SQL database resides in the cluster group, you must now install the CommServe software on every passive node as well. For step-by-step instructions, see [Manually Installing the Software on a Passive Node](#).

POST-INSTALL CONSIDERATIONS

GENERAL

- Review Install Considerations after installing the software.
- Install post-release updates or Service Packs that may have been released after the release of the software. Alternatively, you can enable Automatic Updates for quick and easy installation of updates in the CommCell® console.

[Back to Top](#)

Install the CommServe and Database Engine on Separate Computers

TABLE OF CONTENTS

Overview

Setup CommServe Computer

Setup SQL Server Computer

Moving the Database

Setting up the SQL Server Account

Changing DSN Settings

Protecting the Database - Setting up the Disaster Recovery Backup

Restoring the Database

Installing Updates

Uninstalling Updates

OVERVIEW

The CommServe and the Microsoft SQL Server Database Engine can be installed on separate computers.

The following procedure describes the steps involved in building such a topology. Note that these procedures require familiarity and understanding of both the Microsoft SQL Server Database Engine and the Windows operating system.

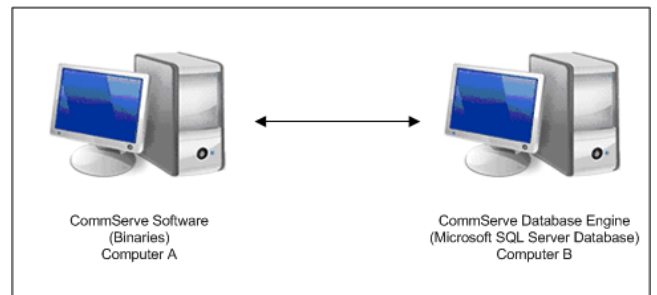
This procedure can be used when you initially install the software, or when you split an existing CommServe.

The following are not supported in this configuration:

- CommServe Name Change
- CommServe Disaster Recovery Tool (For disaster recovery procedures in this configuration, See Setting up the Disaster Recovery Backup and Restoring the Database)

The setup requires the following:

- CommServe software to be installed on CommServe and SQL Server computers. This installation will automatically install SQL Server software.
- A reliable and fast network connection between these two computers.



SETUP COMMSERVE COMPUTER

1. Install the CommServe software on the computer that will host the CommServe.
2. Verify that no jobs are in progress or scheduled to occur while setting up this configuration.
If jobs are in progress or other tasks (such as reports or updates) are scheduled, either perform this task at another time or disable all activity or disable all scheduled tasks from the CommCell Console.
3. Stop all services on the CommServe computer.

See Install the CommServe for step-by-step instructions.

To disable activity control:

1. From the CommCell Browser, right-click the **CommServe** and then click **Properties**.
2. Click **Activity Control** tab.
3. Clear **Enable All Job Activity** and **Enable Scheduler** box.
4. Click **OK**.

To stop services:

1. Click the **Start** button on the Windows task bar and then click **All Programs**.
2. Navigate to **bull | Calypso** and click **Service Control Manager**.
3. Select **All Services** in **Services**.
4. Click **Stop** to stop all services.

SETUP SQL SERVER COMPUTER

4. Install the CommServe software on the SQL Server computer. This installation will automatically install SQL Server software.

See Install the CommServe for step-by-step instructions.

See System Requirements - CommServe for more information on the SQL Server

version.

5. Stop all services on the SQL Server computer.
Note that the CommServe Services must be disabled permanently.

MOVING THE DATABASE

6. In the CommServe computer, using the **SQL Server Management Studio**, backup the **CommServ** database and create a .dmp file.

7. Copy the backup dump (.dmp) file created in **Step 4** to SQL Server Computer using any of the following method:
 - Using a physical media
 - Using a network drive that is accessible from both the Servers

8. In the SQL Server computer, using the **SQL Server Management Studio**, restore the **CommServ** database.

To stop services:

1. Click the **Start** button on the Windows task bar and then click **All Programs**.
2. Navigate to **bull | Calypso** and click **Service Control Manager**.
3. Select **All Services** in **Services**.
4. Click **Stop** to stop all services.

Perform the following steps to back up the CommServe database to a full database backup:

1. Open **Microsoft SQL Server Management Studio**.
2. Navigate to **Server Instance | Database | CommServ**.
3. Right-click the **CommServ** database, select **Tasks** and then click **Backup**. The **Back Up Database** dialog box appears.
4. In the **Database**, verify the database name.
5. In the **Backup type**, select **Full**.
6. In the **Backup Component**, select **Database** option.
7. Accept the default backup set name in the **Name**, or you can enter a different name for the backup set.
8. Specify when the **Backup set will expire**. By default **After** is selected with value **0**.
9. In the **Destination** area select **Disk** option. To select the path, click **Add**. The selected path will be displayed in the **Backup to** list.
10. To remove backup destination, select the destination path and click **Remove**.
11. Click **OK**.

Perform the following steps to restore the full database to the SQL Server computer:

1. Open **Microsoft SQL Server Management Studio**.
2. Navigate to **Server Instance | Database**.
3. Right-click **Database**, select **Restore Database**. The **Restore Database** dialog box appears.
4. On the **General** page, do the following:
 - In the **To Database**, select or type the name of a database.
 - To specify the source and location of the backup sets to restore, select **From device** option.
Click the **Browse** button, **Backup dialog box** appears.
In the **Backup media**, select one of the device type.
Click **Add** to provide the path of dump file copied in the previous step. Click **OK**.
5. On the **Options** page, do the following:
 - In the **Restore options**, choose any of the options, appropriate for your situation.
 - The **Recovery state** determines the state of the database after the restore operation.
Choose **Leave the database non-operational, and do not roll back the uncommitted transactions. Additional transaction logs can be restored. (RESTORE WITH NORECOVERY)** option.

9. Run the following query from SQL Management Studio on SQL Server Computer:

Usage:

```
exec CommServ..executeCSSetupScripts '<path>'
```

Example

```
exec CommServ..executeCSSetupScripts 'C:\Program Files\Bull  
Calypso\Calypso\'
```

Where

<path> - This is the path of CommServe Installation Directory on SQL Server Computer.

6. Click **OK**.

SETTING UP THE SQL SERVER ACCOUNT

10. On the CommServe computer, from the **Registry Editor**, edit the following values to point to SQL Server Computer:

- **sCONNECTION**
- **sDOMAIN**
- **sINSTANCE**

To open and edit the registry key:

1. From **Taskbar**, click **Start**, and then click **Run**.
2. Type **regedit**, and then click **OK**.
3. Navigate to the following key:

**HKEY_LOCAL_MACHINE\SOFTWARE\CommVault
Systems\Galaxy\Instance<xxx>\Database**

4. Edit the following values:
 - **sCONNECTION** set it to *<SQL Server computer>_commserv*
 - **sDOMAIN** set it to *<SQL Server computer>*
 - **sINSTANCE** set it to *<SQL Server computer>\BullCalypso*

CHANGING DSN SETTINGS

11. On the CommServe computer, modify the DSN Settings for the CommServe database to point to the database in the SQL Server computer.

1. Open **Control Panel | Administrative Tools | Data Sources (ODBC)**.
2. Click the **System DSN** tab.
3. Click **<CommServe computer>_commserv** and then click **Configure**.
4. Edit the following values:
 - Name** - set it to *<SQL Server computer>_commserv*
 - Server** - set it to *<SQL Server computer>\BullCalypso*
5. Click **Next**.
6. Choose the **With SQL Server authentication using a login ID and password entered by the user** option.
7. Select the **Connect to SQL Server to obtain default settings for the additional configuration options** check box and enter the login and password of the *sa* user in the SQL Server computer.
8. Click **Next** twice and then click **Finish**. (Nothing needs to be changed on these dialog boxes.)
9. Click **Test Data Source**.

The result should be **TEST COMPLETED SUCCESSFULLY**.

If not make sure SQL server on the SQL Server computer is accessible and the login information given are correct.

10. Click **OK**.

To start the services:

1. Click the **Start** button on the Windows task bar and then click **All Programs**.
2. Navigate to **bull | Calypso** and click **Service Control Manager**.
3. Select **All Services** in **Services**.

12. Restart the services on the CommServe computer and re-enable jobs that were disabled.

4. Click **Start** to start all services.

To enable activity control:

1. From the CommCell Browser, right-click the **CommServe** and then click **Properties**.
2. Click **Activity Control** tab.
3. Select **Enable All Job Activity** and **Enable Scheduler** box.
4. Click **OK**.

PROTECTING THE DATABASE - SETTING UP THE DISASTER RECOVERY BACKUP

As Disaster Recovery Backup will not work in this setup, use the following steps to protect the database:

13. Disable the Disaster Recovery Backup schedule.

Use the following steps to disable a schedule:

1. From the CommCell Browser, right-click the **<CommServe>**, point to **View** and then click **Schedules**.
2. Select and right-click the **DR Backup Full** schedule in the right pane and click **Disable**.
3. Click **Yes** to disable the schedule.

14. Install the File System *iDataAgent* on the SQL Server computer.

See Getting Started - Windows File System Deployment for more information.

15. Using the File System *iDataAgent*, create a subclient which includes a script in the pre-scan phase to create a **.dmp** file of the **CommServ** database. Schedule regular backups of this subclient database from file system *iDataAgent*.

Recommended schedule is a daily full backup.

Use the following command line in a batch file and attach the batch file as a PreBackup Process:

```
<sql install path>\Isql.exe -S <SQL ServerName> -U
sa -P <sapwd> -q "BACKUP DATABASE [CommServ] TO DISK
= 'C:\cs.dmp'"
```

This should create a dump file c:\cs.dmp.

You can choose the folder in which the .dmp file is created.

16. If you want a copy of the dump in a disk library (similar to Disaster Recovery Backup) copy the dump file to another location. This can be included in the post-backup phase.

RESTORING THE DATABASE

17. If you wish to recover the database, restore the dump file using the File System *iDataAgent* on the SQL Server computer and then recover the database using the **SQL Server Management Studio**.

INSTALLING UPDATES

Use the following steps to install updates on CommServe and SQL Server computers:

Perform the following steps to install updates on SQL Server computer:

1. Services on SQL Server computer are already disabled.
2. Navigate to the **<Service Pack>** directory.
3. Execute the following command:

```
InstallUpdates.exe -doNotUpdateDB -nostartsvc -silent -vm
Instance001
```

Perform the following steps to install updates on CommServe computer:

1. Stop all services on the CommServe computer.
2. Navigate to the **<Service Pack>** directory.
3. Execute the following command:

```
InstallUpdates.exe -nostartsvc -silent -vm Instance001
```
4. If **PendingDBOperation** registry key is available at the following location on CommServe computer, then delete the key.

```
HKEY_LOCAL_MACHINE\SOFTWARE\CommVault Systems\Galaxy\UpdateFlags\
```
5. Start all the services on the CommServe computer.

UNINSTALLING UPDATES

Use the following steps to uninstall updates on Commserve and SQL Server computers:

Perform the following steps to install updates on CommServe computer:

1. Stop all services on the CommServe computer.
2. Navigate to the `Base` directory.
3. Execute the following command:

```
Removeupdates.exe -silent -nostartsvc -vm Instance001 -undo bin
```
4. If `PendingDBOperation` registry key is available at the following location on the CommServe computer, then delete the key.

```
HKEY_LOCAL_MACHINE\SOFTWARE\CommVault Systems\Galaxy\UpdateFlags\
```
5. Start all the services on the CommServe computer.

Perform the following steps to install updates on SQL Server computer:

1. Services on SQL Server computer are already disabled.
2. Navigate to the `Base` directory.
3. Execute the following command:

```
Removeupdates.exe -silent -nostartsvc -vm Instance001 -donotupdatedb
```

Install/Upgrade the CommServe With an Existing Database - How To

Topics | **How To**

TABLE OF CONTENTS

Install Requirements

Before You Begin

Install Procedure

- Getting Started
- Select Components for Installation
- Set Up the Required Privileges
- Set Up the Microsoft SQL Server Instance
- Select CommServe Database
- Set User Names and Passwords
- Configure the CommCell for Web-Based Administration
- Schedule Automatic Update
- Verify Summary of Install Options
- Remove the Required Privileges
- Setup Complete

Post-Install Considerations

INSTALL REQUIREMENTS

When installing the CommCell® components, you always install the CommServe® software first. The CommServe Server communicates with all clients and MediaAgents and coordinates operations (backups, restores, copies, migration, media management, etc.) within a CommCell.

If you are upgrading from a previous release, use the **Database Upgrade** tool to upgrade the database to the current release. See Install Database Upgrade - Tool for more information. Obtain the CommServe database dump after the upgrade.

Verify that the computer in which you wish to install the software satisfies the minimum requirements specified in System Requirements - CommServe.

This procedure describes the steps involved in installing CommServe with an existing upgraded CommServe database.

If you choose to install additional components simultaneously, refer to the appropriate procedures for installation requirements and steps specific to the component. Note that when you install multiple components, the sequence of the install steps may vary.

Review the following Install Requirements before installing the software:

GENERAL

- Do not install the CommServe® software on a compressed drive.
- Close all applications and disable any programs that run automatically, including anti-virus, screen savers and operating system utilities. Some of the programs, including many anti-virus programs, may be running as a service. Stop and disable such services before you begin. You can re-enable them after the installation.
- Do not install the CommServe® on a computer that has Microsoft Exchange Server or an Oracle database.
- Verify that you have the software installation disc that is appropriate to the destination computer's operating system. Make sure that you have the latest software installation disc before you start to install the software. If you are not sure, contact your software provider.

NETWORK

- If your CommServe® computer has multiple Network Interface Cards and IP addresses, make certain that all network communication paths are working. Also, make sure that the network interface to be used in the CommServe installation is set as the first one to be bound to the network. For more information on Network Interface Cards, see the Network Requirements.

TERMINAL SERVICES

- When installing CommCell components using Terminal Services, you must specify a UNC path to the installer. When using a UNC path to install the CommServe, SQL must already be installed and the database instance must already be configured.

BEFORE YOU BEGIN

- Log on to the client as local Administrator or as a member of the Administrators group on that computer.

INSTALL PROCEDURE

GETTING STARTED

1. Place the Software Installation Disc for the Windows platform into the disc drive.

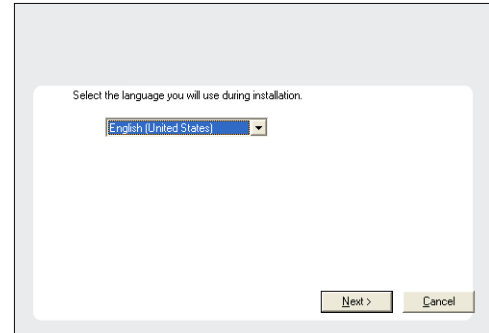
After a few seconds, the installation program is launched.

If the installation program does not launch automatically:

- Click the **Start** button on the Windows task bar, and then click **Run**.
- Browse to the installation disc drive, select **Setup.exe**, click **Open**, then click **OK**.

NOTES

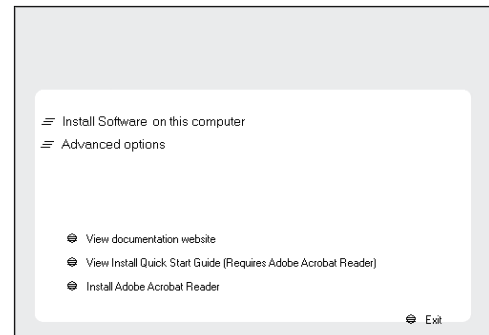
- If you are installing on Windows Server Core editions, mount to Software Installation Disc through command line, go to the **AMD64** folder and run **Setup.exe**.
2. Choose the language you want to use during installation. Click the down arrow and select the desired language from the drop-down list, and click **Next** to continue.



3. Select the option to install software on this computer.

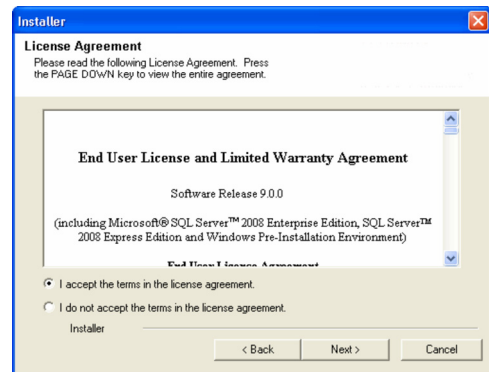
NOTES

- The options that appear on this screen depend on the computer in which the software is being installed.



4. Read the license agreement, then select **I accept the terms in the license agreement**.

Click **Next** to continue.



SELECT COMPONENTS FOR INSTALLATION

5. Select the component(s) to install.

NOTES

- Your screen may look different from the example shown.
- Components that either have already been installed, or which cannot be installed, will be dimmed. Hover over the component for additional details.
- If you wish to install the agent software for restore only, select **Install Agents for Restore Only** checkbox. See Installing Restore Only Agents for more information.
- The **Special Registry Keys In Use** field will be highlighted when `GalaxyInstallerFlags` registry key is enabled. Move the mouse pointer over this

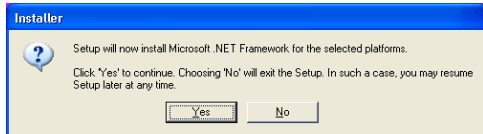
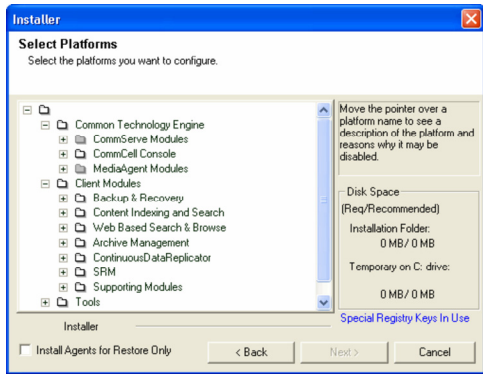
field to see a list of registry keys that have been created in this computer.

Click **Next** to continue.

To install the CommServe software from the **Common Technology Engine** folder expand the **CommServe Modules** folder and select the following:

- CommServe

The **CommCell Console** and **Java Runtime Environment** will be selected by default. **CommCell Console** and **Java Runtime Environment** is located in the **CommCell Console** folder.



6. Click **YES** to install Microsoft .NET Framework package.

NOTES

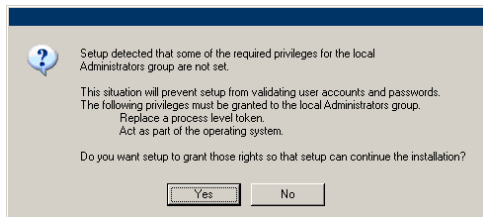
- Follow the on-screen prompts for installing the Microsoft .NET Framework package.
- If you are prompted to install the Service Pack for the Microsoft .NET Framework, click **Yes**.
- This prompt is displayed only when Microsoft .NET Framework is not installed.
- Once the Microsoft .NET Framework is installed, the software automatically installs the Microsoft Visual J# 2.0 package.

SET UP THE REQUIRED PRIVILEGES

7. Click **Yes** to set up the required privileges for the local administrators group.

NOTES

- This option will only appear if the Windows user account used to install the software does not have the required administrator rights (e.g., if the operating system was newly installed).
- If you choose to click **Yes**, the install program will automatically assign the required rights to your account. You may be prompted to log off and log back on to continue the installation.
- If you choose to click **No**, the installation will be aborted.
- You will be prompted at the end of the installation to decide if you want these privileges to be revoked.



The install program checks your Windows user account for the following necessary operating system rights:

- Right to increase quotas (this is referred to as adjust memory quotas for a process on Windows Server 2003).
- Right to act as a part of the operating system.
- Right to replace a process level token.

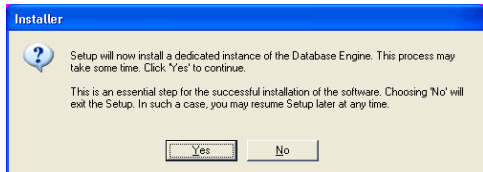
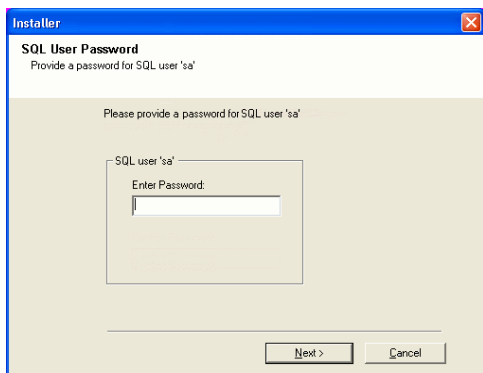
SET UP THE MICROSOFT SQL SERVER INSTANCE

8. Specify the SQL Server System Administrator password.

NOTES

- This is the password for the administrator's account containing the CommServe database.

Click **Next** to continue.



9. Click **Yes** to set up a dedicated instance of Microsoft SQL Server for the CommServe Server.

NOTES

- This prompt will only be displayed if SQL Server database instance is not installed on this computer.
- Clicking **No** will exit the install program.

- Enter the Installation Path for the Database Engine.

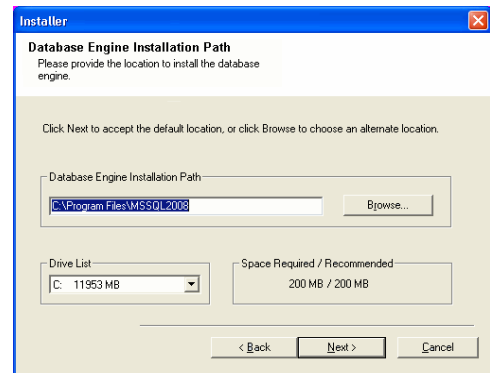
NOTES

- This is the location where you want to setup the Microsoft SQL Server System databases.
- If you plan to perform VSS enabled backups on the CommServe computer, it is recommended that the CommServe database is not installed on the system drive. VSS restores could cause system state restore issues.

Click **Browse** to change directories.

Click **Next** to continue.

The install program installs the database instance.



- Enter the MSSQL Server Installation Path.

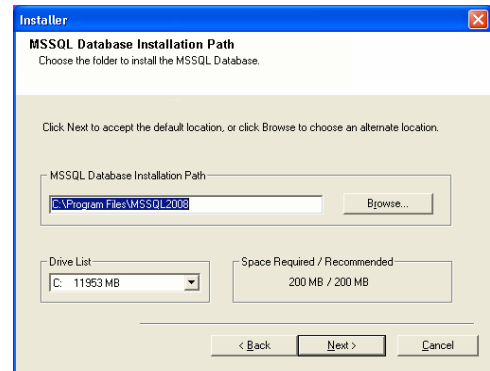
NOTES

- This is the location where you want to install Microsoft SQL Server.

Click **Browse** to change directories.

Click **Next** to continue.

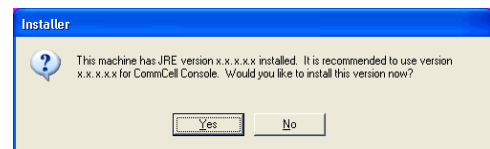
This step may take several minutes to complete.



- Click **Yes** to install the Java Runtime Environment (JRE) or click **No** if you would like to use the JRE Version already available in your computer.

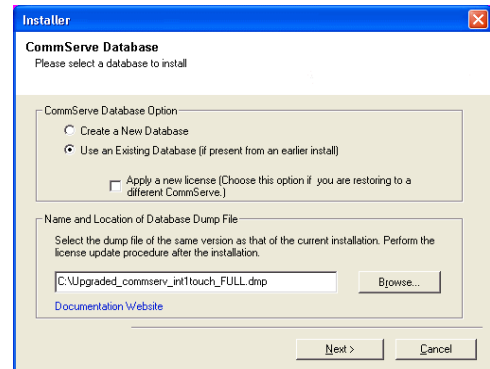
NOTES

- This prompt will be displayed only if the computer is running a JRE version prior to the one supplied in this installation program or no JRE version is available at all. See System Requirements - CommServe for more information on JRE versions.



SELECT COMMSEVE DATABASE

- Select **Use an Existing Database** to use a CommServe database from an earlier installation. Click **Browse** to locate the CommServe database dump.

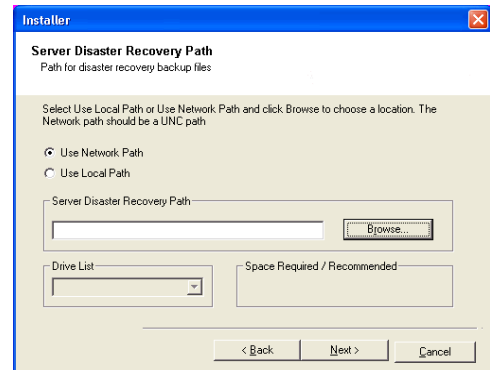


- Enter the network or local path where Disaster Recovery Backup files should be stored.

NOTES

- For cluster, specify a shared drive.
- If you selected **Use Network Path**, you must enter the **Network share username** and the **Network share password**.
 - The Network share username is the domain\username of the user that has administrative rights to the Disaster Recovery Backup destination path.
 - The Network share password is the password of the network share username.

Click **Next** to continue.



SET USER NAMES AND PASSWORDS

15. Enter the **CommCell Username** and **CommCell Password**.

NOTES

- The CommCell username and password will be used by the Administrator user to log on to the CommCell Console. This user is automatically created during installation and, by default, has the necessary capabilities to perform all functions. Additional CommCell users with the same or less security rights can be created after the installation of the software.

Click **Next** to continue.

16. Enter and confirm the **Media Password**.

NOTES

- This password is used to protect unauthorized data access from media used by the system.
- If you choose to password protect your media, it is essential that you record this password. In certain disaster recovery scenarios, it may be necessary to read your backup data directly from the backup media. This password will be required to directly access the media.

Click **Next** to continue.

CONFIGURE THE COMMCELL FOR WEB-BASED ADMINISTRATION

17. Click **Yes** to configure the CommCell Console for web administration, or Click **No** to continue without configuring the CommCell Console for web administration.

NOTES

- The Internet Information Server (IIS) must be installed on this computer in order to configure for web administration.
- Configuring this computer for web administration allows you to:
 - Access the CommCell Console and Books Online from a remote computer using a Web browser.
 - View CommCell reports via a Web browser.
 - Access Books Online by clicking the Help button (the icon with a ?) in the CommCell Console.

18. Specify the location where you want to install the software.

NOTES

- Do not install the software to a mapped network drive.
- Do not use the following characters when specifying the destination path: / : * ? " < > | #
It is recommended that you use alphanumeric characters only.
- If you intend to install other components on this computer, the selected installation directory will be automatically used for that software as well.
- If a component is already installed in this computer, this screen may not be displayed. The software will be automatically installed in the same location that was previously specified.

Click **Browse** to change directories.

Click **Next** to continue.

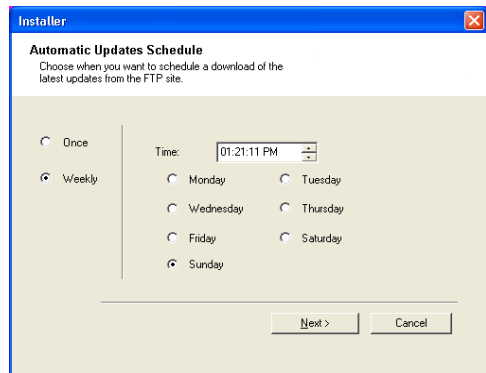
SCHEDULE AUTOMATIC UPDATE

19. Schedule to download the latest software updates from the FTP site.

NOTES

- This screen will appear, when you select the **Schedule FTP Download of Automatic Updates** option in the above step.
- Automatic Updates Schedule allows automatic downloading of software updates on a single or weekly basis.
- If you do not select this option, you can schedule these updates later from the CommCell Console.

Click **Next** to continue.

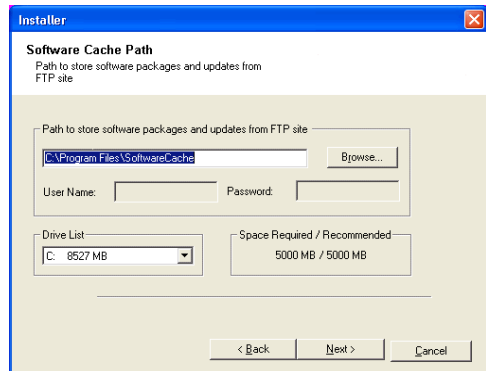


20. Specify the path where the update files from the FTP site should be stored.

NOTES

- This prompt will only be displayed if the **Setup Software Cache** option was enabled.

Click **Next** to continue.

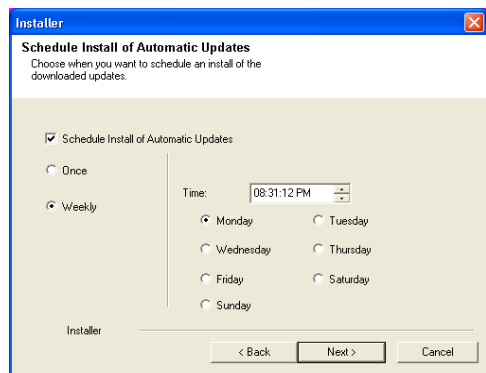


21. If necessary, select this option to schedule an automatic installation of software updates.

NOTES

- Schedule Install of Automatic Updates allows automatic installation of the necessary software updates on the computer on a single or weekly basis. If you do not select this option, you can schedule these updates later from the CommCell Console.
- To avoid conflict, do not schedule the automatic installation of software updates to occur at the same time as the automatic FTP downloading of software updates.
- If a component has already been installed, this screen will not be displayed; instead, the installer will use the same option as previously specified.

Click **Next** to continue.



VERIFY SUMMARY OF INSTALL OPTIONS

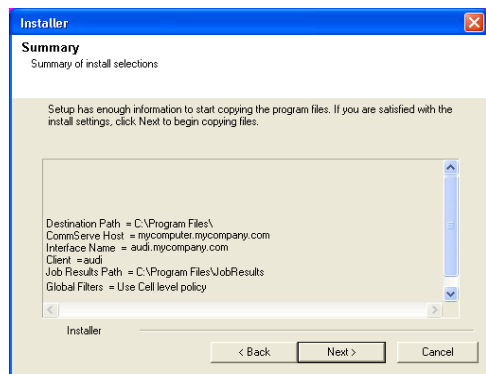
22. Verify the summary of selected options.

NOTES

- The **Summary** on your screen should reflect the components you selected for install, and may look different from the example shown.

Click **Next** to continue or **Back** to change any of the options.

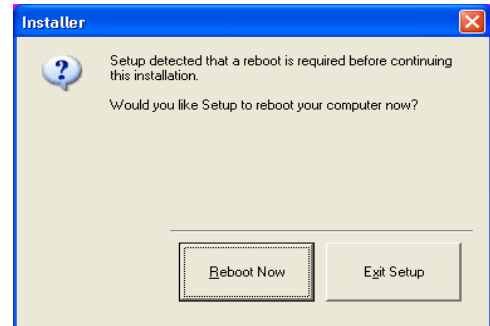
The install program now starts copying the software to the computer. This step may take several minutes to complete.



23. The System Reboot message may be displayed. If so, select one of the following:

- **Reboot Now**
If this option is displayed without the **Skip Reboot** option, the install program has found files required by the software that are in use and need to be replaced. If **Reboot Now** is displayed without the **Skip Reboot** option, reboot the computer at this point. The install program will automatically continue after the reboot.
- **Exit Setup**

If you want to exit the install program, click **Exit Setup**.

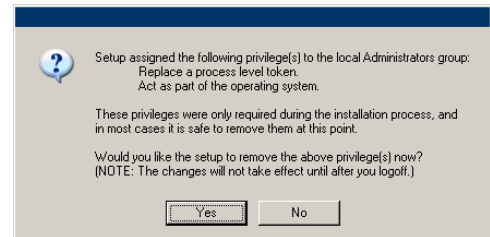


REMOVE THE REQUIRED PRIVILEGES

24. Click **Yes** to remove the privileges that were assigned earlier by the install program. If you do not wish to remove them, click **No**.

NOTES

- This option will only be displayed if you were prompted to assign the privileges earlier in the installation.



SETUP COMPLETE

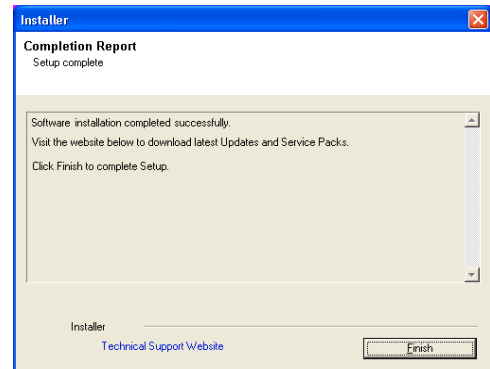
25. Setup displays the successfully installed components.

NOTES

- The **Setup Complete** message displayed on your screen will reflect the components you installed, and may look different from the example shown.
- If you install an Agent with the CommCell Console open, you need to refresh the CommCell Console (F5) to see the new Agents.
- If **Reboot Now** button is displayed make sure to reboot the computer before performing any other operations from the computer.

Click **Finish** to close the install program.

The installation is now complete.



26. To complete the installation, follow the configuration requirements in rebuilding the CommServe in a disaster recovery scenario.

See Configure the CommServe Computer for step-by-step instructions.

POST-INSTALL CONSIDERATIONS

GENERAL

Review Install Considerations after installing the software.

Install the CommServe SNMP Enabler

TABLE OF CONTENTS

Install Requirements

Before You Begin

Install Procedure

- Getting Started
- Cluster Selection
- Select Components for Installation
- Set Up the Required Privileges
- SNMP Trap Configuration
- Verify Summary of Install Options
- Remove the Required Privileges
- Setup Complete

Post-Install Considerations

INSTALL REQUIREMENTS

The following procedure describes the steps involved in installing the CommServe SNMP Enabler on both clustered and non-clustered environment.

The CommServe SNMP Enabler software must be installed on the CommServe computer.

Verify that the computer in which you wish to install the software satisfies the minimum requirements specified in System Requirements - CommServe for a cluster.

Review the following Install Requirements before installing the software:

GENERAL

- Verify that SNMP Services for Windows are running on the CommServe computer.
- Obtain a valid license for the CommServe SNMP Enabler software.
- SNMP Version 1 (SNMPv1) is the currently supported SNMP protocol.

CLUSTER

- In a clustered environment, the CommServe SNMP Enabler can be installed from the active node in the cluster group using the following procedure. The software can also be automatically installed on all available passive nodes when the software is installed in the cluster group, or you can choose to install any passive node(s) separately.
- Check the following on the cluster computer in which you wish to install the software:
 - Cluster software is installed and running.
 - Active and passive nodes are available.
 - Disk array devices configured with access to the shared array.
 - Public Network Interface Card is bound first, before the private Network Interface Card. (Does not apply to NetWare Cluster.)

BEFORE YOU BEGIN

- Log on to the CommServe computer as a member of the **Domain Administrator** group on that computer.
- On a clustered computer, ensure that you are logged on to the **active node** as the Domain User with administrative privileges to all nodes on the cluster.

INSTALL PROCEDURE

GETTING STARTED

1. Place the Software Installation Disc for the Windows platform into the disc drive.

After a few seconds, the installation program is launched.

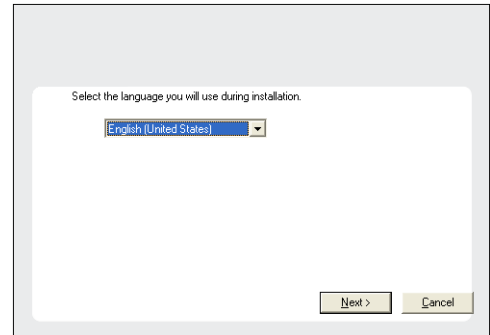
If the installation program does not launch automatically:

- Click the **Start** button on the Windows task bar, and then click **Run**.
- Browse to the installation disc drive, select **Setup.exe**, click **Open**, then click **OK**.

NOTES

- If you are installing on Windows Server Core editions, mount to Software Installation Disc through command line, go to the **AMD64** folder and run **Setup.exe**.

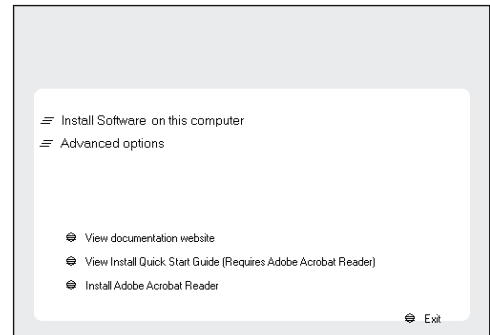
- Choose the language you want to use during installation. Click the down arrow and select the desired language from the drop-down list, and click **Next** to continue.



- Select the option to install software on this computer.

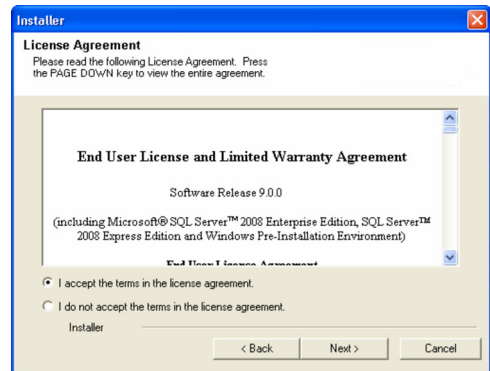
NOTES

- The options that appear on this screen depend on the computer in which the software is being installed.



- Read the license agreement, then select **I accept the terms in the license agreement**.

Click **Next** to continue.



CLUSTER SELECTION

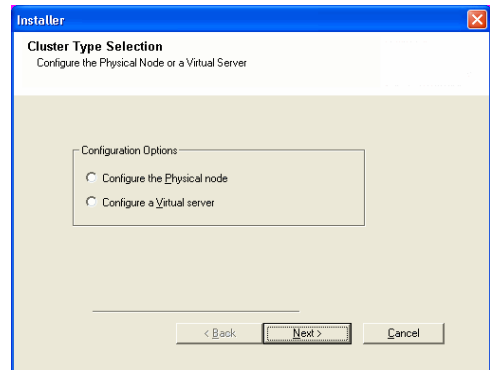
If you are installing in clustered environment, follow the steps below. For non-clustered environment, skip to Select Components for Installation.

- Select **Configure a Virtual Server**.

Click **Next** to continue.

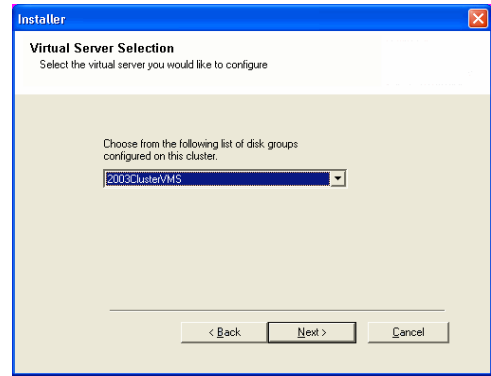
NOTES

- You will only see this screen if you are installing the SNMP Enabler software onto a physical node with the CommServe Database residing in the cluster group.



- Select the disk group in which the cluster group resides.

Click **Next** to continue.



SELECT COMPONENTS FOR INSTALLATION

7. Select the component(s) to install.

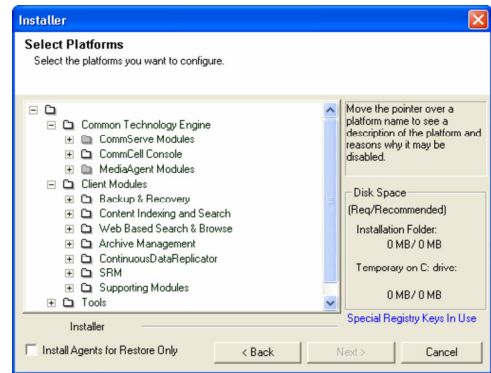
NOTES

- Your screen may look different from the example shown.
- Components that either have already been installed, or which cannot be installed, will be dimmed. Hover over the component for additional details.
- If you wish to install the agent software for restore only, select **Install Agents for Restore Only** checkbox. See Installing Restore Only Agents for more information.
- The **Special Registry Keys In Use** field will be highlighted when `GalaxyInstallerFlags` registry key is enabled. Move the mouse pointer over this field to see a list of registry keys that have been created in this computer.

Click **Next** to continue.

To install the CommServe SNMP Enabler, expand the `CommServe Modules` folder and select the following:

- CommServe SNMP Enabler

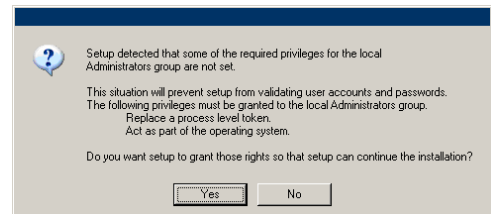


SET UP THE REQUIRED PRIVILEGES

8. Click **Yes** to set up the required privileges for the local administrators group.

NOTES

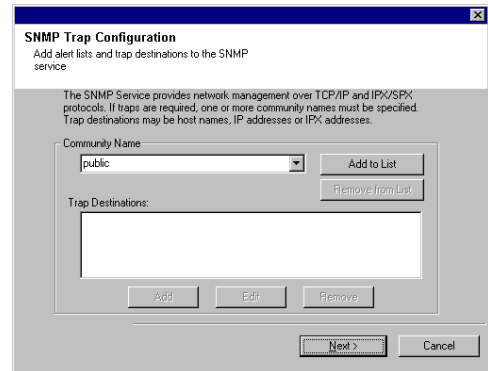
- This option will only appear if the Windows user account used to install the software does not have the required administrator rights (e.g., if the operating system was newly installed).
- If you choose to click **Yes**, the install program will automatically assign the required rights to your account. You may be prompted to log off and log back on to continue the installation.
- If you choose to click **No**, the installation will be aborted.
- You will be prompted at the end of the installation to decide if you want these privileges to be revoked.
- The install program checks your Windows user account for the following necessary operating system rights:
 - Right to increase quotas (this is referred to as adjust memory quotas for a process on Windows Server 2003).
 - Right to act as a part of the operating system.
 - Right to replace a process level token.



SNMP TRAP CONFIGURATION

9. Add alert lists and trap destinations to the SNMP service:

- Type a name for the group of computers to receive SNMP traps in the **Community** name pane.
- Click **Add to list** to add the name of the community to the drop down menu.
- Click **Add** to add destination computer(s) that will receive SNMP traps.



VERIFY SUMMARY OF INSTALL OPTIONS

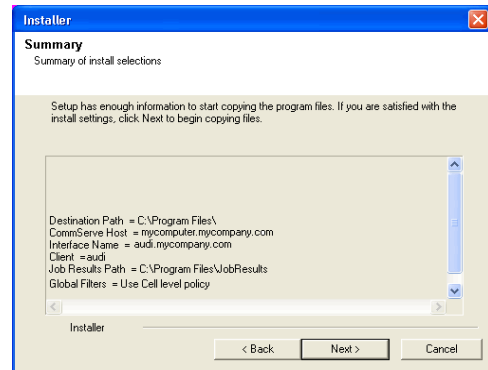
10. Verify the summary of selected options.

NOTES

- The **Summary** on your screen should reflect the components you selected for install, and may look different from the example shown.

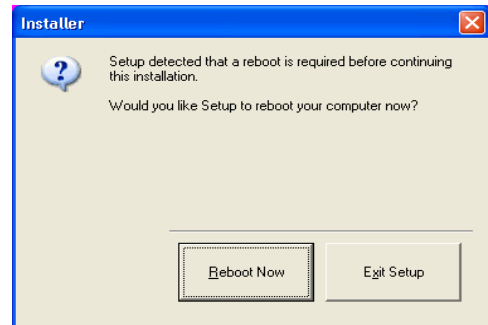
Click **Next** to continue or **Back** to change any of the options.

The install program now starts copying the software to the computer. This step may take several minutes to complete.



11. The System Reboot message may be displayed. If so, select one of the following:

- Reboot Now**
If this option is displayed without the **Skip Reboot** option, the install program has found files required by the software that are in use and need to be replaced. If **Reboot Now** is displayed without the **Skip Reboot** option, reboot the computer at this point. The install program will automatically continue after the reboot.
- Exit Setup**
If you want to exit the install program, click **Exit Setup**.

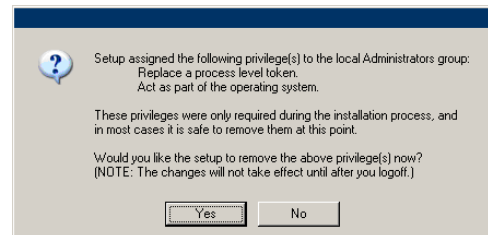


REMOVE THE REQUIRED PRIVILEGES

12. Click **Yes** to remove the privileges that were assigned earlier by the install program. If you do not wish to remove them, click **No**.

NOTES

- This option will only be displayed if you were prompted to assign the privileges earlier in the installation.



INSTALL REMAINING CLUSTER NODES

If you are installing in clustered environment, follow the steps below to install on remaining nodes of the cluster. For non-clustered environment, skip to Setup Complete.

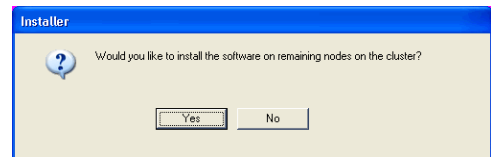
13. To install/upgrade the software on the remaining nodes of the cluster, click **Yes**. To complete the install for this node only, click **No**.

14. Select cluster nodes from the **Preferred Nodes** list and click the arrow button to move them to the **Selected Nodes** list.

NOTES

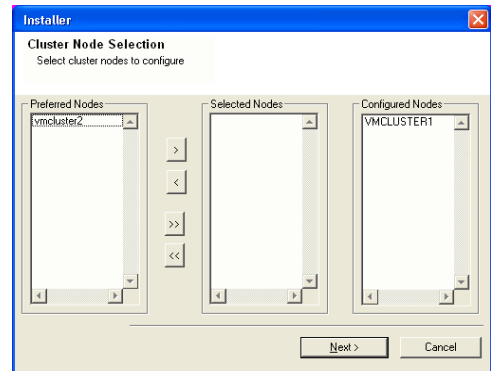
- The list of **Preferred Nodes** displays all the nodes found in the cluster; from this list you should only select cluster nodes configured to host this cluster group server.
- Do not select nodes that already have multiple instances installed. For more information, see Multi Instancing.

When you have completed your selections, click **Next** to continue.



15. Type the **User Name** and **Password** for the Domain Administrator account, so that the installer can perform the remote install/upgrade of the cluster nodes you selected in the previous step.

Click **Next** to continue.



16. The progress of the remote install for the cluster nodes is displayed; the install can be interrupted if necessary.

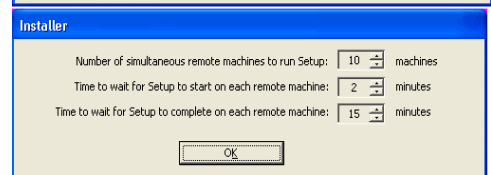
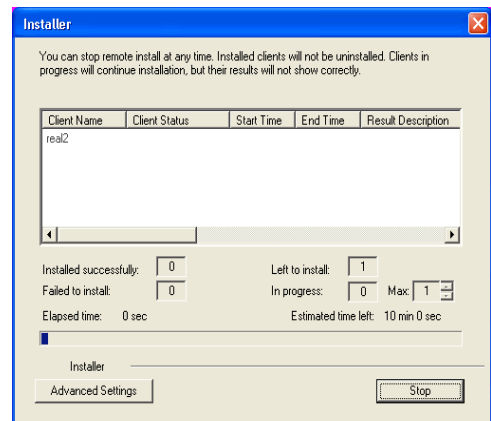
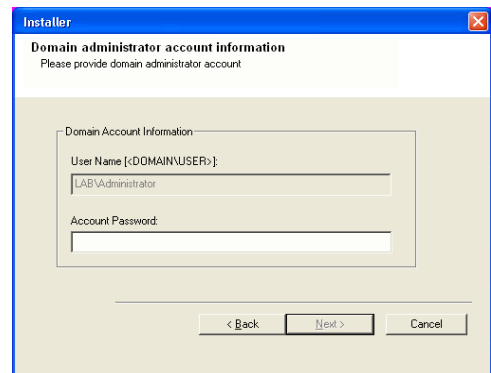
Click **Stop** to prevent installation to any nodes after the current ones complete.

Click **Advanced Settings** to specify any of the following:

- Maximum number of nodes on which Setup can run simultaneously.
- Time allocated for Setup to begin executing on each node, after which the install attempt will fail.
- Time allocated for Setup to complete on each node, after which the install attempt will fail.

NOTES

- If, during the remote install of a cluster node, setup fails to complete or is interrupted, you must perform a local install on that node. When you do, the install begins from where it left off, or from the beginning if necessary. For procedures, see Manually Installing the Software on a Passive Node.

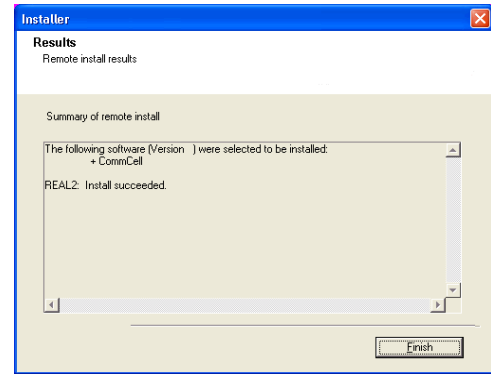


17. Read the summary for remote installation to verify that all selected nodes were installed successfully.

NOTES

- If any node installation fails, you must manually install the software on that node once the current installation is complete. (See Manually Installing the Software on a Passive Node for step-by-step instructions.)
- The message displayed on your screen will reflect the status of the selected nodes, and may look different from the example.

Click **Next** to continue.



SETUP COMPLETE

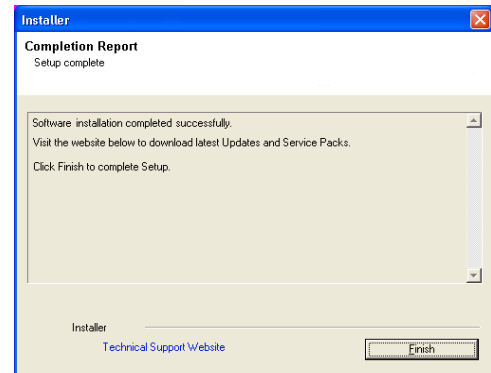
18. Setup displays the successfully installed components.

NOTES

- The **Setup Complete** message displayed on your screen will reflect the components you installed, and may look different from the example shown.
- If you install an Agent with the CommCell Console open, you need to refresh the CommCell Console (F5) to see the new Agents.
- If **Reboot Now** button is displayed make sure to reboot the computer before performing any other operations from the computer.

Click **Finish** to close the install program.

The installation is now complete.



19. If you are installing in a clustered environment, proceed as follows, based on your installation configuration:

- If you installed both the CommServe software and the CommServe database in the cluster group:
 - a. Fail over the disk group containing the CommServe to the passive nodes at least once, so that the configurations to the passive node occur. This must be done before installing any other software components. The install program updates the passive nodes on the cluster so that the cluster group server can fail over. A program to create the CommServe Data Source Name (DSN) is launched automatically on each passive node.
 - b. Fail back the nodes, then continue on to the MediaAgent installation.
 - c. If the passive node was not available while installing the software, you must manually install the software on the passive node now. (See [Manually Installing the Software on a Passive Node](#) for step-by-step instructions.)
 - d. You must install the CommCell Console on a physical node of the cluster before proceeding. For instructions, see [Install the CommCell Console - Windows](#).
- If you installed the CommServe software on the active physical node, and the SQL database resides in a cluster group, you must now install the CommServe software on every passive node as well. For step-by-step instructions, see [Manually Installing the Software on a Passive Node](#).

POST-INSTALL CONSIDERATIONS

- Once the CommServe SNMP Enabler software is installed, verify that each computer defined during the installation to receive SNMP Traps is properly set up through their trap receiver software.

Silent Install - CommServe/CommNet Server

TABLE OF CONTENTS

Install Requirements

Before You Begin

Install Procedure

- Getting Started
- Select Components for Installation
- Configuration of Other Installation Options
- Set User Names and Passwords
- Configure the CommCell® Console for Web-Based Administration
- Verify Summary of Install Options
- Setup Complete

Playback Procedure

Post Install Considerations

INSTALL REQUIREMENTS

A silent install consists of two distinct phases. In the recording phase, an install is recorded, saving your install options to an `.xml` file. In the playback phase, the `.xml` file is played back by the install program, which installs the software with the recorded options without any prompting. Through this method, the deployment of the software can be automated.

RECORD REQUIREMENTS

To record an install, the install program is started from the command line with the parameters described below. When recording an install, note the following:

- The install program only records your choices, it does not execute the install.
- No license is consumed when recording an install.
- All Agents are selectable when recording an install.
- Review the System Requirements and the Installation procedures for each component you are installing.
- Close all applications and disable any programs that run automatically, including antivirus, screen savers and system utilities. Some of the programs, including antivirus software, may be running as a service. Stop and disable such services before you begin. You can re-enable them after recording the install.
- If you intend to play back this recorded install on multiple computers, choose options that are applicable to all those computers. For example when specifying an installation folder, be sure it exists on all target computers.
- If your network does not have DNS lookup or some other name resolution facility, you may be asked to enter the IP address of the server computer.

PLAYBACK REQUIREMENTS

Playing back a recorded installation installs the software with the options saved in the `.xml` file you created during the record procedures. Note the following when playing back a recorded install:

- A license is consumed on the server for each licensed component you install.
- You will not be prompted for any information, but note that the install program (`QInstaller.exe`) will appear in the Windows Task Manager.
- Review the System Requirements and the Installation procedures for each component you are installing.
- If your network does not have DNS lookup or some other name resolution facility, you may be asked to enter the IP address of the server computer.

BEFORE YOU BEGIN

- Log on to the client as local Administrator or as a member of the Administrators group on that computer.

INSTALL PROCEDURE

GETTING STARTED

1. Place the software installation disc for the Windows platform into the disc drive. After a few seconds, the installation program is launched.
Click **Exit** to close the install program.
2. Choose the language you want to use during installation. Click the down arrow and select the desired language from the drop-down list, and click **Next** to continue.

3. Select the **Advanced options** to install software.

NOTES

The options in the installation menu depends on the computer in which the software is being installed, and may look different from the example shown.

4. Select **Create a recording of user selections - Record Mode** option to start the recording of the install.

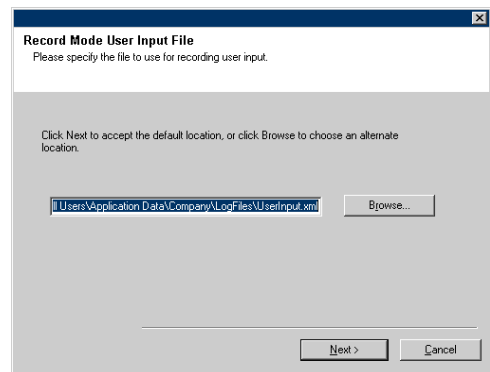
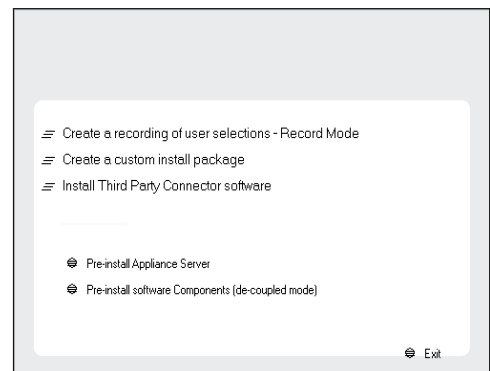
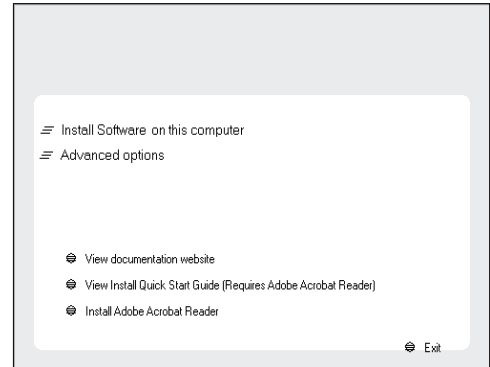
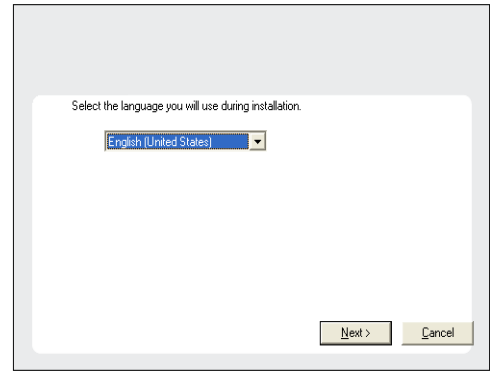
5. The install options will be recorded to a file called `UserInput.xml` which will be located in the `C:\Documents and Settings\Company\LogFiles\` folder.

Click **Browse** to change directories.

Click **Next** to continue.

6. Read the license agreement, then select **I accept the terms in the license agreement**.

Click **Next** to continue.





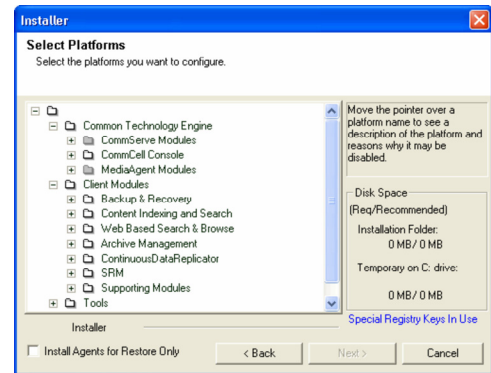
SELECT COMPONENTS FOR INSTALLATION

7. Select the component(s) to install.

NOTES

- Your screen may look different from the example shown.
- Components that either have already been installed, or which cannot be installed, will be dimmed. Hover over the component for additional details.
- If you wish to install the agent software for restore only, select **Install Agents for Restore Only** checkbox. See Installing Restore Only Agents for more information.
- The **Special Registry Keys In Use** field will be highlighted when `GalaxyInstallerFlags` registry key is enabled. Move the mouse pointer over this field to see a list of registry keys that have been created in this computer.

Click **Next** to continue.



CONFIGURATION OF OTHER INSTALLATION OPTIONS

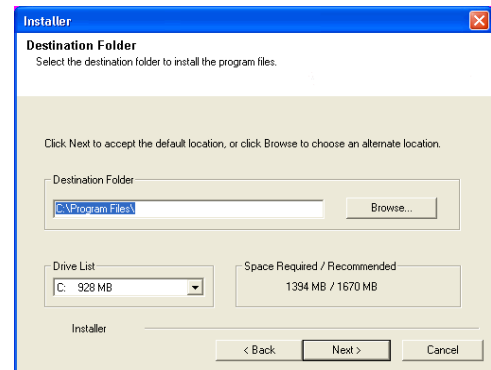
8. Specify the location where you want to install the software.

NOTES

- Do not install the software to a mapped network drive.
- Do not use the following characters when specifying the destination path:
/ : * ? " < > | #
It is recommended that you use alphanumeric characters only.
- If you intend to install other components on this computer, the selected installation directory will be automatically used for that software as well.
- If a component is already installed in this computer, this screen may not be displayed. The software will be automatically installed in the same location that was previously specified.

Click **Browse** to change directories.

Click **Next** to continue.



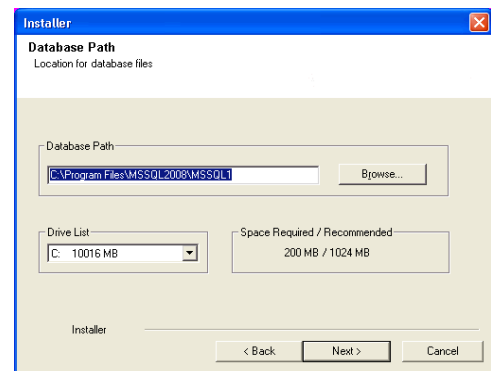
9. Specify the location of the database.

NOTES

- Do not specify a mapped network drive.
- You can either accept the default or select a different location on a local disk drive. However, you must ensure that the drive has at least 1GB of free space.
- The directory file path selected should not be located on a FAT drive. A FAT drive cannot be supported as the location for this database because it does not allow a temporary sparse file to be generated when creating the database snapshot, which is required for data verification.
- If the default metadata database directory is low in disk space, provide a path that is not associated with another application.

Click **Browse** to change directories.

Click **Next** to continue.

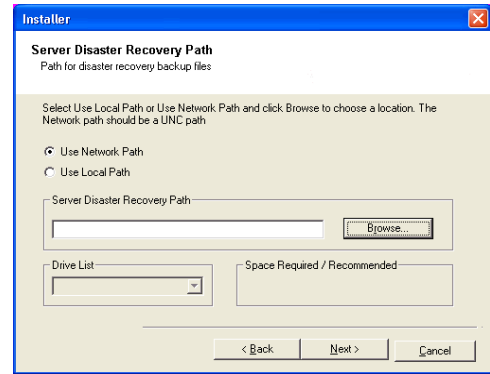


10. Enter the network or local path where Disaster Recovery Backup files should be stored.

NOTES

- For cluster, specify a shared drive.
- If you selected **Use Network Path**, you must enter the **Network share username** and the **Network share password**.
 - The Network share username is the domain\username of the user that has administrative rights to the Disaster Recovery Backup destination path.
 - The Network share password is the password of the network share username.

Click **Next** to continue.



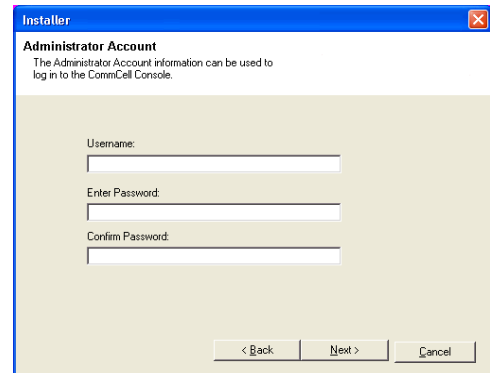
SET USER NAMES AND PASSWORDS

11. Enter the **CommCell Username** and **CommCell Password**.

NOTES

- The CommCell username and password will be used by the Administrator user to log on to the CommCell Console. This user is automatically created during installation and, by default, has the necessary capabilities to perform all functions. Additional CommCell users with the same or less security rights can be created after the installation of the software.

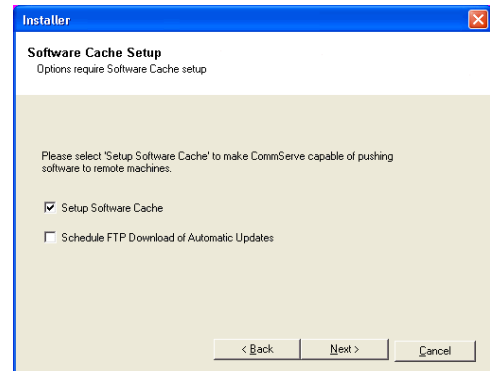
Click **Next** to continue.



12. Select **Setup Software Cache** option to download the software updates automatically.

Select **Schedule FTP Download of Automatic Updates** option to schedule automatic FTP downloading of software updates.

Click **Next** to continue.

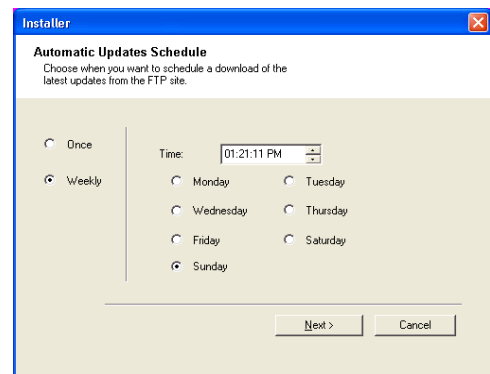


13. Schedule to download the latest software updates from the FTP site.

NOTES

- This screen will appear, when you select the **Schedule FTP Download of Automatic Updates** option in the above step.
- Automatic Updates Schedule allows automatic downloading of software updates on a single or weekly basis.
- If you do not select this option, you can schedule these updates later from the CommCell Console.

Click **Next** to continue.

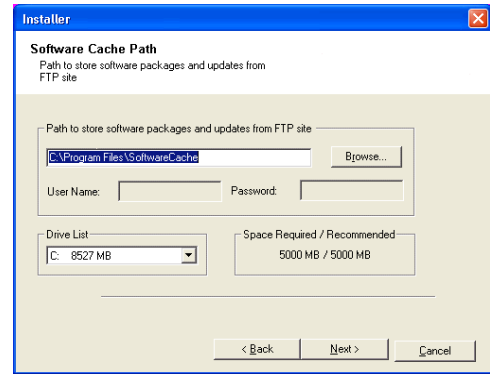


14. Specify the path where the update files from the FTP site should be stored.

NOTES

- This prompt will only be displayed if the **Setup Software Cache** option was enabled.

Click **Next** to continue.

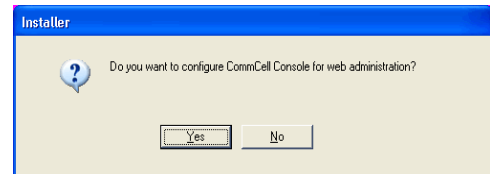


CONFIGURE THE COMMCELL® CONSOLE FOR WEB-BASED ADMINISTRATION

15. Click **Yes** to configure the CommCell Console for web administration, or Click **No** to continue without configuring the CommCell Console for web administration.

NOTES

- The Internet Information Server (IIS) must be installed on this computer in order to configure for web administration.
- Configuring this computer for web administration allows you to:
 - Access the CommCell Console and Books Online from a remote computer using a Web browser.
 - View CommCell reports via a Web browser.
 - Access Books Online by clicking the Help button (the icon with a ?) in the CommCell Console.



VERIFY SUMMARY OF INSTALL OPTIONS

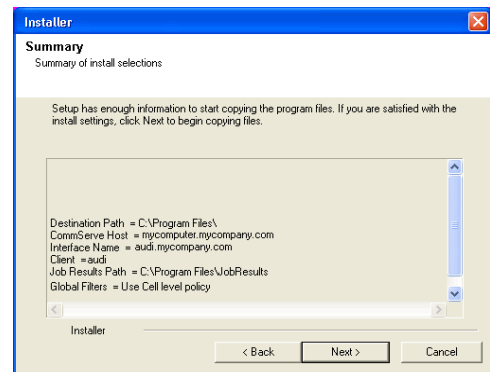
16. Verify the summary of selected options.

NOTES

- The **Summary** on your screen should reflect the components you selected for install, and may look different from the example shown.

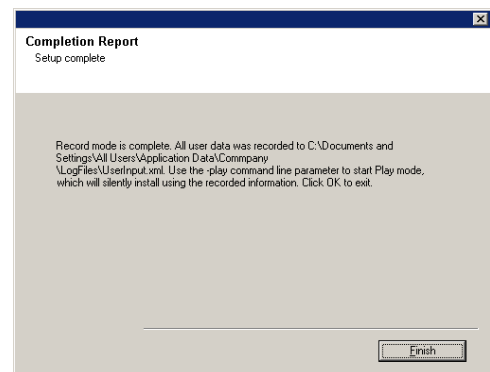
Click **Next** to continue or **Back** to change any of the options.

The install program now starts copying the software to the computer. This step may take several minutes to complete.



SETUP COMPLETE

17. Click **OK**.
This completes the recording.



The UserInput.xml file created during the record mode can be edited to meet particular needs, such as using the generated file as a base, and customizing it for many different playback install.

See XML Input File for CommServe Silent Install for the example of the contents of a default xml input file generated during the record mode of a CommServe and for the list of parameters, the default values and description.

PLAYBACK PROCEDURE

1. Log on to the client as local Administrator or as a member of the Administrators group on that computer.
2. Place the software installation disc for the Windows platform into the disc drive. After a few seconds, the installation program is launched.
Click **Exit** to close the install program.
3. Click the Windows **Start** button, point to **Programs**, point to **Accessories**, then click **Command Prompt**.

To start the installation, type the following command:

```
QInstaller.exe /play "path\filename.xml"
```

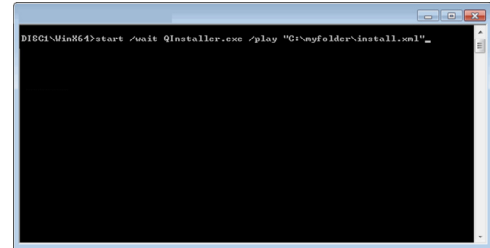
For example, if you type `QInstaller.exe /play "C:\Documents and Settings\Company\LogFiles\UserInput.xml"`, the file called `UserInput.xml` located in the `C:\Documents and Settings\Company\LogFiles\` folder will be played back, installing the software with all the recorded options to the local computer.

NOTES

Your screen may look from the example shown.

4. The installation proceeds silently, with no indication on the screen. Any errors generated are written to the `GalaxyInstallerErrors.txt` file. For more information on the installation, see `GalaxyInstallerLog.txt`.

When the `QInstaller.exe` application is no longer shown in the Windows Task Manager, the install is complete.



POST-INSTALL CONSIDERATIONS

ALL AGENTS

Review the Post-Install Considerations specific to the components that were installed using this procedure. (See Installation Considerations for a list of all Install procedures.)

Custom Calendar

Topics | How To | Related Topics

Overview

- Scheduling and Custom Calendars
- Auxiliary Copy and Custom Calendars
- Data Aging Based on Extended Retention with Copies using Custom Calendars

How to Use Custom Calendars

Other Operations

- Audit Trail
- Events

Best Practices

Related Reports

OVERVIEW

The standard Gregorian calendar, which starts on the first day of January and is comprised of months that have a set number of days, is used as the basis for all scheduled operations, as well as data aging and auxiliary copies.

For organizations that use custom calendars for their fiscal year (i.e., a calendar that starts on a different day and month, and whose months have a unique number of days), standard calendars may pose a problem when operations must be scheduled according to the days of their custom calendar.

The Custom Calendar feature gives users the ability to create custom calendars so that their operations can be run within the boundaries of their own custom calculated time. A company may base their custom year on a calendar that starts in February, ends in January, and whose months have a unique number of days. This feature allows users to use the same custom calendar for their scheduled operations, and as the basis for copy data to storage policy copies, and for the aging of data from these copies.

Use the Control Panel from the **Tools** menu on the CommCell Console to create custom calendars.

SCHEDULING AND CUSTOM CALENDARS

Custom calendars can be used for weekly, monthly and yearly schedules. For example, a monthly schedule for a custom calendar that defines months that are 32 days long will run every 32 days, starting on the starting day of the month as defined in the calendar. Yearly schedules will run every n days (the number of days defined in the calendar), and will start on the day that is defined as the start of the custom calendar year.

AUXILIARY COPY AND CUSTOM CALENDARS

Selective storage policy copies associated with custom calendars will have data copied during auxiliary copy operations either monthly, quarterly, half yearly, or yearly based on the days defined in the calendar. If a storage policy copy is re-associated with a different calendar, the auxiliary copy operation re-calculates the dates in which data is copied based on the time definitions set in the custom calendar.

DATA AGING BASED ON EXTENDED RETENTION WITH COPIES USING CUSTOM CALENDARS

A data aging operation that ages data from a storage policy copy with the Extended Retention option enabled will age data according to the time definitions set in the custom calendar, if that copy is using a custom calendar.

For example, let's assume that you want to preserve the tapes containing the last full and incremental backups copied during monthly periods that end on the last Friday of the month. In order to do this, you must define a custom calendar to make the last Friday of the month signify last day of the month, and you must select the **Last Full Backup of Time Period** option from the associated storage policy copy's properties Retention dialog. When selected, the last full backup of each extended retention rule will be retained, providing there are no remaining full backup scheduled for the same subclient during that time period. To define the custom calendar to make the last Friday of the month signify last day of the month, see Create a Custom Calendar. In this case, the defined calendar would resemble the following:

Month	Days	Start Date
January 2009	30	January 1
February 2009	28	January 31
March 2009	28	February 1
April 2009	28	March 28
May 2009	35	April 25

June 2009	28	May 30
July 2009	35	June 27
August 2009	28	August 1
September 2009	28	August 29
October 2009	35	September 26
November 2009	28	October 31
December 2009	28	November 28

HOW TO USE CUSTOM CALENDARS

The following section provides the steps for using Custom Calendars.

1. Create a Custom Calendar
 - A custom calendar can be created from the Custom Calendars dialog box.
2. Create a Job Schedule
 - A custom calendar can be selected for a monthly or yearly schedule from the Schedule Details tab of the Schedule Details dialog box. The custom calendar can be used as an alternative to a standard calendar.
3. Associate a Custom Calendar to a Storage Policy Copy
 - A custom calendar can be associated with a storage policy copy from the General tab of the **Copy Properties** dialog box.
 - Once associated, Auxiliary Copy and Data Aging operations of this copy will be based on the custom calendar.

Custom calendars are not supported in Express versions of the software.

CUSTOM CALENDARS AND OTHER OPERATIONS

AUDIT TRAIL

Operations performed with this feature are recorded in the Audit Trail. See Audit Trail for more information.

EVENTS

One year from the date in which a custom calendar definition is missing from a custom calendar, a Major event is generated in the Event Viewer every 24 hours.

BEST PRACTICES

Consider the following when creating custom calendars:

- If you plan to use a custom calendar, be sure that the calendar has been defined for several years. If the time definitions for a custom calendar have expired:
 - Related schedules will be deleted.
 - Data Aging operations will not prune data from a storage policy copy using an expired custom calendar.
- Changing a time definition in a custom calendar for a time that occurs in the past will:
 - Change the way data is aged from a copy that has the Extended Retention option enabled, according to the dates of the custom calendar.
 - Change the time intervals by which data is copied to a selective copy, according to the dates of the custom calendar.
- It is recommended that new storage policy copies and schedules be created for use with a new custom calendar, but this is not necessary.

RELATED REPORTS

CommCell Configuration Report

The CommCell Configuration report identifies the schedules and/or storage policy copies that are using custom calendars.

Job Schedule-List and Job Schedule-Interval reports

The Job Schedule reports identify the schedules that are using custom calendars.

Storage Policy Report

The Storage Policy report identifies the storage policy copies that are using custom calendars.

[Back to Top](#)

Custom Calendar - How To

[Topics](#) | [How To](#) | [Related Topics](#)

[Associate a Custom Calendar to a Storage Policy Copy](#)

[Create a Custom Calendar](#)

[Create a Job Schedule](#)

[Delete a Custom Calendar](#)

[Modify a Custom Calendar](#)

ASSOCIATE A CUSTOM CALENDAR TO A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To associate a custom calendar to a storage policy copy:

1. Right-click the storage policy copy for which you wish to associate a custom calendar, and then click **Properties**.
2. From the General tab of the **Copy Properties** dialog box, select a calendar from the **Calendar for Selective Copy and Extended Retention** checkbox.
3. Click **OK** to save your changes.

Associating a custom calendar to a storage policy copy changes the time intervals by which data is copied to and aged from this copy.

CREATE A CUSTOM CALENDAR

Required Capability: See Capabilities and Permitted Actions

▶ To create a custom calendar:

1. From the CommCell Browser, right-click the CommServe, click **Control Panel**, and then click **Custom Calendars**.
2. From the Custom Calendars dialog box, click **Add**.
3. From the Add a new Calendar dialog box:
 - Enter the name of the calendar in the **Name** box.
 - Select a beginning month in the **Begin Month** drop down list.
 - Enable the **Make this calendar the default for all operations** option to use this calendar for all subsequent scheduled operations, selective copy rules and extended retention rules.
 - Click the **Define Custom Months** check box.
 - Select the year in which the calendar is to begin in the **Begin Year** drop down list.
 - Enter the date in which the starting date of this custom calendar is to start relative to a standard calendar. For example, if your calendar is to start on February 10, select that date in the fields provided.

NOTE

The start date of a custom calendar must be within 15 days prior to or after day 1 of the selected **Begin Month**. For example, if you select January (2007) as the **Begin Month**, then the start date of the custom calendar can be defined as any date from December 15th (2006) through January 15th (2007).

- Click **Define Months**.
4. From the Define Months for <n> dialog box:
 - Click **Previous** and **Next** to scroll to the appropriate year.
 - In the **Days** column, enter the number of days for each month. (Minimum: 15 days / Maximum: 45 days)
 - Click **Apply**.

- The start dates of each month will adjust accordingly based on the number of days for each month in the **Days** column.
 - Click **Previous** and **Next** to customize any additional years.
 - Click **OK**.
5. The new calendar is displayed in the **Custom Calendars** window.
-

CREATE A JOB SCHEDULE

Required Capability: See Capabilities and Permitted Actions

▶ To create a job schedule for an operation:

1. From the dialog box of the appropriate operation, click **Schedule**.
 2. In the Schedule Details dialog box that appears, select the appropriate scheduling options.
 3. Click **Options** to view the Advanced Schedule Options dialog box.
 4. Specify the following options:
 - Range of recurrence:** Specify the date on which you want this schedule to take effect.
 - Repeat:** Select the value for which you want to run the job repeatedly on the day in which the job is scheduled to run.
 - Time Zone:** Select a specific time zone from which the job schedule time will be based.
 5. You can also confirm and/or edit (where applicable) your choices from the **Job Summary** tab. For a monthly or yearly schedule, you can select either a standard calendar or a custom calendar.
 6. Click **OK**.
-

DELETE A CUSTOM CALENDAR

Required Capability: See Capabilities and Permitted Actions

▶ To delete a custom calendar:

1. From the CommCell Browser, right-click the CommServe, click **Control Panel**, and then click **Custom Calendars**.
2. From the Custom Calendars dialog box, click a calendar, and then click **Delete**.
3. Click **Yes** to the confirmation prompt.

A custom calendar that is currently being used for a schedule or a selective copy cannot be deleted. Re-assign the schedule or storage policy to another calendar (or the standard calendar) before deleting this calendar.

MODIFY A CUSTOM CALENDAR

Required Capability: See Capabilities and Permitted Actions

▶ To modify a custom calendar:

1. From the CommCell Browser, right-click the CommServe, click **Control Panel**, and then click **Custom Calendars**.
2. From the Custom Calendars dialog box, select a calendar, and then click **Edit**.
3. From the Edit Calendar dialog box:
 - Modify the name of the calendar in the **Name** box.
 - Enable the **Make this calendar the default for all operations** option to use this calendar for all subsequent scheduled operations, selective copy rules and extended retention rules.
 - Enter the date in which the starting date of this custom calendar is to start relative to a standard calendar. For example, if your calendar is to start on February 10, select that date in the fields provided.

NOTE

The start date of a custom calendar must be within 15 days prior to or after day 1 of the selected **Begin Month**. For example, if you select January (2007) as the **Begin Month**, then the start date of the custom calendar can be defined as any date from December 15th (2006) through January 15th (2007).

- Click **Define Months**.

4. From the Define Months for <n> dialog box:

- Click **Previous** and **Next** to scroll to the appropriate year.
- In the **Days** column, enter the number of days for each month. (Minimum: 15 days / Maximum: 45 days)
- Click **Apply**.
- The start dates of each month will adjust accordingly based on the number of days for each month in the **Days** column.
- Click **Previous** and **Next** to customize any additional years.
- Click **OK**.

5. The calendar is now edited.

Modification made to a custom calendar take effect upon the completion of the next scheduled job associated with the original custom calendar, i.e., a scheduled job will still take place as planned according to the original calendar definitions, and upon completion of the job, the new custom calendar definitions will take effect.

[Back to Top](#)

Storage Policies

Topics | How To | How Do I | Support | Related Topics

Overview

- Quick Recovery Agent

Types of Storage Policies

- Standard Storage Policy for iDataAgent Backup and/or DataArchiver Archiving
- Disaster Recovery Backup Storage Policy

Data Aging and Storage Policy Time Zones

Storage Policy Operations

Best Practices

- Limit the Number of Storage Policies in Your CommCell Environment
- Disable Additional Subclient Associations with a Storage Policy
- Password Protect the Media Associated with a Storage Policy
- Hide Inactive Storage Policies

Considerations

- NAS-attached Libraries and Drive Pools
- NAS Clients
- Subclients
- Incremental Storage Policy
- Deleting a Storage Policy
- Disaster Recovery Backup Storage Policy
- Synchronous Copies
- Selective Copies
- Data Streams

Audit Trail

Related Reports

OVERVIEW

Storage policies act as the primary channels through which data is included in data protection and data recovery operations. A storage policy forms the primary logical entity through which a subclient or instance is backed up. Its chief function is to map data from its original location to a physical media. The system provides a default iDataAgent storage policy for each media library, stand-alone, or disk drive once they are configured.

You can create storage policies to:

- Customize data retention periods for different subclients.

For example, where it may be necessary to restore/recover old data, you may want to create a storage policy with longer retention periods when performing data protection operations on a server. On the other hand, if the data being protected is not as critical, you can set a shorter retention period in order to release the media more quickly.

- Define the number of streams available to run simultaneous data protection or data recovery operations for all subclients that use the same storage policy.

For example, if you set a stream count to three in the storage policy:

- data protection operations from three subclients using the same storage policy can run simultaneously rather than in series.
- data protection operations from one subclient using multiple streams can run up to three streams simultaneously. (Streams are supported for certain database iDataAgents and File System Multi-Streaming is supported for certain non-database iDataAgents, allowing increased data protection and data recovery speed by splitting the data across multiple tapes simultaneously.)

When a storage policy is configured to use more than one data stream, it is important that the data streams are equally used; parallel copying using multiple source and destination drives may not be effective if the data is concentrated in one stream. The stream randomization feature enables random choosing of the data streams, increasing the rate of data transfer by copying data from different streams in parallel. See [Enable Stream Randomization](#) for instructions.

Also, it is recommended that you configure the tuning parameters to evenly distribute the data across all the streams. You can specify the interval to check

the data size in the streams and the threshold to decide data distribution among the streams. See Tune Stream Randomization for instructions.

A secondary copy of a storage policy provides a means of making an additional copy of backed up data and is used in auxiliary copy operations, or data protection operations that create inline copies.

QUICK RECOVERY AGENT

If you are using the Quick Recovery Agent, this agent uses QR Policies for the data included in the agent's Quick Recovery Creation operations. For more information on QR Policies, see QR Policies.

TYPES OF STORAGE POLICIES

Two types of storage policies can be defined. They are:

- Standard: *iDataAgent Backup* and *DataArchiver Archiving*
- Disaster Recovery Backup

The following sections provide a brief description of the storage policies.

STANDARD STORAGE POLICY FOR */DATAAGENT BACKUP* AND *DATAARCHIVER ARCHIVING*

A standard storage policy can be created to run both *iDataAgent Backup* and *DataArchiver archiving* operations.

/DATAAGENT BACKUP

The Standard storage policy for *iDataAgent Backups* is used by subclients associated with *iDataAgents*, to perform backup and restore operations. Subclients can be configured to use storage policies using one of the following methods:

- One storage policy for all types of backups, including full and non-full backups.
- One storage policy for full backups and another storage policy for non-full backups (incrementals and differentials). The storage policy for non-full backups is referred to as the Incremental Storage Policy. For more information on Incremental Storage Policy, see Incremental Storage Policy.
- For SQL Server *iDataAgents*, it is possible to have one storage policy for full backups, another storage policy for differential backups (using incremental storage policy), and another storage policy for transaction log backups.

By default, the retention period for the *iDataAgent Backup* data is set for an infinite period of time. This retention period can be modified to better suit your data retention needs. If the retention time is changed, it is recommended that you keep this data for a minimum of 15 days and two cycles. For more information on changing retention rules, see Retention.

DATAARCHIVER ARCHIVING

The Standard storage policy for *DataArchiver Archiving* is used by subclients associated with *DataArchiver* agents, to perform archiving and recovery/retrieval of archived data. The retention period for *DataArchiver* data can only be set by time, not cycles.

By default, the retention period for the *DataArchiver* data is set to be retained for an infinite period of time. If you want to change this retention time, it is recommended that it be set for a minimum of 365 days.

For more information on the *DataArchiver* agents, see the appropriate product features page.

Quick Recovery Agent uses QR policies for QR volume creation and QR volume recovery operations.

DISASTER RECOVERY BACKUP STORAGE POLICY

As an extra protection to rebuild your CommCell in the event of a disaster, Disaster Recovery Backup storage policies are used to store metadata to media. This metadata stores information about the CommCell and the backed up data. In case of a system failure, you can get Disaster Recovery Backup data back from the media used by the Disaster Recovery Backup storage policy. Though standard storage policies can be used for Disaster Recovery Backup data, it is not recommended.

A default Disaster Recovery Backup storage policy [*CommServeDR (host name)*] is automatically created when the first library in the CommCell is configured. This type of storage policy is recommended because it only writes the Disaster Recovery Backup data to the media, and its default retention period is defined as 60 days and 60 cycles, which can be easily changed during configuration. The media being used for this storage policy should be removable to prevent accidental data loss due to system failure. If the first library configured is a disk library, change your Disaster Recovery Backup configuration to use a Disaster Recovery Backup storage policy associated with a tape library as soon as the first tape library is configured. You can create as many Disaster Recovery Backup storage policies as needed.

When there is no secondary copy using a tape library for the active disaster recovery storage policy, a secondary copy will be automatically created when you configure a tape library. Also, an automatic auxiliary copy schedule will be created, which will run every 15 minutes.

By default, the retention period for Disaster Recovery Backup data is set to be retained for 60 days and 60 cycles. If you want to change the retention time for Disaster Recovery Backup data, it is recommended that you keep the default setting as the minimum with predefined extended retention rules defined as: weekly = 180 days, and monthly = infinite.

For more information, see Disaster Recovery Backup.

DATA AGING AND STORAGE POLICY TIME ZONES

Storage policies, and all subsequent storage policy copies, automatically inherit the CommServe's defined time zone. This impacts when data aging jobs are pruned, as jobs are retained until the specified date and time specified in the storage policy.

If your environment has a storage policy for clients in a different time zone than the CommServe, you should define a specific time zone for the storage policy to prune data in the appropriate time zone.

If you have a storage policy impacting multiple clients in different time zones, you can prune jobs according to each client computer's time zone.

You can designate the following time zones for a storage policy; they are:

- CommServe's Time Zone (default setting)
- Client Computers' Time Zones
- Storage Policy Time Zone

Changing the designated time zone for an active storage policy can pose potential problems for your environment. Data aging operations prune data according to the time zone of the associated storage policy. Changing the time zone can cause a data aging job to prune data at an earlier or later time.

For example, a storage policy's designated time zone is defined as Eastern Standard Time (US and Canada), and several backup jobs are set to be pruned on October 31st. If the storage policy's time zone is changed to Eastern Standard Time (Australia), the jobs will still be pruned on October 31st; however, they will be pruned a day earlier.

As such, changing the time zone of a storage policy is recommended only for advanced users, due to the potential loss of data and environmental impact.

For step-by-step instructions, see Designate a Time Zone for a Storage Policy.

STORAGE POLICY OPERATIONS

Storage policy operations allow you various options for customization and maintenance. These include features such as optimizing tape speeds, verifying data validity for restoring and copying, and ensuring alternate data paths.

Various storage policy operations dealing with creation and maintenance are available in the CommCell Browser at the storage policy level. These options are discussed below.

CREATE A STORAGE POLICY

You can create a storage policy in the CommCell Console from the Storage Policy level. A Storage Policy Wizard guides you through the process of creating a storage policy. By default, the primary copy gets created when a new storage policy is created.

CREATE A SECONDARY COPY

When a storage policy is created, the software automatically creates a primary copy. All data from data protection operations from the subclient(s) is channeled through the primary copy.

In addition, you can create any number of additional secondary copies to the same/different libraries and MediaAgents. These copies are components of storage policies and are used in auxiliary copy operations, and can either be synchronous or selective. For more information about storage policy copies, see Storage Policy Copies.

PERFORM AN AUXILIARY COPY OPERATION

During an Auxiliary Copy operation, data is copied from the primary copy to the secondary (synchronous or selective) copies that you have defined.

DATA VERIFICATION

You can configure a copy for Data Verification so that all backups, all full backups, or backups occurring on or after a certain date will be verified during a data verification operation.

CLONING

The Cloning Policies feature allows you duplicate a storage policy that retains all of the options of the original storage policy. A cloned storage policy is identical to the original policy, except it does not retain the original associated subclients. See Cloning Policies for an overview.

DELETE

You may decide to delete a storage policy if:

- You determine that you do not need the data that was backed up through that storage policy.
- Data no longer exists on the storage policy and you have no plans to use it for future data protection operations.

VIEW MEDIA NOT COPIED

You can view the media that has data that has not yet been copied to all secondary copies within a storage policy. This will help you determine which media are required for operations, and how much data must be copied.

This media can be viewed from the Media Not Copied dialog box.

VIEW JOBS

You can view and perform operations on the jobs that reside on, or are scheduled to be copied to, a storage policy copy. For more information on the **View Jobs** feature, see Jobs on a Storage Policy Copy. Selecting the **Advanced** button provides you with additional viewing options, which you can select in the Jobs in Storage Policy Advanced Filter Options dialog box. From here, you can view jobs based on:

- content indexing status
- availability
- aged data

Results will display in the Job for Storage Policy Copy window.

SCHEDULES

You can view the schedules of jobs associated with a storage policy copy. For more information, see Scheduling.

CONTENT INDEXING

You can configure and run content indexing operations. For more information, see Content Indexing.

BEST PRACTICES**LIMIT THE NUMBER OF STORAGE POLICIES IN YOUR COMMCELL ENVIRONMENT**

When you create a subclient, you must associate that subclient with a storage policy. The associated storage policy enables the data protection/archive operations and recovery/retrieve operations to be conducted for the subclient's data. When the data stored on media meets its retention criteria and data aging is run, the data is logically deleted (i.e., removed from the CommServe database). If all of the data on a media is pruned, the media is recycled. That is, it is returned to the scratch pool that is currently associated with the storage policy copy containing the media.

It is good practice to limit the number of storage policies in your CommCell environment; this will better utilize your media since media cannot be shared across storage policies. Limiting the number of storage policies means using less media to store your data. Whereas having many storage policies in your environment would utilize much more media to store the same amount of data.

If you currently have many storage policies in your environment, you can consolidate your storage policies by following these steps:

1. Identify a storage policy or create a new storage policy for the purposes of consolidating all of your storage policies. For step-by-step instructions, refer to Create a Storage Policy.
2. Select the subclients to be associated to the storage policy designated for the purposes of consolidation. For step-by-step instructions, refer to Associate Multiple Subclients to a Storage Policy.
3. Rename those storage policies that are no longer associated with subclients. The new name should include a phrase indicating that the storage policy is no longer in use, e.g., "storage_policy_1" should be renamed as "storage_policy_1_old".

CAUTION

Do not delete the storage policies that are no longer being used. Deletion of a storage policy prior to all data being aged from the associated media will lead to a loss of data.

There are several things to consider when reassigning subclient storage policy associations, refer to Considerations: Subclients.

DISABLE ADDITIONAL SUBCLIENT ASSOCIATIONS WITH A STORAGE POLICY

If a storage policy is inactive, it is not recommended that it be deleted due to a potential loss of data if the deletion of the storage policy occurs prior to all the data being aged from the associated media. It is best to disable it for additional subclient associations to prevent new backup operations from running to that storage policy. For more information, see Disable/Enable Additional Subclient Associations for a Storage Policy. Note that when a storage policy is marked as disabled for subclient associations, the storage policy will not be listed as available when creating or editing the associations of a subclient. The subclient will also not be available for association when a new client is being installed to the CommServe, which has a disabled storage policy.

If a Storage Policy is marked as disabled for subclient associations, you have the ability to hide these storage policies by enabling the **Do not show storage policies disabled for subclient association** parameter in Media Management Configuration.

To hide the storage policies disabled for subclient association:

1. From the CommCell Browser, right-click the CommServe icon, and select **Control Panel** and **Media Management**.
2. From the Media Management Configuration (Service Configuration) dialog box, select a parameter and change the **Value** field.

3. Click **OK**.

PASSWORD PROTECT THE MEDIA ASSOCIATED WITH A STORAGE POLICY

The storage policy level media password is used to prevent unauthorized access to the data residing on media used by the system for a storage policy. If not enabled, the CommServe Level Media Password is the default password. To see how to enable this feature, see Password Protect the Media of a Storage Policy.

If you choose to password protect your media, it is essential that you record this password. In certain disaster recovery scenarios, it may be necessary to read your backup data directly from the backup media (using Media Explorer, for example). This password will be required to directly access the media.

HIDING STORAGE POLICIES

There are two ways to hide storage policies. You can hide inactive storage policies or you can use permissions to hide specific storage policies from specific users.

HIDE INACTIVE STORAGE POLICIES

Inactive storage policies can be hidden from the CommCell Console to simplify management, report generation, and reduce overall clutter in large configurations. Storage policies with infinite or long-term retention can be hidden using this feature, which reduces the risk of accidentally removing important information. To see how to use this feature, see Hide Inactive Storage Policies.

Once a storage policy is hidden, you cannot associate it with a subclient. Additionally, you cannot hide a storage policy if any subclients are associated with it. If you try to hide a storage policy with one or more associated subclients, an error message displays, stating to re-associate the subclients before hiding it.

You can choose to disable the hiding of storage policies through the Service Configuration tab of the Media Management Configuration Control Panel.

HIDING STORAGE POLICIES BASED ON USER PERMISSIONS

You can determine which storage policies are available to specific groups using user permissions. This allows you to simplify management, report generation, and reduce overall clutter in large configurations. To see how to use this feature, see Hide Storage Policies Based on User Permissions.

CONSIDERATIONS

- It is recommended that you do not change any of the storage policy properties while the storage policy is being used by an operation. (e.g., data protection operation, data recovery operation, data aging, auxiliary copy, synthetic full, etc.)
- A storage policy cannot be deleted if there are any data aging, data recovery operations, or auxiliary copy jobs running on the storage policy.
- If a Storage Policy was changed without converting the next backup operation to a full backup, data aging operations will not age the data after the last full backup until:
 - a new full backup operation is run on the subclient for which the storage policy changed
 - it has met its retention criteria.

NAS-ATTACHED LIBRARIES AND DRIVE POOLS

In an environment with NAS file servers, consider the following when creating and using storage policies:

- Data can be backed up to a library directly attached to a NAS file server; however, a NAS client of one type (e.g., NetApp, Celerra, etc.) should never use a storage policy with a data path pointing to a library directly attached to a NAS file server of another type.
- If the default data path on the primary copy of a storage policy points to a drive pool attached to a NAS file server, then all additional data paths on the primary copy or any other copy must also point to a drive pool attached to the same type of NAS file server.
- For Storage Policies utilizing a drive pool directly attached to a NAS file server, any MediaAgent specified in a data path must have connectivity to that NAS file server.
- If the default data path on the primary copy of a storage policy points to a drive pool configured on a MediaAgent, then all additional data paths on the primary copy or any other copy must also point to a drive pool configured on a MediaAgent. If NDMP Remote Server (NRS) is installed on the MediaAgent in the default data path, then NRS must also be installed on the MediaAgent specified in any additional data paths.
- Data from any Agent can be backed up to a library attached to a NAS file server, by selecting a Storage Policy for a NAS-attached library. All copies of the Storage Policy must utilize the NAS-attached library.
- Tapes written to by the file server to a NAS attached tape drive cannot be migrated to a MA attached library and then read for a restore. Even if the NDMP Remote Server is installed on the MediaAgent, the tape written to directly by the file server cannot be read by the MediaAgent.

NAS CLIENTS

- For all NAS clients, data can be backed up through a MediaAgent on which you have installed NDMP Remote Server (NRS). When creating or selecting a storage policy for use with NRS, ensure the specified MediaAgent has a Drive Pool configured, and all requisite software installed and configured for the NAS iDataAgent. Such storage policies will be available for use by the subclient, when you Associate a Subclient to a Storage Policy. The data protection and recovery jobs will run on the MediaAgent where the selected drive pool for that job is configured.
- NAS Load-Balancing - The Drive Pools, Storage Policies, and Subclients for NAS can be configured so that backup, restore, and auxiliary copy jobs will be

spread among different MediaAgent, and thus the processor load for these jobs will occur on different machines. For more information, see Advanced - NAS iDataAgent Configuration.

SUBCLIENTS

- Whenever you create a subclient, you must associate that subclient with a data storage policy. The associated storage policy is the one through which data protection/archive operations and recovery/retrieve operations for the selected subclient are conducted. Some agents may also have a separate storage policy association for transaction logs.
- You must re-associate the subclients of a storage policy if you want to delete it. You can re-associate all the subclients of a storage policy at the same time.
- Re-associating the subclients of a storage policy automatically forces the next backup to be a full backup.
- When a user changes the storage policy association of a subclient, a subclient is deleted, or a client or an agent is deleted, only the retention days must be exceeded for data to be aged. In these cases, retention cycles are set to zero (0). However, when a client or an agent is deconfigured, the associated data will be aged according to the associated storage policy copy's defined retention time and cycle rules. In this case, retention cycles are honored. If necessary, you can enable the **Ignore Cycles Retention on De-Configured Clients** option from the control panel's Media Management Configuration (Service Configuration) dialog box so that the defined retention cycle rules are ignored for the data associated with deconfigured clients.
- If you plan to change the associated data storage policy of a subclient that has been backed up/archived, keep in mind the following considerations:
 - Verify that the retention period of the primary copy of the target storage policy satisfies your requirements. If necessary, either change the retention period of the primary copy or create a new storage policy with a primary copy that has the desired retention period.
 - When assessing retention periods, be particularly careful in the case of multiple subclients. To maintain consistency, we recommend that the data for all subclients within an agent/backup set/instance/database/partition expire at the same time. Therefore, if you change storage policy associations, you should keep in mind the retention periods of any sibling subclient data as well.
 - For the Image Level iDataAgent, if you have assigned volumes from a single database to multiple subclients, all of those subclients should have the same retention period.
 - The data that was backed up/archived through the previous storage policy remains valid for the length of time expressed in the associated retention period. Since the data remains valid, you can still recover/retrieve it if necessary.
 - All subclient data that was backed up through the previous storage policy will be aged based on its storage policy copy retention time (days) rule only. If you select to run a full backup after changing the storage policy, all subclient data on the new storage policy will be aged according to its retention time and cycle rules. If you select to run a non-full backup as the next backup operation, it is recommended that you run a full backup as soon as possible. All non-full backups run before a full backup will be retained as a partial cycle according to the new storage policy copy's retention cycle rule (even though not a full cycle). The non-full backups (partial cycle) will be aged when the new storage policy copy's retention time and cycle rules are met.

For more information, see Data Aging.

- For most iDataAgents, the user is given a choice whether or not to automatically convert the next backup of that subclient into a full backup. However, for DataArchiver Agents, the system automatically converts the next operation for that subclient into a new index job. You may want to verify that this does not result in conflicts with any operation rules that have been established.
- It is not possible to change a storage policy association for a subclient that is being backed up/archived. If the subclient is newly established and has no data protection/archive history, then you can change the associated storage policy.
- Oracle and Oracle RAC subclients use two storage policies, one for data which is set at the subclient level, and one for Archive Logs which is set at the instance level.
- For Informix subclients, you can specify the maximum number of streams used for database backup operations by setting the BAR_MAX_BACKUP parameter in the \$ONCONFIG file on the Informix client. Also, the number of streams specified by the storage policy must be greater than or equal to the number specified by the BAR_MAX_BACKUP parameter.
- For NAS subclients, you can select a Storage Policy associated with either of the following:
 - drives configured on a MediaAgent with the following installed:
 - NDMP Remote Server
 - File System iDataAgent
 - drives configured on a NAS file server
- For NAS subclients using NRS, there are specific considerations for storage policies to be used. For more information, see NAS Clients.
- For Image Level subclients, the Storage Policy must reside on the client where the snapshot command will be executed.
- For SQL Server subclients:
 - System database subclients only use one storage policy.
 - Non-system database user-defined subclients can use two storage policies:
 - one for full and differential database backups
 - one for the storage policy's own Incremental backup.
 - Non-system database default subclients can use up to three different storage policies:
 - one for full and differential database backups

- one for the storage policy's own Incremental backup
- one for transaction log backups.
- Changing the associated transaction log storage policy does not require conversion to a full backup.
- If you are using the auxiliary copy feature of combining streams, the **Number of Transaction Log Backup Streams** must be set to one.

INCREMENTAL STORAGE POLICY

- You cannot enable a storage policy as an incremental storage policy if that storage policy already has an incremental storage policy enabled.
- The incremental storage policy option is available for a Standard storage policy.
- If you are using a different MediaAgent for an incremental storage policy than the MediaAgent used for a full storage policy, one of the following conditions must be met:
 - The primary copies of both this storage policy and the selected incremental storage policy use a shared index cache.
 - The primary copies of both this storage policy and the selected incremental storage policy are set to use preferred data paths.
 - If it is a case of failover/round robin, the primary copies of both this storage policy and the selected incremental storage policy must have the same data paths.
- An incremental storage policy must be de-associated from a storage policy before that storage policy can be deleted.
- If an incremental storage policy is de-associated from a storage policy, the most recent incremental backup may be pruned before the next full backup occurs.
- If you want to perform a synthetic full backup using an alternate MediaAgent (one other than the MediaAgent used for the Primary backup), you must configure an Incremental Storage Policy.

DELETING A STORAGE POLICY

- A Storage Policy can only be deleted if it is not associated with any subclients.
- When a storage policy is deleted, all the data from data protection operations associated with the storage policy is removed from the CommServe database. Thus, once a storage policy is deleted, the data from data protection operations associated with the storage policy cannot be restored/recovered.
- Data backed up/archived using this storage policy will not be available for data recovery operations. The storage policy will be deleted even if disk volumes are not accessible.
- Verify that you will no longer need the data that was backed up/archived using the storage policy, and verify that the storage policy will not be needed for future data protection operations before deleting a storage policy.

DISASTER RECOVERY BACKUP STORAGE POLICY

- A Disaster Recovery Backup storage policy cannot be deleted if there are any data aging, data recovery operations, or auxiliary copy jobs running on this storage policy.
- It is recommended that you do not delete a Disaster Recovery Backup storage policy before exporting the media containing your Disaster Recovery Backups. If you delete a Disaster Recovery Backup storage policy before exporting this media, the media may be used by another data protection operation and it can be overwritten. Once the media is exported, you can use Media Explorer to restore the metadata from this media.

SYNCHRONOUS COPIES

- It is recommended that synchronous copies be configured with a retention period that is greater than or equal to that of the primary copy.
- Synchronous copies should be configured using the same number of data streams as the primary, unless that secondary copy has the `Combined to <n> Streams` option enabled.

SELECTIVE COPIES

- It is recommended that selective copies are configured with a retention period that is greater than or equal to that of the primary copy.
- Selective copies should be configured using the same number of data streams as the primary, unless the copy has the **Combined to <n> Streams** option enabled.
- For Oracle and Oracle RAC, selective copies are supported for Selective Online Full and Offline Full operations only.

DATA STREAMS

- The number of data streams is the same for all the copies in the storage policy; hence the number of data streams cannot be changed for individual copies. Only copies with the **Combined to <n> Streams** option can be changed.
- You can change the number of data streams if the storage policy does not have any data protection operation data associated with it. However, you cannot decrease the number of streams for a storage policy that contains data associated with a subclient that supports multiple streams, e.g., a subclient associated with SQL iDataAgent, and the number of streams defined in the subclient properties are more than the number you are modifying. This will prompt an error.

AUDIT TRAIL

Operations performed with this feature are recorded in the Audit Trail. See Audit Trail for more information.

RELATED REPORTS

STORAGE POLICY REPORT

The Storage Policy Report provides information about the storage policies and associated subclients based on the selected filter criteria.

[Back to Top](#)

Storage Policies - How To

[Topics](#) | [How To](#) | [How Do I](#) | [Support](#) | [Related Topics](#)

- [Allow Erase Data in Storage Policy](#)
 - [Associate a Subclient to a Storage Policy](#)
 - [Associate Multiple Subclients to a Storage Policy](#)
 - [Change the Copy Precedence](#)
 - [Change the Maximum Number of Streams](#)
 - [Change the Name of a Storage Policy](#)
 - [Create a Selective Copy](#)
 - [Create a Storage Policy](#)
 - [Create a Synchronous Copy](#)
 - [Delete a Disaster Recovery Backup Storage Policy](#)
 - [Delete a Storage Policy that has an Incremental Storage Policy Enabled](#)
 - [Delete a Standard Storage Policy](#)
 - [Designate a Time Zone for a Storage Policy](#)
 - [Disable an Incremental Storage Policy from a Storage Policy](#)
 - [Enable an Incremental Storage Policy](#)
 - [Enable/Disable Stream Randomization](#)
 - [Tune Stream Randomization](#)
 - [Migrate a Disk Library](#)
 - [Password Protect the Media of a Storage Policy](#)
 - [Re-associate the Subclients of a Storage Policy](#)
 - [Start an Auxiliary Copy](#)
 - [View the Jobs Scheduled For a Storage Policy](#)
 - [View/Edit a Storage Policy](#)
 - [Disable/Enable Additional Subclient Associations for a Storage Policy](#)
 - [Hide Inactive Storage Policy](#)
 - [Hiding Storage Policies based on User Permissions](#)
-

ALLOW ERASE DATA IN STORAGE POLICY

Before You Begin

- An Erase Data license must exist.

Required Capability: See Capabilities and Permitted Actions

▶ To assign a storage policy for erasing data:

1. From the CommCell Browser, right-click the storage policy you want to allow for the erasing of data, then click **Properties**.
 2. From the (General) tab of the **Storage Policy Properties** dialog box, select the **Allow Erase Data** check box.
 3. Click **OK**.
-

ASSOCIATE A SUBCLIENT TO A STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

▶ To associate a subclient to a storage policy:

1. From the CommCell Browser, right-click the subclient whose associated storage policy you want to change, then click **Properties** from the shortcut menu.
 2. Click the Storage Device tab of the Subclient Properties dialog box.
 3. From the **Storage Policy** list of the **Data Storage Policy** tab, select a data storage policy to associate with this subclient. If necessary, click the **Create Storage Policy** button to create a new storage policy to which the subclient can then be associated.
 4. From the Changing a Storage Policy window select the next type of backup operation. Click **OK**.
 5. If applicable for your agent, you can change the number of data streams from the **Number of Data/Database Backup Streams** field.
 6. If applicable for your agent, click the **Log Storage Policy** tab and select a storage policy to associate with this transaction log subclient from the **Transaction Log Storage Policy** list. Also, you can set the **Number of Transaction Log Backup Streams** from this tab.
 7. Click **OK** to save your changes and close the Subclient Properties Storage Device tab.
-

ASSOCIATE MULTIPLE SUBCLIENTS TO A STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

▶ To associate multiple subclients to a storage policy:

1. From the CommCell Browser, right-click on the **Storage Policy** node, and select the **Associate Subclients** option.
 2. From the **Subclient Association with Storage Policy** window, select (highlight) the subclients to be associated or re-associated to a storage policy.
 3. Select the storage policy from the **Change all selected Storage Policies to** drop-down menu. All selected (highlighted) subclients will be associated to this storage policy.
 4. Click **OK** to save your changes.
-

CHANGE THE COPY PRECEDENCE

Required Capability: See Capabilities and Permitted Actions

▶ To change the copy precedence of a storage policy copy:

1. From the CommCell Browser, right click the storage policy whose copy precedence you want to change, and then click **Properties**.
 2. From the Copy Precedence tab of the **Storage Policy Properties** dialog box, select a synchronous or selective copy and click the arrow buttons to change its copy precedence. The arrows will move a copy to a higher or lower precedence in increments of 1. For more information, see Recovering Data From Copies.
 3. Click **OK**.
-

CHANGE THE MAXIMUM NUMBER OF DATA STREAMS

Required Capability: See Capabilities and Permitted Actions

▶ To change the maximum number of data streams:

1. From the CommCell Browser, right click the storage policy whose quantity of data streams you want to change, and then click **Properties**.
2. From the General tab of the **Storage Policy Properties** dialog box, type the number of data streams that you want to allocate for the storage policy in the **Device Streams** field.

3. Click **OK** to save your changes.

CHANGE THE NAME OF A STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

▶ To rename a storage policy:

1. From the CommCell Browser, right click the storage policy that you want to rename, and then click **Properties**.
2. From the General tab of the **Storage Policy Properties** dialog box, type the new name (up to 32 characters) in the **Storage Policy Name** field.
3. Click **OK** to save your changes.

CREATE A SELECTIVE COPY

Required Capability: See Capabilities and Permitted Actions

▶ To create a selective copy:

1. From the CommCell Browser, right-click the storage policy for which you wish to create the secondary copy, click **All Tasks** and then click **Create New Copy**.
2. From the General tab of the **Copy Properties** dialog box:
 - Enter the copy name in the **Copy Name** box.
 - Select the **Combine to <n> Streams** check box if you want to combine data streams during an auxiliary copy operation on this copy.
 - Deselect the **Active** check box if you want to specify that this should be an inactive copy.
 - Select the library, MediaAgent, drive pool, and the scratch pool from the lists (drive pool and scratch pool are not applicable to disk libraries).
 - Select the **Selective Copy** check box. The **Selective Copy** tab is enabled.
3. Select a standard or custom calendar from the **Calendar for Selective Copy and Extended Retention** drop-down list. Note that this option is only available if a custom calendar was created.
4. From the Retention tab of the **Copy Properties** dialog box:
 - Click the **Enable data aging** checkbox, to enable or disable Data Aging on this copy.
 - Click the **Enable Managed Disk Space for disk data**, to enable or disable Managed Disk Space.
 - Change the retention time and retention cycles of the Basic Retention Rules from their default settings of infinite, if needed.
 - Change the Extended Retention Rules, if necessary.
5. Click the Copy Policy tab of the **Copy Properties** dialog box:
 - Choose a date from the **Backups On And After** field. This date can be on, before, or after the current CommServe date. When the date entered is after the current CommServe date, jobs that are to be copied, as well as partially copied jobs will be disabled for a copy. If no date is entered, all backup data will be copied from the primary copy to the secondary copy.
 - Click the **Specify source for Auxiliary Copy** check box if you wish to copy data from a copy other than the primary copy.

The **All Backups** option is not available for selective copies; therefore, you must choose a date from the **Backups On And After** field.
6. Click the Selective Copy tab.
 - Select **Automatically select Full Backups** (all fulls) to automatically copy all full backups regardless of time.
 - Select **Automatically select Full Backups** (daily, weekly, monthly, quarterly, half yearly, or yearly) for the copy to be time-based. If the copy is time based, you can select one of the following options:
 - **First full backup**
 - **Last full backup** (which is based on the following two options):
 - **Select most recent job if there are no more full backup schedules in current time period**
Specifies that the last full backup of the specified time period will be copied from the source copy to this copy if there are no future full backup schedules within the same time period.
 - **Wait until the current time period is over before selecting a backup for this time period**
Specifies that, after the end of the specified time period, the last full backup during that time will be copied from the source copy to this copy. Note that this option is not enabled if the source of the selective copy is a Primary Copy that is defined with zero cycle retention or configured as a spool copy; this is because jobs can be aged immediately after they are copied to synchronous copies, which is before the current time period ends.

- Select **Automatically select Full Backups** (Advanced) to copy all full backups based on the advanced backup frequency options.
 - Select **Every [x] Cycle(s)**, to copy full backup after the specified number of cycles.
 - Select **Every [x] Day(s)**, to copy full backup after the specified number of days.
 - Select **Every [x] Week(s)**, to copy full backup after the specified number of weeks.
 - Select **Every [x] Month(s)**, to copy full backup after the specified number of months.
 - Select **Do not Automatically select jobs** so no backups will be copied to this copy unless they are manually selected for copy from the Job for Storage Policy Copy dialog box or the **Select most recent full backup when auxiliary copy starts** option has been selected from the Auxiliary Copy Options dialog box.
7. If there are no auxiliary copy schedules defined for all copies of the storage policy, you are asked to confirm if you would like to schedule auxiliary copy operations for this copy. Select **Default Schedule**, if you would like an auxiliary copy operation to be scheduled to be run daily at 8:00 A.M., select **Custom Schedule** if you would like to define a schedule, select **Automatic Schedule** if you would like an Automatic Copy to run every 30 minutes, or select **Do Not Schedule**. Click **Yes** if you would like to run or schedule this job. Click **OK**.

CREATE A STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

▶ To create a storage policy:

1. From the CommCell Browser, right-click the Storage Policies node, and select New Storage Policy from the shortcut menu.
2. Follow the prompts displayed in the Storage Policy Wizard to configure the following:
 - Type of Storage Policy: Backup, Compliance Archiver or Disaster Recovery Backup
 - Name of Storage Policy (and Incremental Storage Policy, if selected)
 - Name of the Primary Copy
 - Name of the default library to which the Primary Copy should be associated
 - Name of the MediaAgent
 - Stream and Retention Configuration (default is infinite)
 - Designate Primary Copy for Deduplication: Yes or No. Also, select the Deduplication Type: Block Level or Object Level.

If you wish to enable deduplication at the source, select the Enable Client Side Deduplication option.

If you select No, you cannot enable deduplication on the primary copy at a later time. However, you can enable deduplication on the secondary copies during creation. See Enable Deduplication in a Secondary Copy for details.

 - Name of the Deduplication Store, MediaAgent for Deduplication Store access, and location of the Deduplication Database. If you wish to create a new deduplication store for the Storage Policy, then select Create New Deduplication Store and provide the location of the store. If you wish to deduplicate against an existing deduplication store from a different Storage Policy, then select Use Existing Deduplication Store and select the desired deduplication store from the list. Note that the deduplication database must be located in a folder and not directly under the root of a disk volume.
3. The **Review Summary** window is displayed. Review your selections and then click **Cancel**, **Back** (to return to a previous window to change a selection), or **Finish** (to exit and create the storage policy).

CREATE A SYNCHRONOUS COPY

Required Capability: See Capabilities and Permitted Actions

▶ To create a synchronous copy:

1. From the CommCell Browser, right-click the storage policy for which you wish to create the secondary copy, click **All Tasks** and then click **Create New Copy**.
2. From the General tab of the Copy Properties dialog box:
 - Select the **Combine to <n> Streams** check box if you want to combine data streams during an auxiliary copy operation on this copy.
 - De-select the **Active** check box if you want to specify that this should be an inactive copy.
 - Enable **Inline Copy** for data to be backed up to this copy in addition to the primary copy.
 - Select **Do Not Make Inline Copy to Same Library** to prevent a job from being copied to the same library during Inline Copy operations.
 - Enable **Parallel Copy** for data to be copied to multiple secondary copies concurrently rather than sequentially.
 - Select the library, MediaAgent, master drive pool and scratch pool from the lists (not applicable for disk libraries).
3. From the Retention tab of the Copy Properties dialog box:

- Click the **Enable data aging** checkbox, to enable or disable Data Aging on this copy.
 - Click the **Enable Managed Disk Space for disk data**, to enable or disable Managed Disk Space.
 - Change the retention time and retention cycles of the Basic Retention Rules from their default settings of infinite, if needed.
 - Change the Extended Retention Rules, if necessary.
4. Click the Copy Policy tab of the `Copy Properties` dialog box:
- Choose a date from the **Backups On And After** field. This date can be on, before, or after the current CommServe date. When the date entered is after the current CommServe date, jobs that are to be copied, as well as partially copied jobs will be disabled for copy. If no date is entered, all backup data will be copied from the primary copy to the secondary copy.
 - Click the **Specify source for Auxiliary Copy** check box if you wish to copy data from a copy other than the primary copy.
- The **All Backups** option is not available for selective copies; therefore, you must choose a date from the **Backups On And After** field.
5. Click **OK** to save your changes.
6. If there are no auxiliary copy schedules defined for all copies of the storage policy, you are asked to confirm if you would like to schedule auxiliary copy operations for this copy. Select **Default Schedule**, if you would like an auxiliary copy operation to be scheduled to be run daily at 8:00 A.M., select **Custom Schedule** if you would like to define a schedule, select **Automatic Schedule** if you would like a Automatic Copy to run every 30 minutes, or select **Do Not Schedule**. Click **Yes** if you would like to run or schedule this job. Click **OK**.

DELETE A DISASTER RECOVERY BACKUP STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

Before you Begin

Create a new Disaster Recovery storage policy — a CommCell must have at least one Disaster Recovery storage policy. If you wish to deconfigure the mount path to reclaim the space, use a different library for the new storage policy.

▶ To delete a Disaster Recovery Backup storage policy:

1. From the CommCell Browser, right-click the CommServe icon, click **Control Panel**, and select **DR Backup Settings**.
2. From the **DR Backup Settings (Export Settings)** dialog box, in the **Back Up Metadata to this DR Storage Policy** dropdown list, select the newly-created storage policy.
3. From the CommCell Browser, select the Storage Policies parent node to view the property details of all the storage policies displayed in the right-hand windowpane. Check the **Disable Subclient Association** checkbox for the Storage Policy for which you want to delete.
4. From the CommCell Browser, right-click the Disaster Recovery Backup storage policy that you want to delete, click **All Tasks** and then click **Delete**.
5. A warning dialog box will display indicating that this policy is the active target of disaster recovery backups and a new target should be specified prior to deletion. Click **Continue**.

If your Disaster Recovery Backup storage policy is defined in such a way that it is backing up to a removable media, a dialog box displays with a selection to export media. Note that you will not be prompted to export media if your Disaster Recovery Backup storage policy backs up data to disk media.
6. If you choose to export media, from the **Export Media (Delete Storage Policy)** dialog box, select the media to be exported and click **OK**.
7. Type an outside storage location in the **Export Media** dialog box and click **Export**. Click **OK** to the message displayed. For more information on exporting media, see Exporting a Specific Media.
8. You can continue to export the existing media or choose to continue with the deletion.
9. After clicking **Continue**, the Disaster Recovery Backup storage policy is deleted.
10. If you chose to delete the storage policy without exporting media, you are prompted to confirm that you want to delete the storage policy. Click **OK**. The Disaster Recovery Backup storage policy is deleted. The associated mount path can then be deconfigured.

DELETE A STORAGE POLICY THAT HAS AN INCREMENTAL STORAGE POLICY ENABLED

Required Capability: See Capabilities and Permitted Actions

▶ To delete a storage policy that has an incremental storage policy enabled:

1. From the CommCell Browser, right-click the storage policy you want to delete, then click **Properties**.
2. From the General tab of the **Storage Policy Properties** dialog box, clear the **Incremental Storage Policy** check box.
3. Click **OK** to save your changes.

4. From the **Force Full Backup - Confirmation** dialog box, select either the **Force next backup to be a full (Recommended)** field or the **Do not force** field (if you do not want to force the next backup to be a full backup).
5. Click **OK**.
6. Right-click the storage policy that you want to delete, click **All Tasks** and then click **Delete**.
7. Click **Yes** to the confirmation message.
8. Type **erase and reuse media**. Click **OK**.
9. The selected storage policy is deleted and removed from the CommCell Browser.

If subclients are still associated with the storage policy that you want to delete, an explanatory message is displayed and the delete operation is aborted.

DELETE A STANDARD STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

▶ To delete an iDataAgent Backup or DataArchiver storage policy:

1. From the CommCell Browser, right-click the storage policy that you want to delete, and click **Properties**.
2. Review the **Associated Subclients** tab. If you find any subclients associated to the storage policy, re-associate them using the **Re-Associate** option. Click **OK** to save the changes.

Alternatively, you can disable all subclient association. From the CommCell Browser, select the Storage Policies parent node to view the property details of all the storage policies displayed in the right-hand windowpane. Check the **Disable Subclient Association** checkbox for the Storage Policy for which you want to delete.

3. From the CommCell Browser, right-click the storage policy that you want to delete, click **All Tasks** and then click **Delete** from the short-cut menu.
4. Click **Yes** to the confirmation message.
5. Type **erase and reuse media**. Click **OK**.
6. The selected storage policy is deleted and removed from the CommCell Browser. The associated mount path can then be deconfigured.

If subclients are still associated with the storage policy that you want to delete, an explanatory message is displayed and the delete operation is aborted.

DESIGNATE A TIME ZONE FOR A STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

▶ To designate a time zone for a storage policy:

1. From the CommCell Browser, right-click desired storage policy, and select **Properties**.
2. From the Storage Policy Properties dialog box, click the Advanced tab.
3. Click the Time Zone drop-down list, and select a time zone.
 - **CommServe Time Zone:** Selected by default. Jobs are pruned according to the CommServe designated time zone.
 - **Client Time Zone:** Select to prune jobs according to each associated client computer's designated time zone.
 - **Time Zone:** Select the time zone (e.g., *(UTC) Coordinated Universal Time*) to use to prune jobs.
4. Click **OK** to close the Warning dialog.
5. Click **OK** to close the Storage Policy Properties dialog and save your changes.

Changing the designated time zone for an active storage policy can pose potential problems for your environment. Data aging operations prune data according to the time zone of the associated storage policy. Changing the time zone can cause a data aging job to prune data at an earlier or later time.

For example, a storage policy's designated time zone is defined as Eastern Standard Time (US and Canada), and several backup jobs are set to be pruned on October 31st. If the storage policy's time zone is changed to Eastern Standard Time (Australia), the jobs will still be pruned on October 31st; however, they will be pruned a day earlier.

As such, changing the time zone of a storage policy is recommended only for advanced users, due to the potential loss of data and environmental impact.

DISABLE AN INCREMENTAL STORAGE POLICY FROM A STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

▶ To disable a storage policy that is associated with a full storage policy:

1. From the CommCell Browser, right click the storage policy that you want to disable the incremental storage policy from, then click **Properties**.
 2. From the (General) tab of the **Storage Policy Properties** dialog box, clear the check box.
 3. Click **OK** to save your changes.
 4. From the **Force Full Backup - Confirmation** dialog box, select either the **Force next backup to be a full (Recommended)** field or the **Do not force** field (if you do not want to force the next backup to be a full backup).
 5. Click **OK**.
-

ENABLE AN INCREMENTAL STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

▶ To enable an incremental storage policy:

1. From the CommCell Browser, right click the storage policy that you want to enable an incremental storage policy, then click **Properties**.
 2. From the General tab of the **Storage Policy Properties** dialog box, select a storage policy from the **Incremental Storage Policy** list.
 3. Click **Yes** to the confirmation prompt that the next backup for all subclients for this storage policy will be forced to be a full backup.
 4. From the **Force Full Backup - Confirmation** dialog box, select either the **Force next backup to be a full (Recommended)** field or the **Do not force** field (if you do not want to force the next backup to be a full backup).
 5. Click **OK** to save your changes.
-

ENABLE/DISABLE STREAM RANDOMIZATION

Required Capability: See Capabilities and Permitted Actions

▶ To enable stream randomization:

1. From the CommCell Browser, right click the storage policy for which you want to enable stream randomization, then click **Properties**.
2. From the General tab of the **Storage Policy Properties** dialog box, mark the checkbox for **Enable Stream Randomization**. Note that this field is only enabled when the storage policy is configured to use more than one (1) data stream.
3. Click **OK**.

To disable this feature, deselect the checkbox.

TUNE STREAM RANDOMIZATION

Required Capability: See Capabilities and Permitted Actions

▶ To tune the stream randomization feature:

1. From the **Control Panel**, double-click **Media Management**.
 2. From the **Resource Manager Configuration** tab of the **Media management Configuration** dialog box, perform the following:
 - In the **Interval (in minutes) to calculate valid data size for streams** field specify the interval to calculate the data size for streams.
 - In the **Threshold (in GB) to decide how to distribute data among streams for backup** field specify the threshold to decide data distribution among streams.
 3. Click **OK** to save the changes.
-

MIGRATE A DISK LIBRARY

Required Capability: See Capabilities and Permitted Actions

▶ To perform a disk library migration from one MediaAgent to another MediaAgent:

1. Right-click the disk library that you want to migrate to another MediaAgent and click **Migrate Disk Library**.
2. A message is displayed indicating that this operation migrates the disk library to another MediaAgent. Click **OK**.
3. The Select MediaAgent dialog box is displayed. This dialog box displays the current MediaAgent that the disk library is associated with and allows you to select a MediaAgent to migrate to. From the drop-down list, select the MediaAgent you want to migrate to and click **OK**.
4. The disk library will now be associated with the selected MediaAgent. To view the disk library properties to verify successful migration, right click on the disk library where you want to view the properties, and click **Properties**.

The MediaAgent is displayed on the **General** tab.

5. Make sure that the mount path associated with the disk library, points to valid path. (See Add or Modify Mount Paths for step-by-step instructions.)

PASSWORD PROTECT THE MEDIA OF A STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

▶ To password protect the media of a storage policy:

1. From the CommCell Browser, right click the storage policy for which you wish to password protect the media, and then click **Properties**.
2. From the Advanced tab of the **Storage Policy Properties** dialog box, select the **Enable Storage Policy Level Media Password** option. Note that the media password is used to prevent unauthorized access to the data residing on media used by the system for this storage policy. If not enabled, the CommServe Level Media Password is the default password.
3. Enter the password information accordingly, and click **OK** to save your changes.

RE-ASSOCIATE THE SUBCLIENTS OF A STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

▶ To re-associate the subclients of a storage policy:

1. From the CommCell Browser, right-click the storage policy whose subclients you want to re-associate, and then click **Properties**.
2. Click the Associated Subclients tab of the **Storage Policy Properties** dialog box.
3. Select the subclients, and then click **Re-Associate**.
4. In the Storage Policy List dialog box, from the **Select storage policy to which all the subclients will be associated:** list, select a storage policy you would like to re-associate the subclients to. Click **OK**.

To re-associate the storage policy copy of a DDB Backup subclient, make sure to select non-deduplicated storage policy copy.

5. Click **OK** to save your changes.


START AN AUXILIARY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To start an auxiliary copy:

1. From the CommCell Browser, right-click the storage policy for which you want to perform an auxiliary copy, click **All Tasks**, and then click **Run Auxiliary Copy**.
2. In the **Auxiliary Copy** dialog box, the Storage Policy field is already populated with the name of the Storage Policy you selected.
3. If the source copy is configured with a shared library, select the **Source MediaAgent** for the auxiliary copy.
4. Select **All Copies** to copy data from the source copy to all secondary copies defined, or select a copy from the **Select a Copy** list box.
5. Select **Start new media** to copy the data to a different tape or optical media. On a disk, this option, when selected, creates a new volume folder for the operation.
6. Select the number of streams to copy in parallel from the **Number of Streams to Copy in Parallel** pane, or select **Allow Maximum**.
7. Select **Mark media full after successful operation** to mark the media that is used for this operation full after the auxiliary copy operation has successfully completed.

8. Select **Select Most Recent Full Backup When Auxiliary Copy Starts** to have the most recent successful full backup for each subclient copied when the Auxiliary Copy job is run.
 9. From the Job Initiation tab on the **Auxiliary Copy** dialog box, select the time for this job to run or choose to **Run Immediately**. You can also configure an alert for this job.
 10. Click **Advanced** to configure the **Vault Tracker**, **Startup** and **Job Retry** options.
 - o Click **Vault Tracking** to select additional Vault Tracker options for this operation from the Vault Tracking dialog box.

Note: This option is only available if a Vault Tracker license is available in the CommServe.
 - o Click **Startup** to change the priority of this job and, if necessary, to start this job in a suspended state from the Startup dialog box.
 - o Click the **Job Retry** tab to specify the job running time and the number of job retries. See Restarting Jobs and Job Running Time for more information.
- 

The **Number of Retries** specified for this particular job will only be used by the system if Auxiliary Copy was configured as a **Restartable** job type in the Job Management Control Panel. For procedures, see Specify Job Restartability for the CommCell.
11. Click **OK** to start the auxiliary copy operation. A progress bar displays the progress of the operation.

VIEW THE JOBS SCHEDULED FOR A STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

▶ To view the jobs scheduled for a storage policy:

From the CommCell Browser, right-click the storage policy for which you want to view the jobs scheduled,

click **All Tasks**, and then click **Schedules**. The Scheduled Jobs Dialog dialog box displays the jobs scheduled for this storage policy.

VIEW/EDIT A STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

▶ To view/edit a storage policy:

1. From the CommCell Browser, right click the storage policy that you want to view, and then click **Properties**.
2. From the Storage Properties dialog boxes, you can view/edit the fields as deemed necessary.
3. Click **OK** to save your changes.

You can view basic storage policy property descriptions by clicking on a Storage Policy in the CommCell Browser. The storage policy details are displayed in the right-hand windowpane.

DISABLE/ENABLE ADDITIONAL SUBCLIENT ASSOCIATIONS FOR A STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

▶ To disable additional subclient associations for a a storage policy:

1. From the CommCell Browser, select the **Storage Policies** parent node to view the property details of all the storage policies displayed in the right-hand windowpane.
2. Check the **Disable Subclient Association** checkbox for the Storage Policy for which you want to disable/enable additional subclient associations.

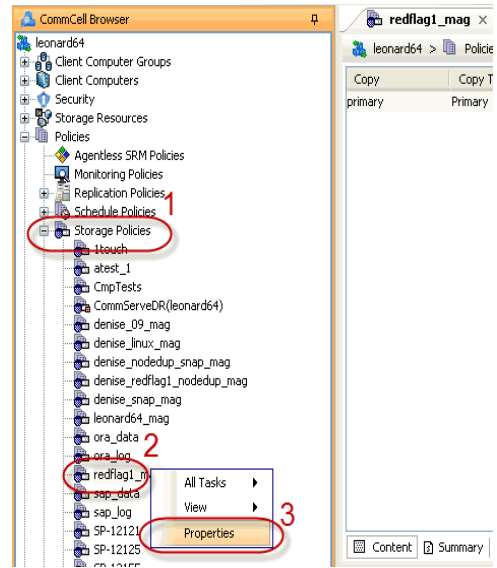
If a storage policy is marked as disabled for subclient associations, the storage policy will not be listed as available when creating/or editing the associations of a subclient. The subclient will also not be available for association when a new client is being installed to the CommServe, which has a disabled storage policy.

HIDE INACTIVE STORAGE POLICIES

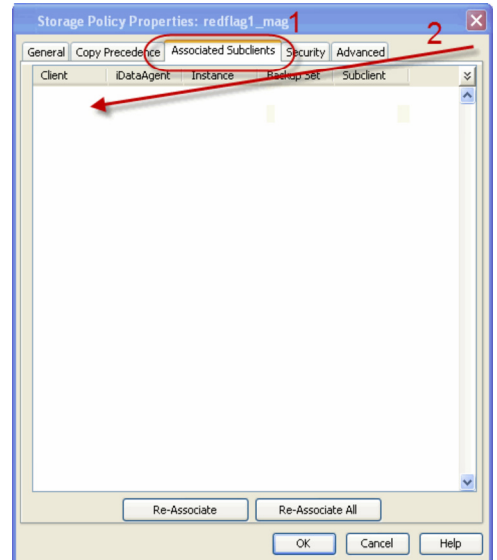
Required Capability: See Capabilities and Permitted Actions

▶ To hide Storage Policies from the CommCell Console:

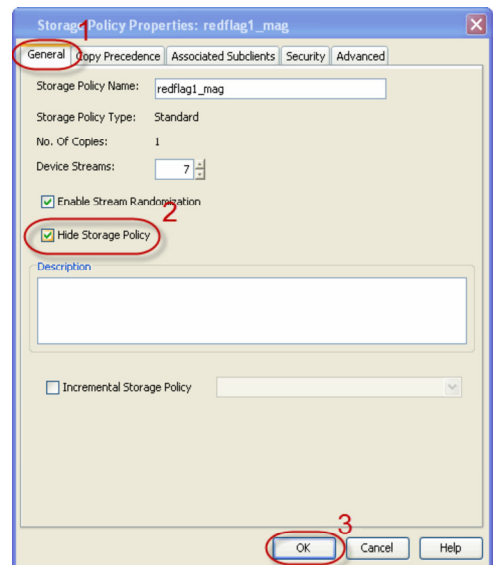
1. Right-click the desired Storage Policy and select **Properties**.



2. Click the **Associated Subclients** tab to ensure that no subclients are associated with the specified storage policy.



3. Click the **General** tab, and select **Hide Storage Policy**.
Click **OK** to save your changes. The storage policy is removed from the CommCell Console.



To display hidden storage policies, open the Media Management Control Panel, and view the Service Configuration

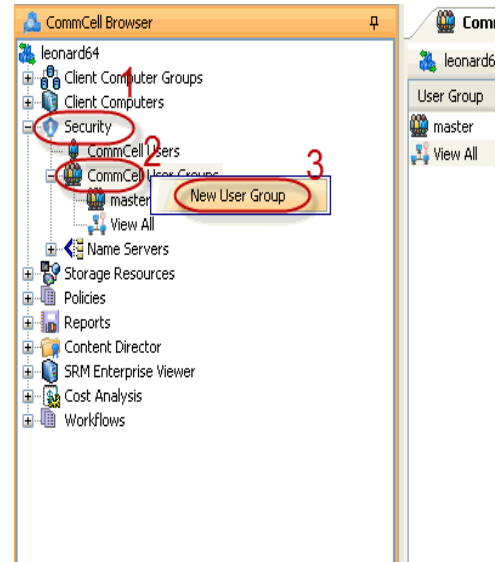
tab. Then, change the value for the **Show hidden storage policies** parameter from 0 to 1.

HIDE STORAGE POLICIES BASED ON USER PERMISSIONS

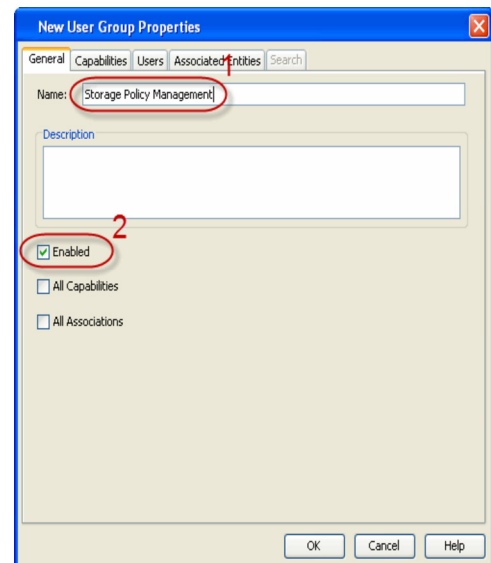
Required Capability: See Capabilities and Permitted Actions

▶ To hide Storage Policies from the CommCell Console:

1. Click **Security** and then right-click **CommCell User Group**, and select **New User Group**. The New User Group Properties dialog displays.

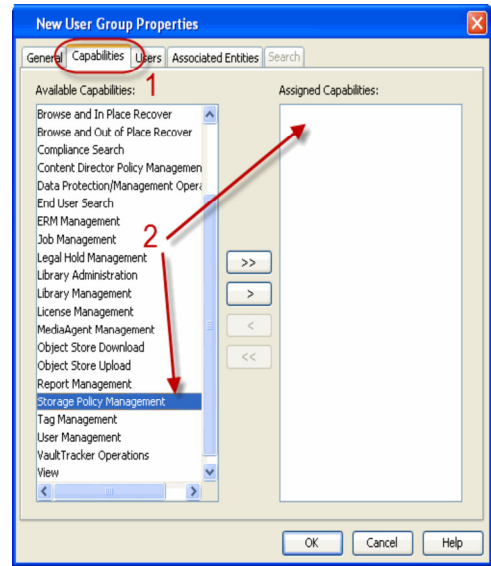


2. Name the group (e.g., Storage Policy Management), and ensure that the **Enabled** checkbox is selected

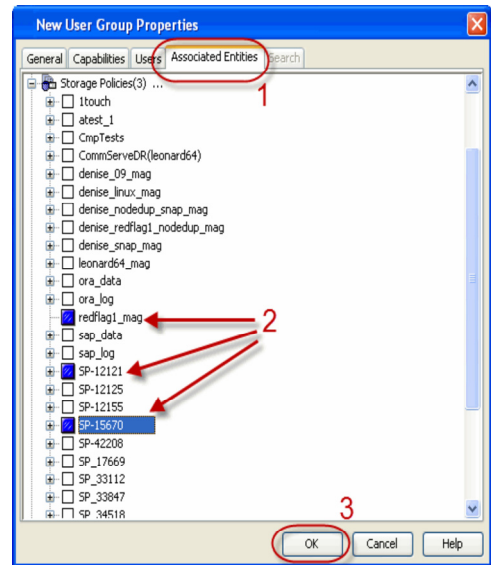
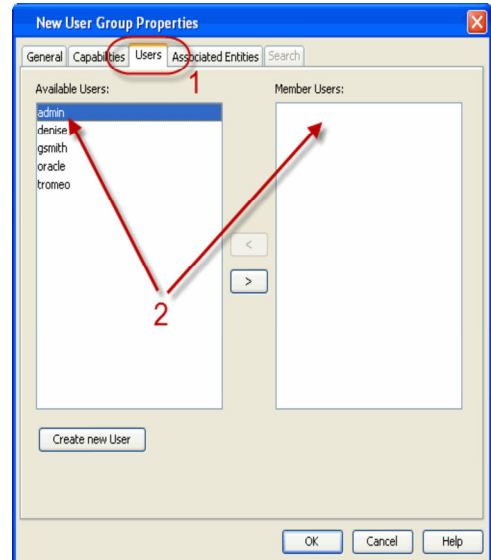


3. Click the **Capabilities** tab. Double-click **Storage Policy Management** to add it to the Assigned Capabilities list.

- Click the **Users** tab. Double-click all applicable users to add them to the Member Users list.



- Click the **Associated Entities** tab. Expand Storage Policies. Select the applicable storage policies.
Click **OK** when finished. When the users log into the commcell only the selected storage policies are displayed.



Back To Top

Storage Policy Copies

[Topics](#) | [How To](#) | [Support](#) | [Related Topics](#)

Overview

- [Primary Copy](#)
- [Secondary Copy](#)
- [WORM Copy](#)
- [Snapshot Copy](#)
- [Supported Copy Types per Storage Policy Type](#)

[Automatic Copy](#)

[Deferred Copy](#)

[Inline Copy](#)

[Jobs on a Storage Policy Copy](#)

[Source Copy](#)

[Spool Copy](#)

[Subclient-Based Storage Policy Copy](#)

[Storage Policy Copies Operations](#)

- [Disk Volume Reconciliation](#)
- [Mark Active Media Full](#)
- [Change Data Path](#)
- [Delete a Storage Policy Copy](#)
- [Schedules](#)
- [View Media Not Copied](#)
- [View Media](#)
- [View Jobs](#)
- [View Aged Media](#)

[Storage Policy Copy Considerations](#)

- [Auxiliary Copy](#)
- [Backups On and After Date](#)
- [Data Path](#)
- [Delete a Storage Policy Copy](#)
- [Disable a Job](#)
- [Hardware Compression](#)
- [Inactive Storage Policy Copy](#)
- [Prune a Job](#)
- [Retain a Job](#)
- [View Retained Jobs](#)
- [Retention Rules](#)
- [Secondary Copy](#)
- [Spool Copy](#)

[Best Practices](#)

- [Managed Disk Space](#)

[Audit Trail](#)

[Storage Policy Copy Properties](#)

[Related Reports](#)

OVERVIEW

A storage policy copy provides the means to make additional copies of the data. Copies can be created by performing an auxiliary copy operation, or by performing a data protection operation that creates Inline copies.

Each storage policy consists of one or more storage policy copies. There are several types of storage policy copies. They are:

PRIMARY COPY

The primary copy is automatically created by the system when a storage policy is created. All data protection operations that use a given storage policy use the primary copy. The primary copy carries all data that is directed to its parent storage policy.

SECONDARY COPY

A secondary copy of a storage policy provides a means of making an additional copy of protected data and is used in auxiliary copy operations, or data protection operations that create inline copies. An auxiliary copy operation or a data protection operation with an inline copy replicates the data that has been protected through the primary copy to the secondary copies within the same storage policy. While a secondary copy can use the same library as the primary, it is recommended that a different library is used for a secondary copy.

When configured, each copy is assigned a set of attributes. These attributes define the nature of the data protection data that is protected and/or copied on a copy. Such attributes include the:

- Destination library of the data secured through the copy
- Data retention rules or all data to be secured through the copy
- Copy precedence
- Copy type (synchronous or selective)

There are two types of secondary copies. They are synchronous copies and a selective copies. The following section describes each.

SYNCHRONOUS COPY

During an auxiliary copy operation or a data protection operation that creates an inline copy, all data protection operations occurring on or after a selected date on the primary copy are copied to a synchronous copy. In case data is lost, you can restore/recover the same data from a synchronous copy. Note that you can promote a synchronous copy to be the primary copy.

SELECTIVE COPY

A selective copy allows you to copy backup data selectively from a source copy to this copy, providing for better tape rotation. Since only selective backups can be copied to selective copies, the selective copies cannot be promoted to the primary copy, only synchronous copies can be promoted. Note that the data selection process does not have to be the same for all auxiliary copies.

During an auxiliary copy operation or a data protection operation that creates an inline copy, only those backups from the primary copy that meet certain criteria will be copied to a selective copy. You can define a selective copy to be time-based, automatically selected, or automatically not selected on the primary copy.

If the copy is defined as All Fulls, all full backups on the primary copy will be copied during an auxiliary copy operation or a data protection operation that creates an inline copy. If the copy is defined as time-based, only the first or last full backup that occurs within each selected weekly, monthly, quarterly, half-yearly, or yearly interval will be copied. You have the option of creating and associating a custom calendar to the copy, so that the intervals can be further customized.

Selective Copy will copy Selective Online Full and Offline Full jobs for Oracle agent and regular Full Jobs which has linked log backups are copied for other database agents like DB2, Sybase etc.

For File System and File System like Agents, the selective copy will copy backup jobs that completed with errors. However, if these jobs are associated with Database Agents, the selective copy will not copy them.

- Backup jobs for some agents are not self contained because they require data from subsequent jobs in order to be successfully restored, and therefore, cannot be copied to selective copies. Since Oracle online and SQL File/File Group (FFG) backup jobs are dependant upon corresponding transaction logs for restorability, their data will not be copied to a selective copy.
- The selection period for a selective copy is determined only by the copy creation time. The **Backups on or After** option in the **Copy Policy** tab does not affect the selection period for a given selective copy because this option is only used to decide which backup job after specified date is qualified to be picked. Also, note that the selection period cannot be manipulated from the CommCell Console.

For more information, see:

- Auxiliary Copy With Synchronous and Selective Copies
- Grandfather-Father-Son (GFS) Tape Rotation

WORM COPY

WORM Copy is an option that prevents the deletion of data that is not qualified for aging. The expiration date for the read-only lock is set to match the data retention time established in the storage policy copies. These archive files cannot be modified or deleted by any user or application until the specified retention date. Once the retention expires, the system deletes the archives as a part of Data Aging.

Once selected and saved for a storage policy copy, the following rules are enabled:

- WORM Copy cannot be cleared.
- Data aging rules cannot be reduced (i.e., made shorter), ensuring that data can not be deleted earlier than expected.
- Data aging rules can be increased (i.e., made longer).

This feature can be enabled from the General tab of the `Copy Properties` dialog box.

Note that, users that are members of **master** user group can change the retention period manually for a specific retained jobs of a Worm copy. See [Manually Modify the Retention of the Retained Jobs for WORM Copy](#) for step-by-step instructions.

SNAPSHOT COPY

A snapshot copy of the storage policy is an additional copy of the protected data which is used in SnapProtect Backup operations. The snapshot copy stores the meta data information related to the SnapProtect backup.

SUPPORTED COPY TYPES PER STORAGE POLICY TYPE

The following table lists the types of **storage policies** and the types of **storage policy copies** that support that storage policy:

Storage Policy Type	Storage Policy Copy Type
Standard	Primary Copy
	Synchronous Copy*
	Selective Copy*
Disaster Recovery Backup	Primary Copy
	Synchronous Copy*

*Can also be designated as an Inline Copy.

STORAGE POLICY COPY OPERATIONS

Storage policy operations allow you various options for media maintenance and data viewing. These include features such as designating media as full, changing data paths for media, deleting storage policy copies, and viewing several media data within the system.

DISK VOLUME RECONCILIATION

Disk volume reconciliation allows you to reconcile the discrepancies in the disk volume associated with a storage policy copy data. This feature compares the physical data located in the disk mount path with the metadata records in the CommServe database and provides the list of orphaned jobs and orphaned media space. Orphaned jobs are jobs without corresponding data on the media, and orphaned media is the list of volumes without corresponding jobs in the CommServe. This feature is applicable for disk storage media only.

The orphaned media is displayed with associated details like the Storage Policy, Storage Policy Copy, Library, volume path, No. of Chunks, Size of the data etc., and the orphaned jobs are displayed with details such as Job ID, Client Name, Application Type, Library, Storage Policy, Storage Policy Copy, etc. You can review the information and delete the orphaned jobs and/or orphaned media. When an orphaned media space is deleted, the space is marked for deletion and pruned based on the retention rules set for the copy. When an orphaned job is deleted, the job is removed from the CommServe database. Jobs deleted using this feature are recorded in the Audit Trail. See [Perform a Disk Volume Reconciliation Job](#) and [Reconcile the Differences](#) for step-by-step instructions.

Once a disk volume reconciliation job is executed, you can use the results of the analysis to reconcile the differences at a later time. This allows you to reconcile the differences without executing the job again. See [View the Results of a Disk Volume Reconciliation Job](#) and [Reconcile the Differences](#) for step-by-step instructions.

This feature is supported only for Non-Deduplicated Storage Policy copy.

You can use the Media Information Report to review the results of this job. The details of the orphaned jobs, orphaned media, and the volumes deleted using the job are available in the report.

MARK ACTIVE MEDIA FULL

This option marks all active media within a storage policy copy as full. Subsequent data protection operations or auxiliary copy operations that are directed to the copy will start on new media.

CHANGE DATA PATH

You can change the data paths for:

- The media group used by a storage policy copy to a different library, master drive pool, drive pool and scratch pool within the CommCell.
- A disk library to another disk library.

For comprehensive information, see Data Path considerations.

DELETE A STORAGE POLICY COPY

When a storage policy copy is deleted, the data associated with the copy cannot be restored/recovered.

The primary copy of a storage policy cannot be deleted. If you want to delete a primary copy then you must delete the entire storage policy.

Secondary copies (synchronous, selective) can be deleted from the CommCell Browser if there are no data aging, data recovery operations, or Auxiliary Copy jobs running. Verify that none are running before attempting to delete the copy. See Delete a Secondary Copy.

SCHEDULES

You can view the schedules of jobs associated with a storage policy copy. For more information on scheduling, see Scheduling.

VIEW MEDIA NOT COPIED

You can view the media that has data that has not yet been copied to all secondary copies within a storage policy. This will help you determine which media are required for operations, and how much data must be copied.

This media can be viewed from the Media Not Copied dialog box.

VIEW MEDIA

The software provides information about all the media or mount paths containing data associated with a storage policy copy. This can be useful in various circumstances, including the following:

- You need to know the mount paths location of your data stored on disk media.
- You want to change the data paths for media from one library to another and need to know which media are associated with a given storage policy copy.
- You are scheduling operations and want to make sure that all of the media necessary for the operations are inside the library.
- You want to view the contents on the media.

A list of this media or mount paths can be viewed from the Media List dialog box.

VIEW JOBS

You can view and perform operations on the jobs that reside on, or are scheduled to be copied to, a storage policy copy. For more information on the **View Jobs** feature, see Jobs on a Storage Policy Copy. Selecting the **Advanced** button provides you with additional viewing options, which you can select in the Jobs in Storage Policy Advanced Filter Options dialog box. From here, you can view jobs based on:

- content indexing status
- availability
- aged data

Results will display in the Job for Storage Policy Copy window.

VIEW AGED MEDIA

You can view the media that was used by a storage policy copy from the `Media List` dialog box. Data from data protection operations have been pruned from this media, and the media has already been returned to the scratch volume pool.

Note: This option is available only if the library to which the storage policy copy directs its data is a tape or optical library.

STORAGE POLICY COPY CONSIDERATIONS

- For DataArchiver, making multiple copies for archived data is recommended to avoid single-point-failure. For example, you can create a secondary copy on a disk library that has a short retention period for faster recovery, and you can also create a secondary copy on tape media that has a longer retention period.
- For NAS environments, refer to Storage Policy Considerations for additional information.
- Multi-stream backups of the Microsoft SQL, DB2, DB2 DPF and Sybase agents will be copied during an auxiliary copy operation to a copy that combines streams; however, restore operations may have limitations. See Browse and Restore for more information.

In order to restore SQL, DB2, DB2 DPF and Sybase agent backups from combined streams of Storage Policy copies, a new Storage Policy copy to disk library must be created and an auxiliary copy should be executed. A restore must be performed from this new copy.

- A custom calendar must first be defined before it can be associated with a storage policy copy.

- The same MediaAgent must be used for both the primary and inline copy.
- Consider an Automatic Copy scheduling option. Automatic Copy allows automatic auxiliary copy operations to be performed at specified time intervals on the source copy. This helps ensure that you will have regular additional copies of data from your data protection operations. For more information, see Automatic Copy.
- For Oracle and Oracle RAC, selective copies are supported for Selective Online Full and Offline Full operations only.
- If the default data path on the primary copy of a storage policy points to a drive pool configured on a MediaAgent enabled with NDMP Remote Server (NRS), then the secondary copy must also point to a drive pool configured on a MediaAgent with NRS installed in order to restore the data to a NAS file server.

AUXILIARY COPY

- When refreshing media, if the source of the auxiliary copy is a synchronous copy, the new copy can be a selective or synchronous copy. However, if the source of the auxiliary copy is a selective copy, the new copy must be a selective copy also.
For more information, see Media Refresh.
- If a storage policy copy designates a source copy for auxiliary copy operations, the source copy should not then designate the original storage policy copy as a source copy for auxiliary copy operations.
- If a secondary storage policy copy is enabled with Deduplication, then the Deduplication Store gets created for the copy and the associated data is deduplicated for that copy. See Deduplication for an overview.
- By default, when a browse or data recovery operation is requested (without specifying copy precedence), the software attempts to browse/restore/recover from the storage policy copy with the lowest copy precedence. If the media for the copy with the lowest precedence is offsite, damaged, or if hardware resources are unavailable, then a specific storage policy copy must be specified in the Copy Precedence tab of the **Storage Policy Properties** dialog box. For more information, see Change the Copy Precedence.

BACKUPS ON AND AFTER DATE

- You can only move the **Backups On And After Date** forward for a storage policy copy once it has been defined. This date must be a date which occurs after the date you originally selected.
- If you change the **Backups On And After Date** to a date after the one selected, all data protection operations that were to be copied from the primary copy before the new date will not be copied when an auxiliary copy is run.

DATA PATH

- If you change the data path between two different libraries, and if the storage policy copy using the source library is configured for a data path failover, once the data path is changed you must configure the storage policy copy for a data path(s).
- If your storage policy is configured for Alternate Data Paths, do not perform change the data path for media associated with the primary copy of that storage policy.
- When you change the data paths make sure that the libraries and drives in the source and destination library are compatible. Specifically, the destination library must be capable of reading the bar codes on the media for which you have changed the data path. See the library manufacturer's documentation for compatible bar codes.
- Make sure that the firmware of the source and target library can read the barcodes of media exactly the same way.
- Make sure that the drives of the destination drive pool are compatible with the recording format and hardware type of the migrating media.
 - An example of recording format incompatibility: Data paths can be changed from DLT 4000 drives to DLT 7000 drives as tapes written by DLT 4000 drives can be read in DLT 7000 drives. However, data paths cannot be changed from DLT 7000 drives to DLT 4000 drives, as tapes written by DLT 7000 drives cannot be read in DLT 4000 drives.
 - Another example of hardware type incompatibility: DLT tapes cannot be inserted into AIT or Mammoth drives or vice-versa.
 - Media from an NDMP drive pool can only be changed to another NDMP drive pool. (An NDMP drive pool is one containing drives that are attached to a NAS filer rather than to a MediaAgent.) Data Paths cannot be changed from NDMP to non-NDMP libraries.
- There are sufficient drives in the destination drive pool to accommodate all of the streams of the copy for which the data paths are changed. For example, a drive pool should contain at least three drives to accommodate a three-stream copy.
- It is possible to change the data paths for compatible libraries to stand-alone libraries and vice-versa, and between compatible stand-alone drives to stand-alone drives.
- When you change the data paths from one library to another, you must physically remove all of the media from the source library and insert them into the destination library. It is strongly recommended that you export such media from the source library and immediately import them in the target library. If you want to export all the media from the library, you can use the Mark Media Exported option from the library level. For more information, see Export Media.
- Once you change the data path and import the media in the target library, subsequent data protection operation, which uses these media, will mark active media as Appendable and use a new media.
- If you change the data path on media from a shared library, there is no need to export media from the source library, as the source library and the target library are the same.
- Media is marked as Appendable once it is migrated from any library to another library.

- Data paths for NAS attached libraries can only be added if the MediaAgent used in that data path also has the File System iDataAgent installed on that computer. This is applicable only for Windows MediaAgents.

DELETE A STORAGE POLICY COPY

- When a copy is deleted any data on that copy is permanently lost and hence becomes unavailable for data recovery operations.
- All corresponding media becomes available for reuse and moved to the corresponding scratch pool.
- A secondary copy cannot be deleted if there are any data aging, data recovery operations, or Auxiliary Copy jobs running. Check to see if there are any of these jobs running before attempting to delete the copy.
- A primary copy of a storage policy cannot be deleted. If you want to delete a primary copy then the entire storage policy must be deleted.

DISABLE A JOB

- A job that has been disabled can still be restored/recovered.
- If a primary copy has a disabled job, and during a data recovery operation the software cannot find any data, data from the disabled job will be used.
- If you disable a backup of the last cycle that has occurred, this forces the next backup to be a full backup.
- For the Exchange Database and Image iDataAgents, if you disable an incremental or differential backup, all subsequent backups will be disabled up to the next full backup.

HARDWARE COMPRESSION

- You cannot enable hardware compression on a copy that uses an optical or disk library.
- NetApp attached drive pools: This procedure cannot change the hardware compression setting, which is determined by the access path selected when configuring the drive. By default hardware compression will be shown as enabled.

INACTIVE STORAGE POLICY COPY

- If you mark a copy inactive, your primary copy data can still be pruned without being copied.
- Once a copy is marked as inactive, it cannot be used to transfer data to media.

PRUNE A JOB

- Once a job is pruned from a storage policy copy, it cannot be restored.
- If a job is pruned or deleted, by default the next job is forced to be a full backup, ensuring a consistent cycle that captures all available data. However, if an associated agent supports differential backups, then you can change the next job to be a differential backup. This reduces media consumption, as full backups contain large amounts of data.

RETAIN A JOB

- From the CommCell Console, data protection operations can be manually retained. However, if necessary, the Command Line Interface jobretention operation can be used to manually retain any type of data protection operation for all agent types.
- Once a job has been manually retained, it will not be pruned during a data aging operation. It will be pruned when the manual retention time requirement has been met. Note that jobs can be held infinitely.
- If a job is manually retained, it will still be pruned as a result of the following operations:
 - Deletion of a backup set or instance/partition.
 - Deletion of a Storage Policy
 - Deletion of a Storage Policy copy
 - The **Overwrite Media** option is enabled on the library
 - Deleting the contents of a media

VIEW RETAINED JOBS

You can view list of all retained jobs for a specific storage policy copy. See View Retained Jobs for a Storage Policy Copy for step-by-step instructions.

RETENTION RULES

- Do not change the retention rule of a copy while a data protection, data recovery, or auxiliary copy operation is running.
- Basic Retention Rules are, by default, set to infinite. However, if you opt to specify basic retention rules for a storage policy copy in terms of days and cycles, the default cycle settings are set to 1 cycle.
- It is recommended that secondary copies have a retention period that is greater than or equal to that of the primary copy.
- If the copy is of a storage policy that is associated with an incremental storage policy, the retention period of the primary copy of the full storage policy copy

must be greater than or equal to the retention period of the primary copy of the incremental storage policy.

- The Basic Retention Rule for a storage policy configured for DataArchiver Agents can only be defined by time, not cycles.
- Basic Retention Rules must be defined before Extended Retention Rules can be selected.
- You can set either 0 days or 0 cycles as a basic retention rule on a primary copy, only when there is an active synchronous copy for the storage policy.
- Extended Retention Rules must be chosen in ascending order by the number of days and the selected rule type.
- All non-full backups after the Basic Retention Rules are met are pruned, regardless of any Extended Retention Rules set.
- If multiple backups reside in the same time period of the Extended Retention Rule, the retention order of priority is as follows:
 - The backup is fully copied, but not disabled.
 - The backup is fully copied, but disabled.
 - The backup is marked as **Partial** or **To be Copied** (data for the job is available on the primary copy)
 - The backup is marked as **Partial** (data from the job is pruned, disabled, or Partial on the primary copy)

SECONDARY COPY

- A synchronous copy must be active to be promoted to be a primary copy.
- Selective copies cannot be promoted to be a primary copy.
- It is recommended that the synchronous copy be synchronized with the primary copy before it is promoted. If it is not, you may suffer data loss if data from the primary copy has not yet been copied to the secondary copy before the secondary copy is promoted. Also, unsynchronized promotion causes the next backup to be a full backup.
- The retention period and all defined attributes for a copy is retained when promoted. Therefore, it is recommended that you change the retention period of the copy so that it has a greater than or equal to retention period of the primary copy. See [Change the Retention Rules of a Storage Policy Copy](#) for details on changing the retention period of a storage policy copy.
- It is recommended that you do not promote a copy to be the primary copy while a data protection, data recovery, or auxiliary copy operation is running.
- If your secondary copy that you want to promote uses the **Combined to <n> Streams** option, then that copy must have the same amount of drives available as the primary copy.
- A secondary copy will assume the same data multiplexing factor defined in the primary copy.

SPOOL COPY

- Only a primary copy can be marked as a spool copy with a 0 days and 0 cycles basic retention rule.
- There must be an active synchronous copy.
- Once data is copied to a secondary copy, all data is pruned from a spool copy during a data aging operation.

DATA MULTIPLEXING

Image Level and Image Level ProxyHost

- Data Multiplexing is not supported for more than one stream to a single tape within a job. Multi-streaming is supported, however, each stream must use a different tape. The data on a tape can be multiplexed with a different job, but not with another stream of the same job.

BEST PRACTICES

MANAGED DISK SPACE

For deduplicated storage policy copies, it is recommended that you disable the **Enable Managed Disk Space for disk data** option on **Copy Properties** dialog box (**Retention** tab), for faster pruning of the aged data in order to reclaim space on the disk.

AUDIT TRAIL

Operations performed with this feature are recorded in the Audit Trail. See [Audit Trail](#) for more information.

RELATED REPORTS

JOBS IN STORAGE POLICY COPY REPORT

The Jobs In Storage Policy Copy Report provides a list of data protection jobs associated with the storage policy copies based on the selected filter criteria.

[Back to Top](#)

Storage Policy Copy Operations - How To

[Topics](#) | [How To](#) | [Support](#) | [Related Topics](#)

- [Add a Data Path to a Storage Policy Copy](#)
- [Associate a Custom Calendar to a Storage Policy Copy](#)
- [Associate a Subclient to a Storage Policy](#)
- [Change the Copy Precedence](#)
- [Change the Data Path of a Storage Policy](#)
- [Change the Maximum Number of Data Streams](#)
- [Change the Name of a Storage Policy](#)
- [Change the Name of a Storage Policy Copy](#)
- [Change the Retention Rules of a Storage Policy Copy](#)
- [Change the Scratch Pool Associated With a Storage Policy Copy](#)
- [Configure Storage Policy Copy as WORM Copy](#)
- [Change the Storage Policy Copy Backups on and After Date](#)
- [Combine the Data Streams of a Storage Policy Copy](#)
- [Configure a Storage Policy Copy for Data Verification](#)
- [Configure a Storage Policy Copy for Data Encryption](#)
- [Configure Multiple Data Paths for a Storage Policy Copy](#)
- [Create a Snapshot Copy](#)
- [Create a Selective Copy](#)
- [Create a Spool Copy](#)
- [Create a Storage Policy](#)
- [Create a Subclient-Based Storage Policy Copy](#)
- [Create a Synchronous Copy](#)
- [Delete a Data Path from a Storage Policy Copy](#)
- [Delete a Disaster Recovery Backup Storage Policy](#)
- [Delete an iDataAgent Backup or DataArchiver Storage Policy](#)
- [Delete a Job](#)
- [Delete a Secondary Copy](#)
- [Delete a Storage Policy that has an Incremental Storage Policy Enabled](#)
- [Defer Auxiliary Copy on a Copy](#)
- [Disable a Disaster Recovery Backup From a Disaster Recovery Storage Policy Copy](#)
- [Disable/Enable a Job From a Storage Policy Copy](#)
- [Disable/Enable All Jobs Associated with a Media](#)
- [Create Automatic Copy Schedule](#)
- [Enable a Parallel Copy](#)
- [Enable an Incremental Storage Policy](#)
- [Enable an Inline Copy](#)
- [Enable or Disable Hardware Compression](#)
- [Enable Managed Disk Space for Data](#)
- [Enable Multiplexing for a Storage Policy Copy with Combined Data Streams](#)

Manually Retain a Job on a Storage Policy Copy

Perform a Disk Volume Reconciliation Job and Reconcile the Differences

View the Results of a Disk Volume Reconciliation Job and Reconcile the Differences

Mark a Storage Policy Copy Inactive

Mark the Active Media of a Storage Policy Copy Full

Pick a Job on a Storage Policy Copy for Data Verification

Promote a Synchronous Copy to be a Primary Copy

Prune a Disaster Recovery Backup From a Disaster Recovery Backup Storage Policy Copy

Re-Associate the Subclients of a Storage Policy

Select the Criteria for using an Alternate Data Path

Set a Data Path as the Default Data Path

Specify the Source Copy for an Auxiliary Copy Operation

Start an Auxiliary Copy

View the Aged Jobs of a Storage Policy Copy

View the Aged Media of a Storage Policy Copy

View the Events of a Job on a Storage Policy Copy

View the Items That Failed for a Job on a Storage Policy Copy

View the Job Details of a Job on a Storage Policy Copy

View the Jobs of a Storage Policy Copy

View the Jobs Scheduled For a Storage Policy

View the Jobs Scheduled for a Storage Policy Copy

View Retained Jobs for a Storage Policy Copy

View the Media Not Copied

View the Media of a Job on a Storage Policy Copy

View the Media of a Storage Policy Copy

View the Mount Paths of a Storage Policy Copy

ADD A DATA PATH TO A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To add a data path to a storage policy copy:

1. From the CommCell Browser, right-click the storage policy copy for which you wish to add the data paths, then click **Properties**.
2. Click the Data Paths tab. Note that depending on the criteria selected for using an alternate data path, you may have to share the indexes.
3. Click **Add**.
4. From the Copy Data Path Candidates dialog box, select the data path candidates that you wish to add.
You can select multiple candidates by holding down the CTRL key and clicking on each of the data path candidates that you wish to select.
5. Click **Add**.
6. Click **OK**.
7. Click **OK** in the **Data Paths** tab to save the information.

ASSOCIATE A CUSTOM CALENDAR TO A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To associate a custom calendar to a storage policy copy:

1. Right-click the storage policy copy for which you wish to associate a custom calendar, and then click **Properties**.
2. From the General tab of the **Copy Properties** dialog box, select a calendar from the **Calendar for Selective Copy and Extended Retention** checkbox.
3. Click **OK** to save your changes.

Associating a custom calendar to a storage policy copy changes the time intervals by which data is copied to and aged from this copy.

ASSOCIATE A SUBCLIENT TO A STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

▶ To associate a subclient to a storage policy:

1. From the CommCell Browser, right-click the subclient whose associated storage policy you want to change, then click **Properties** from the shortcut menu.
2. Click the Storage Device tab of the Subclient Properties dialog box.
3. From the **Storage Policy** list of the **Data Storage Policy** tab, select a data storage policy to associate with this subclient. If necessary, click the **Create Storage Policy** button to create a new storage policy to which the subclient can then be associated.
4. From the Changing a Storage Policy window select the next type of backup operation. Click **OK**.
5. If applicable for your agent, you can change the number of data streams from the **Number of Data/Database Backup Streams** field.
6. If applicable for your agent, click the **Log Storage Policy** tab and select a storage policy to associate with this transaction log subclient from the **Transaction Log Storage Policy** list. Also, you can set the **Number of Transaction Log Backup Streams** from this tab.
7. Click **OK** to save your changes and close the Subclient Properties Storage Device tab.

CHANGE THE COPY PRECEDENCE

Required Capability: See Capabilities and Permitted Actions

▶ To change the copy precedence of a storage policy copy:

1. From the CommCell Browser, right click the storage policy whose copy precedence you want to change, and then click **Properties**.
2. From the Copy Precedence tab of the **Storage Policy Properties** dialog box, select a synchronous or selective copy and click the arrow buttons to change its copy precedence. The arrows will move a copy to a higher or lower precedence in increments of 1. For more information, see Recovering Data From Copies.
3. Click **OK**.

CHANGE THE DATA PATH OF A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To change the data path of a Storage Policy Copy:

1. Right click a storage policy copy for which you want to change the data path , click **All Tasks** and click **Change Data Path**.
2. The **Change Data Path** dialog box is displayed.
 - For disk media, select the appropriate **Library** and the **MediaAgent** where you want to migrate the media.
 - For tape and optical media, select the appropriate **Library, Master Drive Pool, Drive Pool, and Scratch Pool** where you want to migrate the media.
3. Click **OK** to change the data path.

CHANGE THE MAXIMUM NUMBER OF DATA STREAMS

Required Capability: See Capabilities and Permitted Actions

▶ To change the maximum number of data streams:

1. From the CommCell Browser, right click the storage policy whose quantity of data streams you want to change, and then click **Properties**.
2. From the General tab of the **Storage Policy Properties** dialog box, type the number of data streams that you want to allocate for the storage policy in the **Device Streams** field.

3. Click **OK** to save your changes.
-

CHANGE THE NAME OF A STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

▶ To rename a storage policy:

1. From the CommCell Browser, right click the storage policy that you want to rename, and then click **Properties**.
 2. From the General tab of the **Storage Policy Properties** dialog box, type the new name (up to 32 characters) in the **Storage Policy Name** field.
 3. Click **OK** to save your changes.
-

CHANGE THE NAME OF A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To change the name of a storage policy copy:

1. From the right pane of the CommCell Browser, right-click the storage policy copy that you wish to rename and then click **Properties**.
 2. From the General tab of the **Copy Properties** dialog box, type the new name in the **Copy Name** field.
 3. Click **OK** to save your changes.
-

CHANGE THE RETENTION RULES OF A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To change the retention rules for a primary or secondary storage policy copy:

1. From the right pane of the CommCell Browser, right-click the storage policy copy for which you wish to change the retention rule, and select **Properties**.
 2. From the Retention tab of the **Copy Properties** dialog box, you can:
 - **Enable Data Aging**. Data Aging must be enabled to set retention rules.
 - Enable **Managed Disk Space for disk data**. This is only enabled when copy points to disk library.
 - Set the Basic Retention Rules for All Backups and Data/Compliance Archiver Data.
 3. Optionally, you can set extended retention rules in the **Extended Retention Rules** pane by:
 - Selecting the number of days to keep All Fulls, the Weekly Full, Monthly Full, Quarterly Full, Half Yearly Full, or the Yearly Full.
 - Selecting the start time of the weekly, monthly, or yearly rule.
 - Selecting the **First full backup of time period** radio button if you want the first full backup of each Extended Retention Rule retained, or select the **Last full backup of time period** (the default) radio button if you want the last full backup of each Extended Retention Rule retained.
 4. Click **OK** to save your changes.
-

CHANGE THE SCRATCH POOL ASSOCIATED WITH A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To change the scratch pool for a storage policy copy:

1. From the right pane of the CommCell Browser, right-click the storage policy copy for which you wish to change the scratch pool, and click **Properties**.
 2. From the General tab of the **Copy Properties** dialog box, select another scratch pool from the **Scratch Pool** list.
 3. Click **OK** to save your changes.
-

CONFIGURE STORAGE POLICY COPY AS WORM COPY

Required Capability: See Capabilities and Permitted Actions

▶ To configure a storage policy copy as a WORM (Write Once Read Many) copy:

1. From the right pane of the CommCell Browser, right-click the storage policy copy for which you wish to change the scratch pool, and click **Properties**.

2. From the General tab of the **Copy Properties** dialog box, select **Worm Copy**.
3. Click **Yes** from the Confirm Streams dialog box.
4. Click **OK** to save your changes.

Cannot be cleared if the option has been selected and the policy has been saved.

WORM Copy cannot be disabled once the option has been selected and the policy has been saved.

CHANGE THE STORAGE POLICY COPY BACKUPS ON AND AFTER DATE

Required Capability: See Capabilities and Permitted Actions

▶ To change the **Backups On And After** date for a storage policy copy:

1. From the right pane of the CommCell Browser, right-click the storage policy copy for want to change the effective date, and click **Properties**.
2. Click the Copy Policy tab of the **Copy Properties** dialog box.
3. Choose a date from the **Backups On And After** field. This date can be on, before, or after the current CommServe date. When the date entered is after the current CommServe date, jobs that are to be copied, as well as partially copied jobs will be disabled for copy. If no date is entered, all backup data will be copied from the primary copy to the secondary copy.

The **All Backups** option is not available for selective copies; therefore, you must choose a date from the **Backups On And After** field.

4. Click **OK** to save your changes.

COMBINE THE DATA STREAMS OF A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To combine the data streams of a storage policy copy:

1. From the right pane of the CommCell Browser, right-click the storage policy copy for which you wish to combine data streams, and select **Properties**.
2. From the Copy Properties (Media) window, select the number of streams to which you wish to combine streams during an auxiliary copy operation in the **Combine Source Data Streams to n Streams** box.
3. Click **OK** to save your changes.

ENABLE MULTIPLEXING FOR A STORAGE POLICY COPY WITH COMBINED DATA STREAMS

Required Capability: See Capabilities and Permitted Actions

▶ To enable multiplexing for a storage policy copy with combined streams:

1. From the right pane of the CommCell Browser, right-click the storage policy copy for which you wish to configure multiplexing, and select **Properties**.
2. From the Copy Properties (Media) window, select the **Multiplex Source Streams** option to enable the feature for this storage policy copy, and then select the **Multiplex Factor**. Note that this feature is only configurable when the storage policy copy has been configured to combine streams, and the copies do not contain deduplicated data.
3. Click **OK** to save your changes.

CONFIGURE A STORAGE POLICY COPY FOR DATA VERIFICATION

Required Capability: See Capabilities and Permitted Actions

▶ To configure a storage policy copy for data verification:

1. From the right pane of the CommCell Browser, right-click the storage policy, and then click **Properties**.
2. From the Advanced tab of the **Copy Properties** dialog box, click the **All Backups** option if you want all backups to be verified during a data verification operation, or click **All Full Backups** if you want only full backups to be verified. You can also click the **Backups On or After Date** option and select a date from the **Select a Date** list. Only those backups that occur on or after the date you select will be verified.

3. Click the **Expiration** option to provide an expiration date for the data verification operation, and select the number of months that the data verification operation will be valid from the **Verification expires after *n* months** list.
 4. Click **OK** to save the changes.
-

CONFIGURE A STORAGE POLICY COPY FOR DATA ENCRYPTION

Required Capability: See Capabilities and Permitted Actions

▶ To configure a storage policy copy for data encryption:

1. From the right pane of the CommCell Browser, right-click a secondary storage policy copy, and then click **Properties**. Note that you cannot configure a primary storage policy copy for data encryption.
 2. From the Advanced tab of the **Copy Properties** dialog box, click the **Encrypt Data** check box to enable options.
 3. Select options based on the criteria described in the **Advanced** tab help.
 4. Click **OK** to save your settings
-

CONFIGURE MULTIPLE DATA PATHS FOR A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To configure multiple data paths for a storage policy copy:

1. Select the criteria under which a storage policy copy must use an alternate data path, as described in Select the Criteria for using an Alternate Data Path.
2. Depending on the criteria selected for using an alternate data path, you may have to share the indexes.
3. Add the data paths to storage policy copies for which you wish to add multiple data paths, as described in Add a Data Path to a Storage Policy Copy.

The storage policy copy will automatically switch to an alternate data path, when the preferred data path is either offline or busy, as established in the criteria for using an alternate data path.

CREATE A SNAPSHOT COPY

Required Capability: See Capabilities and Permitted Actions

▶ To create a snapshot copy:

1. From the CommCell Browser, right-click the storage policy for which you wish to create a snapshot copy, click **All Tasks** and then click **Create New Snapshot Copy**.
 2. From the General tab of the `Copy Properties` dialog box:
 - Enter the copy name in the **Copy Name** field.
 - Select the library, MediaAgent, master drive pool and scratch pool from the lists (not applicable for disk libraries).
 3. From the Retention tab of the `Copy Properties` dialog box:
 - Click the **Enable data aging** checkbox, to enable or disable Data Aging on this copy.
 - Change the retention time and retention cycles of the Basic Retention Rules from their default settings of infinite, if needed.
 4. Click **OK** to save your changes.
-

CREATE A SELECTIVE COPY

Required Capability: See Capabilities and Permitted Actions

▶ To create a selective copy:

1. From the CommCell Browser, right-click the storage policy for which you wish to create the secondary copy, click **All Tasks** and then click **Create New Copy**.
2. From the General tab of the **Copy Properties** dialog box:
 - Enter the copy name in the **Copy Name** box.
 - Select the **Combine to <n> Streams** check box if you want to combine data streams during an auxiliary copy operation on this copy.
 - Deselect the **Active** check box if you want to specify that this should be an inactive copy.

- Select the library, MediaAgent, drive pool, and the scratch pool from the lists (drive pool and scratch pool are not applicable to disk libraries).
 - Select the **Selective Copy** check box. The **Selective Copy** tab is enabled.
3. Select a standard or custom calendar from the **Calendar for Selective Copy and Extended Retention** drop-down list. Note that this option is only available if a custom calendar was created.
 4. From the Retention tab of the **Copy Properties** dialog box:
 - Click the **Enable data aging** checkbox, to enable or disable Data Aging on this copy.
 - Click the **Enable Managed Disk Space for disk data**, to enable or disable Managed Disk Space.
 - Change the retention time and retention cycles of the Basic Retention Rules from their default settings of infinite, if needed.
 - Change the Extended Retention Rules, if necessary.
 5. Click the Copy Policy tab of the **Copy Properties** dialog box:
 - Choose a date from the **Backups On And After** field. This date can be on, before, or after the current CommServe date. When the date entered is after the current CommServe date, jobs that are to be copied, as well as partially copied jobs will be disabled for a copy. If no date is entered, all backup data will be copied from the primary copy to the secondary copy.
 - Click the **Specify source for Auxiliary Copy** check box if you wish to copy data from a copy other than the primary copy.

The **All Backups** option is not available for selective copies; therefore, you must choose a date from the **Backups On And After** field.
 6. Click the Selective Copy tab.
 - Select **Automatically select Full Backups** (*all fulls*) to automatically copy all full backups regardless of time.
 - Select **Automatically select Full Backups** (*daily, weekly, monthly, quarterly, half yearly, or yearly*) for the copy to be time-based. If the copy is time based, you can select one of the following options:
 - **First full backup**
 - **Last full backup** (which is based on the following two options):
 - **Select most recent job if there are no more full backup schedules in current time period**
Specifies that the last full backup of the specified time period will be copied from the source copy to this copy if there are no future full backup schedules within the same time period.
 - **Wait until the current time period is over before selecting a backup for this time period**
Specifies that, after the end of the specified time period, the last full backup during that time will be copied from the source copy to this copy. Note that this option is not enabled if the source of the selective copy is a Primary Copy that is defined with zero cycle retention or configured as a spool copy; this is because jobs can be aged immediately after they are copied to synchronous copies, which is before the current time period ends.
 - Select **Automatically select Full Backups** (*Advanced*) to copy all full backups based on the advanced backup frequency options.
 - Select **Every [x] Cycle(s)**, to copy full backup after the specified number of cycles.
 - Select **Every [x] Day(s)**, to copy full backup after the specified number of days.
 - Select **Every [x] Week(s)**, to copy full backup after the specified number of weeks.
 - Select **Every [x] Month(s)**, to copy full backup after the specified number of months.
 - Select **Do not Automatically select jobs** so no backups will be copied to this copy unless they are manually selected for copy from the Job for Storage Policy Copy dialog box or the **Select most recent full backup when auxiliary copy starts** option has been selected from the Auxiliary Copy Options dialog box.
 7. If there are no auxiliary copy schedules defined for all copies of the storage policy, you are asked to confirm if you would like to schedule auxiliary copy operations for this copy. Select **Default Schedule**, if you would like an auxiliary copy operation to be scheduled to be run daily at 8:00 A.M., select **Custom Schedule** if you would like to define a schedule, select **Automatic Schedule** if you would like an Automatic Copy to run every 30 minutes, or select **Do Not Schedule**. Click **Yes** if you would like to run or schedule this job. Click **OK**.

CREATE A SPOOL COPY

Required Capability: See Capabilities and Permitted Actions

▶ To create a spool copy:

1. From the right pane of the CommCell Browser, right-click the primary storage policy copy that is to be used as a spool copy, then click **Properties**.
 2. From the Retention tab of the **Copy Properties** dialog box, click **Spool Copy (No Retention)**.
 3. Click **OK**.
-

CREATE A STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

▶ To create a storage policy:

1. From the CommCell Browser, right-click the Storage Policies node, and select New Storage Policy from the shortcut menu.
2. Follow the prompts displayed in the Storage Policy Wizard to configure the following:
 - Type of Storage Policy: Backup, Compliance Archiver or Disaster Recovery Backup
 - Name of Storage Policy (and Incremental Storage Policy, if selected)
 - Name of the Primary Copy
 - Name of the default library to which the Primary Copy should be associated
 - Name of the MediaAgent
 - Stream and Retention Configuration (default is infinite)
 - Designate Primary Copy for Deduplication: Yes or No. Also, select the Deduplication Type: Block Level or Object Level.

If you wish to enable deduplication at the source, select the Enable Client Side Deduplication option.

If you select No, you cannot enable deduplication on the primary copy at a later time. However, you can enable deduplication on the secondary copies during creation. See Enable Deduplication in a Secondary Copy for details.

- Name of the Deduplication Store, MediaAgent for Deduplication Store access, and location of the Deduplication Database. If you wish to create a new deduplication store for the Storage Policy, then select Create New Deduplication Store and provide the location of the store. If you wish to deduplicate against an existing deduplication store from a different Storage Policy, then select Use Existing Deduplication Store and select the desired deduplication store from the list. Note that the deduplication database must be located in a folder and not directly under the root of a disk volume.
3. The **Review Summary** window is displayed. Review your selections and then click **Cancel**, **Back** (to return to a previous window to change a selection), or **Finish** (to exit and create the storage policy).

CREATE A SUBCLIENT-BASED STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To create a subclient based storage policy copy:

1. From the right pane of the CommCell Browser, right-click the appropriate secondary storage policy copy, then click **Properties**.
2. From the Associations tab of the **Copy Properties** dialog box, select the client(s), agents, backup set(s) or subclient(s) to be associated with this copy.

When you re-associate a client/subclient to a storage policy copy, only new jobs of the selected client/subclient are copied to a storage policy copy during an Auxiliary copy operation.

3. Click **OK**.

CREATE A SYNCHRONOUS COPY

Required Capability: See Capabilities and Permitted Actions

▶ To create a synchronous copy:

1. From the CommCell Browser, right-click the storage policy for which you wish to create the secondary copy, click **All Tasks** and then click **Create New Copy**.
2. From the General tab of the Copy Properties dialog box:
 - Select the **Combine to <n> Streams** check box if you want to combine data streams during an auxiliary copy operation on this copy.
 - De-select the **Active** check box if you want to specify that this should be an inactive copy.
 - Enable **Inline Copy** for data to be backed up to this copy in addition to the primary copy.
 - Select **Do Not Make Inline Copy to Same Library** to prevent a job from being copied to the same library during Inline Copy operations.
 - Enable **Parallel Copy** for data to be copied to multiple secondary copies concurrently rather than sequentially.
 - Select the library, MediaAgent, master drive pool and scratch pool from the lists (not applicable for disk libraries).
3. From the Retention tab of the Copy Properties dialog box:

- Click the **Enable data aging** checkbox, to enable or disable Data Aging on this copy.
 - Click the **Enable Managed Disk Space for disk data**, to enable or disable Managed Disk Space.
 - Change the retention time and retention cycles of the Basic Retention Rules from their default settings of infinite, if needed.
 - Change the Extended Retention Rules, if necessary.
4. Click the Copy Policy tab of the `Copy Properties` dialog box:
- Choose a date from the **Backups On And After** field. This date can be on, before, or after the current CommServe date. When the date entered is after the current CommServe date, jobs that are to be copied, as well as partially copied jobs will be disabled for copy. If no date is entered, all backup data will be copied from the primary copy to the secondary copy.
 - Click the **Specify source for Auxiliary Copy** check box if you wish to copy data from a copy other than the primary copy.
- The **All Backups** option is not available for selective copies; therefore, you must choose a date from the **Backups On And After** field.
5. Click **OK** to save your changes.
6. If there are no auxiliary copy schedules defined for all copies of the storage policy, you are asked to confirm if you would like to schedule auxiliary copy operations for this copy. Select **Default Schedule**, if you would like an auxiliary copy operation to be scheduled to be run daily at 8:00 A.M., select **Custom Schedule** if you would like to define a schedule, select **Automatic Schedule** if you would like a Automatic Copy to run every 30 minutes, or select **Do Not Schedule**. Click **Yes** if you would like to run or schedule this job. Click **OK**.

DEFER AUXILIARY COPY ON A COPY

Required Capability: See Capabilities and Permitted Actions

▶ To defer Auxiliary Copy operations on this copy:

1. Right-click the secondary storage policy copy for which you wish to defer Auxiliary Copy operations, and then click **Properties**.
2. From the General tab of the **Copy Properties** dialog box, select the **Defer Auxiliary Copy** box, and set the number of days in which to defer the copy.
3. Click **OK** to save your changes.

DELETE A DATA PATH FROM A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To delete a data path from a storage policy copy:

1. From the CommCell Browser, right-click the storage policy copy for which you wish to delete a data path, then click **Properties**.
2. Click the Data Paths tab.
3. Click the data path you wish to delete from the list.
4. Click **Delete**. The data path is deleted.
5. Click **OK** to save the information.
 - You cannot delete a data path that is set as the default data path.
 - You can delete a data path when the associated storage policy is reserved for data protection operations.

DELETE A DISASTER RECOVERY BACKUP STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

Before you Begin

Create a new Disaster Recovery storage policy — a CommCell must have at least one Disaster Recovery storage policy. If you wish to deconfigure the mount path to reclaim the space, use a different library for the new storage policy.

▶ To delete a Disaster Recovery Backup storage policy:

1. From the CommCell Browser, right-click the CommServe icon, click **Control Panel**, and select **DR Backup Settings**.
2. From the **DR Backup Settings (Export Settings)** dialog box, in the **Back Up Metadata to this DR Storage Policy** dropdown list, select the newly-created storage policy.
3. From the CommCell Browser, select the Storage Policies parent node to view the property details of all the storage policies displayed in the right-hand

windowpane. Check the **Disable Subclient Association** checkbox for the Storage Policy for which you want to delete.

4. From the CommCell Browser, right-click the Disaster Recovery Backup storage policy that you want to delete, click **All Tasks** and then click **Delete**.
5. A warning dialog box will display indicating that this policy is the active target of disaster recovery backups and a new target should be specified prior to deletion. Click **Continue**.

If your Disaster Recovery Backup storage policy is defined in such a way that it is backing up to a removable media, a dialog box displays with a selection to export media. Note that you will not be prompted to export media if your Disaster Recovery Backup storage policy backs up data to disk media.

6. If you choose to export media, from the **Export Media (Delete Storage Policy)** dialog box, select the media to be exported and click **OK**.
7. Type an outside storage location in the **Export Media** dialog box and click **Export**. Click **OK** to the message displayed. For more information on exporting media, see Exporting a Specific Media.
8. You can continue to export the existing media or choose to continue with the deletion.
9. After clicking **Continue**, the Disaster Recovery Backup storage policy is deleted.
10. If you chose to delete the storage policy without exporting media, you are prompted to confirm that you want to delete the storage policy. Click **OK**. The Disaster Recovery Backup storage policy is deleted. The associated mount path can then be deconfigured.

DELETE A JOB

A job (or multiple jobs) can be manually deleted. If a job is pruned, it cannot be restored. Additionally, if you delete a job of the last cycle that has occurred, the next job will be automatically converted to a full data protection operation, ensuring a consistent cycle that includes all available data.

Required Capability: See Capabilities and Permitted Actions

▶ To prune a job from a storage policy copy:

1. From the right pane of the CommCell Browser, right-click the storage policy copy whose jobs you want to view, click **View** and then click **Jobs**.
2. Filter the necessary options in the Job Filter for Storage Policy Copy dialog box. Click **OK**.
3. A list of jobs associated with a storage policy copy is displayed in the Jobs for Storage Policy Copy window.
4. Right-click on a job and select **Delete Job**. The Delete Job dialog displays.
5. Select Yes to delete the dependent jobs, and click **OK**. The selected job and all dependent jobs are displayed in the Delete Job dialog.
6. Select the desired jobs. Hold down the **Ctrl** key, to select multiple jobs.
7. Click **OK**.
8. Click **Yes** on the Confirmation pop-up window that appears.

DELETE A STANDARD STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

▶ To delete an iDataAgent Backup or DataArchiver storage policy:

1. From the CommCell Browser, right-click the storage policy that you want to delete, and click **Properties**.
2. Review the **Associated Subclients** tab. If you find any subclients associated to the storage policy, re-associate them using the **Re-Associate** option. Click **OK** to save the changes.

Alternatively, you can disable all subclient association. From the CommCell Browser, select the Storage Policies parent node to view the property details of all the storage policies displayed in the right-hand windowpane. Check the **Disable Subclient Association** checkbox for the Storage Policy for which you want to delete.

3. From the CommCell Browser, right-click the storage policy that you want to delete, click **All Tasks** and then click **Delete** from the short-cut menu.
4. Click **Yes** to the confirmation message.
5. Type **erase and reuse media**. Click **OK**.
6. The selected storage policy is deleted and removed from the CommCell Browser. The associated mount path can then be deconfigured.

If subclients are still associated with the storage policy that you want to delete, an explanatory message is displayed and the delete operation is aborted.

DELETE A SECONDARY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To delete a secondary copy:

1. From the CommCell Browser, right-click the secondary copy that you want to delete, click **All Tasks** and then click **Delete**.
 2. Click **Yes** to the confirmation message.
 3. Type **erase and reuse media**. Click **OK**.
 4. The selected copy is deleted and removed from the CommCell Browser.
-

DELETE A STORAGE POLICY THAT HAS AN INCREMENTAL STORAGE POLICY ENABLED

Required Capability: See Capabilities and Permitted Actions

▶ To delete a storage policy that has an incremental storage policy enabled:

1. From the CommCell Browser, right-click the storage policy you want to delete, then click **Properties**.
2. From the General tab of the **Storage Policy Properties** dialog box, clear the **Incremental Storage Policy** check box.
3. Click **OK** to save your changes.
4. From the **Force Full Backup - Confirmation** dialog box, select either the **Force next backup to be a full (Recommended)** field or the **Do not force** field (if you do not want to force the next backup to be a full backup).
5. Click **OK**.
6. Right-click the storage policy that you want to delete, click **All Tasks** and then click **Delete**.
7. Click **Yes** to the confirmation message.
8. Type **erase and reuse media**. Click **OK**.
9. The selected storage policy is deleted and removed from the CommCell Browser.

If subclients are still associated with the storage policy that you want to delete, an explanatory message is displayed and the delete operation is aborted.

DISABLE A DISASTER RECOVERY BACKUP FROM A DISASTER RECOVERY STORAGE POLICY COPY

Before You Begin

- A job that has been disabled can still be restored/recovered.
- Marking a job disabled is an irreversible operation that cannot be undone.
- If a storage policy copy has a disabled job, and during a data recovery operation no data can be found, data from the disabled job will be used.
- Disabling a Disaster Recovery backup causes an auxiliary copy job to skip that job when an auxiliary copy operation is run.

Required Capability: See Capabilities and Permitted Actions

▶ To disable a Disaster Recovery backup job from a Disaster Recovery Storage Policy Copy:

1. From the right pane of the CommCell Browser, right-click a Disaster Recovery storage policy copy whose backups you want to view, click **View** and then click **Backups**.
2. From the DR Backups For Copy dialog box, right click the Disaster Recovery backup job that you want to disable, then click **Disable Job**.
3. Click **Yes** in the confirmation prompt that appears to disable this Disaster Recovery backup job.

The Disaster Recovery backup job is disabled.

DISABLE AN INCREMENTAL STORAGE POLICY FROM A STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

▶ To disable a storage policy that is associated with a full storage policy:

1. From the CommCell Browser, right click the storage policy that you want to disable the incremental storage policy from, then click **Properties**.
2. From the (General) tab of the **Storage Policy Properties** dialog box, clear the check box.

3. Click **OK** to save your changes.
 4. From the **Force Full Backup - Confirmation** dialog box, select either the **Force next backup to be a full (Recommended)** field or the **Do not force** field (if you do not want to force the next backup to be a full backup).
 5. Click **OK**.
-

DISABLE/ENABLE A JOB FROM A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To disable a job associated with a primary copy:

1. From the right pane of the CommCell Browser, right-click the copy whose jobs you want to disable, click **View** and then click **Jobs**.
2. Select the necessary filter options in the Job Filter for Storage Policy Copy dialog box.
3. Click the **Advanced** button for additional filter options in the Jobs in Storage Policy Advanced Filter Options dialog box. Click **OK**.
4. A list of jobs associated with a storage policy copy is displayed in the Jobs for Storage Policy Copy window.
5. Right-click on a job, and click **Prevent Copy** (for primary copies) or **Do Not Copy** (for secondary copies).
 - o To select multiple jobs, hold down the **Ctrl** key, and right click on the jobs.
6. Select whether you want to prevent the associated incremental jobs in the **Prevent Copy** dialog box.
7. A list of all jobs that will be disabled in addition to the job you selected are displayed in the Prevent Copy dialog box.
8. Click **OK**.
9. Click **Yes** on the Confirmation pop-up window.

▶ To enable a job associated with a primary copy:

1. From the right pane of the CommCell Browser, right-click the primary copy whose jobs you want to disable, click **View** and then click **Jobs**.
 2. Filter the necessary options in the Job Filter for Storage Policy Copy dialog box. Click **OK**.
 3. A list of jobs associated with a storage policy copy is displayed in the Jobs for Storage Policy Copy window.
 4. Right-click on a job, and click **Allow Copy**.
 - o To select multiple jobs, hold down the **Ctrl** key, and right click on the jobs.
 5. Click **Yes** on the Confirmation pop-up window.
-

DISABLE/ENABLE ALL JOBS ASSOCIATED WITH A MEDIA

Required Capability: See Capabilities and Permitted Actions

▶ To disable all jobs associated with a media:

1. From the right pane of the CommCell Browser, right-click the copy containing the media to which you want to disable jobs, click **View** and then click **Media**.
2. From the Media List dialog box, right-click on the media for which you wish to disable jobs and select **Prevent Copy**.
 - o To select multiple media items, hold down the **Ctrl** key, and right click on the media.
3. Click **Yes** on the Confirmation pop-up window.

▶ To enable all jobs associated with a media:

1. From the right pane of the CommCell Browser, right-click the copy containing the media to which you want to enable jobs, click **View** and then click **Media**.
 2. From the Media List dialog box, right-click on the media for which you wish to enable jobs and select **Allow Copy**.
 - o To select multiple media items, hold down the **Ctrl** key, and right click on the media.
 3. Click **Yes** on the Confirmation pop-up window.
-

CREATE AUTOMATIC COPY SCHEDULE

Required Capability: See Capabilities and Permitted Actions

▶ To create an automatic copy schedule:

1. Right-click the storage policy associated with the secondary storage policy copy for which you wish to enable Auxiliary Copy operations, and then click **Run Auxiliary Copy**. To configure the copy options, refer to Start an Auxiliary Copy.
2. From the Job Initiation tab of the **Auxiliary Copy** dialog box, select **Automatic Copy**, and if necessary, change the **Interval** time in which the copy should run; the default is set to every 30 minutes.

You can set the time interval between 15 to 1440 minutes.

3. Click **OK** to save your changes.
-

ENABLE OR DISABLE HARDWARE COMPRESSION

Required Capability: See Capabilities and Permitted Actions

▶ To enable or disable hardware compression:

1. Right-click the storage policy copy and then click **Properties**.
 2. Click the Data Paths tab.
 3. Click the data path for which you wish to change the hardware compression and then click Properties.
 4. From the Data Path Properties dialog box, select the **Hardware Compression** checkbox to enable or de-select to disable hardware compression.
 5. Click **OK** to save your changes.
-

ENABLE A PARALLEL COPY

Required Capability: See Capabilities and Permitted Actions

▶ To enable an Parallel Copy:

1. Right-click the secondary storage policy copy for which you wish to enable the Parallel Copy, and then click **Properties**.
 2. From the General tab of the **Copy Properties** dialog box, select the **Enable Parallel Copy** box.
 3. Click **OK** to save your changes.
-

ENABLE AN INCREMENTAL STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

▶ To enable an incremental storage policy:

1. From the CommCell Browser, right click the storage policy that you want to enable an incremental storage policy, then click **Properties**.
 2. From the General tab of the **Storage Policy Properties** dialog box, select a storage policy from the **Incremental Storage Policy** list.
 3. Click **Yes** to the confirmation prompt that the next backup for all subclients for this storage policy will be forced to be a full backup.
 4. From the **Force Full Backup - Confirmation** dialog box, select either the **Force next backup to be a full (Recommended)** field or the **Do not force** field (if you do not want to force the next backup to be a full backup).
 5. Click **OK** to save your changes.
-

ENABLE AN INLINE COPY

Required Capability: See Capabilities and Permitted Actions

▶ To enable Inline Auxiliary Copy:

1. Right-click the secondary storage policy copy for which you wish to enable Inline Auxiliary Copy, and then click **Properties**.
 2. From the General tab of the **Copy Properties** dialog box, select the **Enable Inline Copy** box.
 3. Click **OK** to save your changes.
-

ENABLE MANAGED DISK SPACE FOR DISK DATA

Related Topics

- Thresholds for Managed Disk Space

Required Capability: See Capabilities and Permitted Actions

▶ To enable managed disk space for disk data:

1. Right-click the storage policy copy for which you wish to enable or disable Data Aging, and then click **Properties**.
2. From the Retention tab of the **Copy Properties** dialog box, select the **Enable Managed Disk Space for disk data** option and click **OK**.
3. From the Mount Paths tab of the **Library Properties** dialog box, set the start and stop data aging disk capacity thresholds in the **Start aging when data occupied on disk is n %** and the **Stop aging when data occupied on disk is n %** boxes, and click **OK** to save changes.

MANUALLY RETAIN A JOB ON A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To manually retain a job on a storage policy copy:

From the CommCell Console, data protection operations can be manually retained. However, if necessary, the Command Line Interface jobretention operation can be used to manually retain any type of data protection operation for all agent types.

1. From the right pane of the CommCell Browser, right-click the storage policy copy whose jobs you want to manually retain, click **View** and then click **Jobs**.
2. Filter the necessary options in the Job Filter for Storage Policy Copy dialog box. Click **OK**.
3. A list of jobs associated with this storage policy copy are displayed in the Jobs for Storage Policy Copy window.
4. Right-click the appropriate job, then click **Retain Job**.
 - To select multiple jobs, hold down the **Ctrl** key, and right click on the jobs.
5. Specify the retention end time in the Manual Retention End Time for Job dialog box.
6. The status for the job is then displayed in the Manual Retention End Time field in the Jobs for Storage Policy Copy window.
7. Click **OK**.
8. If you want this job to be pruned during data aging, right-click the same job, then click **Change Retention**.
 - To select multiple jobs, hold down the **Ctrl** key, and right click on the jobs.
9. Select **Do Not Retain Job** in the Manual Retention End Time for Job dialog box.

PERFORM A DISK VOLUME RECONCILIATION JOB AND RECONCILE THE DIFFERENCES

Required Capability: See Capabilities and Permitted Actions

▶ To an orphaned job or an orphaned data using Disk Volume Reconciliation:

1. From the CommCell Browser, right-click the non-deduplicated storage policy copy for which you wish to perform volume reconciliation, click **All Tasks**, click **Disk Volume Reconciliation** and select **Collect Data From Media**.
2. Click **Yes** in the confirmation dialog box.
3. The disk volume reconciliation job is performed and the details are displayed in the View Results of Disk Admin Job dialog box.
4. The Orphaned Media Space tab displays the list of data that does not have a corresponding job. Right-click the desired orphaned media and click **Delete Contents**. The selected data is deleted from the media.
5. The Orphaned Jobs tab displays the list of jobs without corresponding data on the media. Right-click the desired orphaned job and click **Delete**. The selected job is deleted from CommServe database.
6. Click **Close** to exit.

VIEW THE RESULTS OF A DISK VOLUME RECONCILIATION JOB AND RECONCILE THE DIFFERENCES

Required Capability: See Capabilities and Permitted Actions

▶ To view the results of a previously executed disk volume reconciliation job and reconcile the differences:

1. From the CommCell Browser, right-click the non-deduplicated storage policy copy for which you perform volume reconciliation, click **All Tasks**, click **Disk Volume Reconciliation** and select **View Details and Reconcile**.
2. The results of the previously executed disk volume reconciliation job is displayed in the View Results of Disk Admin Job dialog box.

3. The Orphaned Media Space tab displays the list of data that does not have a corresponding job. Right-click the desired orphaned media and click **Delete Contents**. The selected data is deleted from the media.
 4. The Orphaned Jobs tab displays the list of jobs without corresponding data on the media. Right-click the desired orphaned job and click **Delete**. The selected job is deleted from CommServe database.
 5. Click **Close** to exit.
-

MARK A STORAGE POLICY COPY INACTIVE

Required Capability: See Capabilities and Permitted Actions

▶ To mark a copy inactive:

1. From the right pane of the CommCell Browser, right-click the storage policy copy for which you wish to change the active settings and then click **Properties**.
 2. From the General tab of the **Copy Properties** dialog box, de-select the **Active** checkbox.
 3. Click **OK** to save your changes.
-

MARK THE ACTIVE MEDIA OF A STORAGE POLICY COPY FULL

Required Capability: See Capabilities and Permitted Actions

▶ To mark the active media of a storage policy copy full:

1. From the CommCell Browser, right-click the storage policy copy that you want mark the active media full, click **All Tasks**, and then click **Mark Active Media Full**.
 2. Click **Yes** to the confirmation message.
 3. The active media is full.
-

PICK A JOB ON A STORAGE POLICY COPY FOR DATA VERIFICATION

Required Capability: See Capabilities and Permitted Actions

▶ To select a job for data verification:

1. From the right pane of the CommCell Browser, select a storage policy, then right click the storage policy copy whose job(s) you want to pick for data verification, click **View** and then click **Jobs**.
 2. Filter the necessary options in the Job Filter for Storage Policy Copy dialog box. Click **OK**.
 3. From the Jobs for Storage Policy Copy window, right-click a job, then click **Pick for Data Verification**. If you then decide that you do not want this job to be verified during a data verification operation, right-click the backup and click **Do Not Verify Data**.
 4. Click **Close**.
-

PROMOTE A SYNCHRONOUS COPY TO BE A PRIMARY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To promote a synchronous copy to be the primary copy:

1. From the right pane of the CommCell Browser, right-click the secondary copy that you want to promote and then click **Properties**.
 2. From the General tab of the **Copy Properties** dialog box, select the **Primary Copy** checkbox, and click **OK**.
 3. Click **Yes** to the confirmation prompt that appears.
The selected copy is promoted to be the primary copy for the storage policy.
-

PRUNE A DISASTER RECOVERY BACKUP FROM A DISASTER RECOVERY BACKUP STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To prune a Disaster Recovery backup from a Disaster Recovery Backup storage policy copy:

1. From the right pane of the CommCell Browser, right-click a Disaster Recovery Backup storage policy copy whose backups you want to view, click **View** and then click **Jobs**.
 2. From the DR Backups For Copy dialog box, right click the Disaster Recovery backup job that you want to prune, then click **Prune Job**.
 3. Click **Yes** on the Confirmation pop-up that appears.
The Disaster Recovery backup job is pruned.
-

RE-ASSOCIATE THE SUBCLIENTS OF A STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

▶ To re-associate the subclients of a storage policy:

1. From the CommCell Browser, right-click the storage policy whose subclients you want to re-associate, and then click **Properties**.
2. Click the Associated Subclients tab of the **Storage Policy Properties** dialog box.
3. Select the subclients, and then click **Re-Associate**.
4. In the Storage Policy List dialog box, from the **Select storage policy to which all the subclients will be associated:** list, select a storage policy you would like to re-associate the subclients to. Click **OK**.

To re-associate the storage policy copy of a DDB Backup subclient, make sure to select non-deduplicated storage policy copy.

5. Click **OK** to save your changes.
-

SELECT THE CRITERIA FOR USING AN ALTERNATE DATA PATH

Required Capability: See Capabilities and Permitted Actions

▶ To select the criteria for using an alternate data path for a storage policy copy:

1. From the CommCell Browser, right-click the storage policy copy for which you select the criteria for using an alternate data path, then click **Properties**.
2. Click the Data Path configuration tab.
3. Select the **Automatically add datapaths for existing library** option, if you are using shared libraries.
4. Choose from the following options:

Choose the **Use Alternate Data Paths only when** option to indicate that alternate data paths must be used only when resources are busy and/or resources are offline. If you wish to choose this option, and wish to use some or all available resources in the CommCell, you must first share the index cache.

- Select the **When Resources are Offline** checkbox, to indicate that the storage policy copy must use an alternate data path, when resources are offline.

Resources are MediaAgent, Library, Master Drive Pool, Drive Pool, Drives in the drive pool and spare media in the scratch pool associated with this data path.

- Select **Immediately** to use an alternate data path at once, when resources are offline.
- Select **After** and type the minimum number of hours and minutes after which an alternate data path must be used when resources are offline

- Select the **When Resources are Busy** checkbox, to indicate that the storage policy copy must use an alternate data path when resources are busy.

Resources are all the drives in the library attached to the preferred MediaAgent.

- Select **Immediately** to use an alternate data path at once, when resources are busy.
- Select **After** and type the number of hours and minutes after which an alternate data path must be used, when resources are busy.

Choose the **Round-Robin between Data Paths** option to automatically fail over between all the available data paths. If you wish to choose this option, you must first share the index cache.

Choose the **Use preferred datapath** option to automatically perform LAN-free backups, wherever possible.

5. You can now add the appropriate data paths as described in Add a Data Path to a Storage Policy Copy.
-

SET A DATA PATH AS THE DEFAULT DATA PATH

Required Capability: See Capabilities and Permitted Actions

▶ To set a data path as the default data path from a storage policy copy:

1. From the CommCell Browser, right-click the storage policy copy for which you wish to set as the preferred data path, then click **Properties**.
2. Click the Data Paths tab.
3. Click the data path you wish to set as the preferred data path from the list.
4. Click **Set Default**.

The data path is set as the default data path. Notice the tick mark in the icon displayed in the **Status** column.

5. Click **OK** to save the information.

SPECIFY THE SOURCE COPY FOR AN AUXILIARY COPY OPERATION

Required Capability: See Capabilities and Permitted Actions

▶ To specify the source copy from which data will be copied to this copy during an auxiliary copy operation:

1. From the right pane of the CommCell Browser, right-click the storage policy copy for which you wish to specify the source copy, and then click **Properties**.
2. From the Copy Policy tab of the **Copy Properties** dialog box, select a source copy from the **Specify Source for Auxiliary Copy** list box.

Before specifying the source copy, in the **Association** tab, make sure that the both the storage policy copies have same CommCell entities (clients or subclient etc.,) associated or this copy has a fewer CommCell entities associated than the source copy.

3. Click **OK** to save your changes.

START AN AUXILIARY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To start an auxiliary copy:

1. From the CommCell Browser, right-click the storage policy for which you want to perform an auxiliary copy, click **All Tasks**, and then click **Run Auxiliary Copy**.
2. In the **Auxiliary Copy** dialog box, the Storage Policy field is already populated with the name of the Storage Policy you selected.
3. If the source copy is configured with a shared library, select the **Source MediaAgent** for the auxiliary copy.
4. Select **All Copies** to copy data from the source copy to all secondary copies defined, or select a copy from the *Select a Copy* list box.
5. Select **Start new media** to copy the data to a different tape or optical media. On a disk, this option, when selected, creates a new volume folder for the operation.
6. Select the number of streams to copy in parallel from the **Number of Streams to Copy in Parallel** pane, or select **Allow Maximum**.
7. Select **Mark media full after successful operation** to mark the media that is used for this operation full after the auxiliary copy operation has successfully completed.
8. Select **Select Most Recent Full Backup When Auxiliary Copy Starts** to have the most recent successful full backup for each subclient copied when the Auxiliary Copy job is run.
9. From the Job Initiation tab on the **Auxiliary Copy** dialog box, select the time for this job to run or choose to **Run Immediately**. You can also configure an alert for this job.
10. Click **Advanced** to configure the **Vault Tracker**, **Startup** and **Job Retry** options.
 - Click **Vault Tracking** to select additional Vault Tracker options for this operation from the Vault Tracking dialog box.

Note: This option is only available if a Vault Tracker license is available in the CommServe.
 - Click **Startup** to change the priority of this job and, if necessary, to start this job in a suspended state from the Startup dialog box.
 - Click the **Job Retry** tab to specify the job running time and the number of job retries. See Restarting Jobs and Job Running Time for more information.



The **Number of Retries** specified for this particular job will only be used by the system if Auxiliary Copy was configured as a **Restartable** job type in the Job Management Control Panel. For procedures, see Specify Job Restartability for the CommCell.

11. Click **OK** to start the auxiliary copy operation. A progress bar displays the progress of the operation.
-

VIEW THE AGED JOBS OF A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To view the aged jobs of a storage policy copy:

1. From the right pane of the CommCell Browser, right-click the storage policy copy whose aged backups you want to view, click **View** and then click **Jobs**.
 2. Filter the necessary options in the Job Filter for Storage Policy Copy dialog box.
 3. Click the **Advanced** button, and select the **Include Aged Jobs** or **Show only Aged Jobs** options.
 4. Click **OK**.
 5. The Job for Storage Policy Copy window that appears displays the jobs that were pruned from the selected storage policy copy as dimmed.
 6. Click **Close**.
-

VIEW THE AGED MEDIA OF A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To view the aged media associated with a storage policy copy:

1. From the right pane of the CommCell Browser, right-click the copy whose aged media you want to view, click **View** and then click **Aged Media**.
The Media List dialog box displays information about media that contains data that was pruned from the selected storage policy copy.
 2. Click **Close**.
-

VIEW THE EVENTS OF A JOB ON A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To view the events of a job on a storage policy copy:

1. From the right pane of the CommCell Browser, select a storage policy, then right click the storage policy copy whose jobs you want to view, click **View** and then select **Jobs**.
 2. If you are viewing jobs for a storage policy copy used by *iDataAgents* and/or *DataArchiver Agents*, filter the necessary options in the Job Filter for Storage Policy Copy dialog box. Click **OK**. If you are viewing jobs for a DR Backup storage policy, then skip to the next step.
 3. A list of jobs associated with the storage policy copy is displayed in the Jobs for Storage Policy Copy window or the DR Backups For Copy window.
 4. Right click the job you want to view, then select **View Events**. The All Found Events window is displayed. Use this window to view all of the events associated with this particular job.
 5. Click **OK**.
 6. Click **Close**.
-

VIEW THE ITEMS THAT FAILED FOR A JOB ON A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To view the items that failed for a job on a copy.

1. From the right pane of the CommCell Browser, select a storage policy, then right click the storage policy copy whose jobs you want to view, click **View** and then click **Job**.
 2. Filter the necessary options in the Job Filter for Storage Policy Copy dialog box. Click **OK**.
 3. A list of jobs associated with the storage policy copy is displayed in the Jobs for Storage Policy Copy window.
 4. Right click the job you want to view, then click **View Failed Items**.
 5. Click **OK**.
 6. Click **Close**.
-

VIEW THE JOB DETAILS OF A JOB ON A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To view the job details of a job on a storage policy copy:

1. From the right pane of the CommCell Browser, select a storage policy, then right click the storage policy copy whose jobs you want to view, click **View** and then click **Jobs**.
 2. If you are viewing jobs for a storage policy copy used by *iDataAgents* and/or *DataArchiver* Agents, filter the necessary options in the Job Filter for Storage Policy Copy dialog box. Click **OK**. If you are viewing jobs for a DR Backup storage policy, then skip to the next step.
 3. A list of jobs associated with the storage policy copy is displayed in the Jobs for Storage Policy Copy window or the DR Backups For Copy window.
 4. Right click the job you want to view, and then click **View Job Details**. The details of the job you selected is displayed.
 5. Click **OK**.
 6. Click **Close**.
-

VIEW THE JOBS OF A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To view the jobs on a storage policy copy:

1. From the right pane of the CommCell Browser, right-click the storage policy copy whose data protection operations you want to view, click **View** and then click **Jobs**.
 2. Select the necessary filter options in the Job Filter for Storage Policy Copy dialog box.
 3. Click the **Advanced** button for additional filter options in the Jobs in Storage Policy Advanced Filter Options dialog box.
 4. Click **OK**.
 5. A list of jobs associated with a storage policy copy is displayed in the Jobs for Storage Policy Copy window.
 6. Click **OK**.
-

VIEW THE JOBS SCHEDULED FOR A STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

▶ To view the jobs scheduled for a storage policy:

From the CommCell Browser, right-click the storage policy for which you want to view the jobs scheduled,

click **All Tasks**, and then click **Schedules**. The Scheduled Jobs Dialog dialog box displays the jobs scheduled for this storage policy.

VIEW THE JOBS SCHEDULED FOR A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To view the jobs scheduled for a storage policy copy:

1. From the CommCell Browser, right-click the storage policy copy that you want to view the jobs scheduled for, click **All Tasks**, and then click **Schedules**.
A list of the jobs scheduled for this copy is listed in the Scheduled Jobs dialog box.
 2. Click **OK**.
-

VIEW RETAINED JOBS FOR A STORAGE POLICY COPY

▶ To view the list of all retained jobs for specific storage policy copy:

1. Logon to the CommServe computer.
2. From the command prompt, navigate to `<Software_Installation_Path>\Base`
3. Run the following command:

```
operation execscript -sn ListManuallyRetainedJobs.sql -si StoragePolicyName -si CopyName
```

WHERE

- StoragePolicyName - Name of the storage policy
 - CopyName - Name of the storage policy copy
-

VIEW THE MEDIA NOT COPIED

Required Capability: See Capabilities and Permitted Actions

▶ To view the media necessary for an auxiliary copy to run from the primary copy to all secondary copies, or to a specific copy:

1. From the CommCell Browser, right-click a storage policy, or right-click a primary or secondary storage policy copy that you want to view the media necessary for an auxiliary copy operation, click **View** and then click **Media Not Copied**.
 2. A list of the media necessary for the auxiliary copy operation is displayed in the Media Not Copied dialog box.
 3. Click **Close**.
-

VIEW THE MEDIA OF A JOB ON A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To view the media of a job on a storage policy copy:

1. From the right pane of the CommCell Browser, select a storage policy, then right click the storage policy copy whose jobs you want to view, click **View** and then click **Jobs**.
 2. If you are viewing jobs for a storage policy copy used by *iDataAgents* and/or *DataArchiver Agents*, filter the necessary options in the Job Filter for Storage Policy Copy dialog box. Click **OK**. If you are viewing jobs for a DR Backup storage policy, then skip to the next step.
 3. A list of jobs associated with the storage policy copy is displayed in the Jobs for Storage Policy Copy window or the DR Backups For Copy window.
 4. Right click the job you want to view, then click **View Media**.
 - To select multiple jobs, hold down the **Ctrl** key, and right click on the jobs.
 5. The Media Used By Job ID window appears.
 6. Click **OK**.
 7. Click **Close**.
-

VIEW THE MEDIA OF A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To view the media associated with a storage policy copy:

1. From the right pane of the CommCell Browser, right-click the copy whose media you want to view, click **View** and then click **Media**.
The Media List dialog box that appears displays information about media that contains data from the selected storage policy copy.
 2. Click **Close**.
-

VIEW THE MOUNT PATHS OF A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To view the mount paths associated with a storage policy copy:

1. From the right pane of the CommCell Browser, right-click the storage policy copy whose mount paths you want to view, click **View** and then click **Media**.
The Media List dialog box that appears displays all mount paths in a disk library that contain valid data for the storage policy copy.
 2. Click **Close**.
-

[Back To Top](#)

Alternate Data Paths (GridStor®)

Topics | How To | Troubleshoot | Examples | Support | Related Topics

Overview

Configuring Alternate Data Paths for Primary Copies

- Adding Data Paths to Primary Copies
- Automatically Adding Data Paths for Existing Libraries
- Defining the Criteria for Using Alternate Data Paths
- Setting the Number of Streams for Alternate Data Paths

Configuring Alternate Data Paths for Secondary Copies

Configuring Alternate Data Paths for Subclients

Data Protection Operations using Alternate Data Paths

- Media Usage

Data Recovery Operations using Alternate Data Paths

- When Media is Available in a Library
- When Media is Exported

Important Considerations

- General Considerations
- Clustered Environment
- Considerations for NAS attached libraries
- Considerations for backing up the Microsoft Virtual Server
- Configuring Round Robin of HBA Cards
- Round Robin with Multiplexing

Best Practices

OVERVIEW

Several data paths can be added to a storage policy copy, to ensure the success of data protection and other operations conducted using the storage policy. A data path is the combination of MediaAgent, Library, Drive Pool and Scratch Pool used by the storage policy copy to perform a data protection operation. Each storage policy copy has a default data path which will be used to perform data protection operations. In addition, you can also define alternate data paths in each of the storage policy copies.

Alternate data paths provide the following advantages:

- Alternate data paths provide the facility to automatically switch over to an alternate data path, when one of the components in the default data path is not available. In addition to ensuring the successful completion of data protection jobs, alternate data paths also utilize available libraries and drives in the event of failure or non-availability of these resources.
- Alternate data paths can be used to minimize media utilization by routing data protection operations from several subclients to the same storage policy and hence the same media, instead of creating several storage policies which in turn utilizes a different media for each subclient.
- In addition, the facility to load balance (round robin) between alternate data paths provides the mechanism to load balance or evenly distribute data protection operations between available resources.

Alternate data paths are supported for both the primary and secondary copies associated with storage policies for all libraries. (See Alternate Data Paths (GridStor) -Support for additional details.) Note, however, that there are several differences between the operations performed using primary and secondary copies with alternate data paths. These are explained in detail in the following sections. Note that within the selected storage policy (and its data paths), the facility to define a subset of the data paths at the subclient level is also provided.

LICENSE REQUIREMENT

This feature does not require any additional license.

CONFIGURING ALTERNATE DATA PATHS FOR PRIMARY COPIES

The following options are provided while defining alternate data paths on primary copies:

- Facility to automatically configure the data paths for shared libraries.
- Facility to select the alternate data path based on any one of the following:
 - Use alternate data path when resources are busy or offline,
 - Load balance (Round Robin) between available resources, or
 - Use alternate data path to perform LAN-free data protection operations.

Note that the client and the MediaAgent must be on the same computer, in order to perform a LAN-free operation.

The following sections describes each of these options in detail.

ADDING DATA PATHS TO PRIMARY STORAGE POLICY COPIES

If a storage policy is created during the library configuration process, a default data path is created for the primary copy using the MediaAgent, Library, Drive Pool and default scratch pool combination for drive pools configured within the library. If you create a new storage policy, you must specify a Library, MediaAgent, Drive and Scratch pool combination for the primary copy.

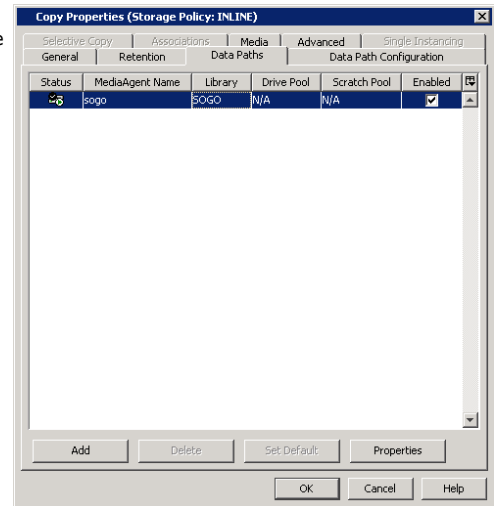
Additional data paths for the primary copy can be defined from the Data Paths tab of the **Copy Properties** dialog box.

See Add a Data Path to a Storage Policy Copy for step-by-step instructions.

The data paths that are available to be added as alternate data paths, depends on the option selected in this dialog box. In addition some of the options may require the index cache to be shared to be accessed as a data path. (These details are explained in the subsequent sections of this document.)

After defining additional data paths, if necessary, you can set any of the data paths as the default data path for the storage policy copy.

See Set a Data Path as the Default Data Path for step-by-step instructions.



AUTOMATICALLY ADDING DATA PATHS FOR EXISTING LIBRARIES

When multiple MediaAgents share the same library (SAN DDS, or direct-attached shared library configurations) the system can automatically add the alternate data paths for each of the storage policies, when this option is enabled. As each of these data paths (MediaAgent, Library, Drive Pool and Scratch Pool) use the same resources, additional index cache configuration is not required. In addition, the criteria for using the alternate data path (described in the following section) must also be specified.

DEFINING THE CRITERIA FOR USING ALTERNATE DATA PATHS

A storage policy can be configured to use an alternate data path using the following criteria:

- When resources are busy or offline - use this option to configure your system to use an alternate data path when resources are busy or offline.
- Load balance between the data paths - use this option to evenly distribute data protection operations amongst drive-pools, thereby not overloading a specific drive-pool.
- LAN preferred data path - use this option to automatically perform LAN-free data protection operations.

Criteria for using alternate data paths can be defined from the Data Path Configuration tab of the **Copy Properties** dialog box. See Select the Criteria for using an Alternate Data Path for step-by-step instructions.

WHEN RESOURCES ARE BUSY OR OFFLINE

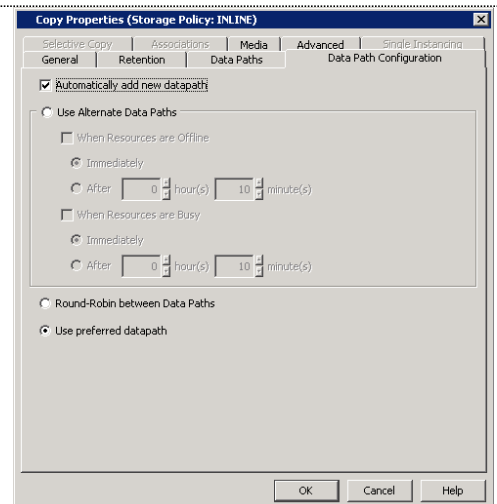
When this option is selected the system automatically uses an alternate data path when resources are busy or offline.

If the **When resources are offline** option is selected, the storage policy will use an alternate data path when one of the following resources is broken or not available and hence marked as **offline** by the user or by the MediaAgent:

- MediaAgent
- Library
- Master Drive Pool
- Drive Pool
- All the drives in the Drive Pool
- No spare media in the scratch pool associated with the copy

If the **When resources are busy** option is selected, the storage policy will use an alternate data path when all the drives in the library are busy.

In both the above options, you can indicate whether an alternate data path must be used immediately or after the specified amount of time.



The list of data paths that will be available when this option is selected will include the following:

- Data paths associated with MediaAgents that share the library with the default data path. In this case, it is not necessary to share the index cache, but the number of alternate data paths will be limited to the list of MediaAgents that share a library.
- List of MediaAgents that share the index with the MediaAgent associated with the default data path. In this case, as other libraries can be included in the list of data paths several alternate data paths can be added. However, keep in mind that the index cache must be shared.

See Index Cache for information on the options available for index cache sharing.

ROUND ROBIN BETWEEN DATA PATHS

When this option is selected the system automatically performs load-balancing between the resources (drives in a library or writers in a disk library) available in all the data paths. Keep in mind that the load-balancing is performed at the drive-pool level as opposed to the MediaAgent level.

The following section illustrates the load balancing operation:

If you have defined 5 data paths with 15 resources, and have 25 data protection operations running concurrently at a given time, load balancing would cause the following to occur:

- The first operation will be performed on the default data path.
- The second (and subsequent operations) will be performed in the next data paths, in the order in which it is added in the **Data Paths** tab of the **Copy Properties** dialog box.
- Once the first 5 operations reserves the resources, the sixth operation will be routed to another resource in the default data path, if one is available. The subsequent operations will be routed to the next data path in the order in which it is added in the **Data Paths** tab of the **Copy Properties** dialog box, until all the resources are occupied.
- Once all the resources are used, the system will constantly check for an available resource, and as soon as one is freed the next job in the queue will be automatically routed to use that resource.

All the MediaAgents that share the index cache with the MediaAgent in the default data path will be available as an alternate data path when this option is selected.

See Also:

- Load Balancing Using Spill and Fill

USE PREFERRED DATAPATH

When this option is selected the system automatically performs LAN free backups wherever possible. It is not necessary to share the index cache for this operation and all available MediaAgents will be available as an alternate data path when this option is selected.

SETTING THE NUMBER OF STREAMS FOR ALTERNATE DATA PATHS

When you add or delete an alternate data path, you must reset the number of streams that are defined for the Storage Policy.

The maximum number of streams for a storage policy, with a primary copy that has alternate data paths should be equal to the sum of all unique drives associated with the drive pools and/or the sum of all writers in the mount paths associated with disk libraries in all alternate data paths. Consider the following scenarios, when the maximum number of streams defined is either too many or too little, when you have specified the criteria to immediately use alternate data paths when resources are busy:

- If the maximum number of streams in a Storage Policy is less than the sum of drives/writers in mount paths associated with all the data paths in a primary copy, then all the resources (drives/writers in mount paths) available in the data paths will not be utilized. For example, if the sum of drives/writers in mount paths in all the data paths is 20, and you have specified 10 as the maximum number of streams, at any given time, only 10 jobs would succeed and the remaining jobs would go into the **Waiting** status with the **Job Delay Reason** stating that no resources are available for the job. In such a situation to fully utilize all the available resources, the maximum number of streams should be set to 20.
- If the maximum number of streams in a Storage Policy is more than the sum of drives/writers in mount paths associated with all the data paths in a primary copy, only as many jobs as the total number of available drives will succeed. For example, if the sum of drives/writers in mount paths in all the data paths is 20, and you have specified 30 as the maximum number of streams, at any given time, only 20 jobs would succeed and the remaining jobs would go into the **Waiting** status with the **Job Delay Reason** stating that no resources are available for the job.

JOBS WITH MULTIPLE STREAMS

For multi-stream jobs, the failover will occur only when all the streams have the necessary resources. For example, if you have a job with 5-streams, and if the necessary resources are not available in the default data path, the failover will occur only when the alternate data path has all the necessary resources - MediaAgent, Library and drive pool with 5 drives. This is the case, irrespective of the criteria (When resources are busy, Round Robin between Data Paths options) specified to use alternate data paths.

CONFIGURING ALTERNATE DATA PATHS FOR SECONDARY COPIES

Data paths can be added to secondary copies to enable LAN free Auxiliary Copy operations, so that network resources can be freed wherever possible.

ADDING DATA PATHS TO SECONDARY COPIES

When a secondary copy is created, you must select the default data path for the copy by selecting the MediaAgent, Library, Drive Pool and scratch pool combination. This data path will be used to access the secondary copy when an Auxiliary Copy operation is performed.

However you can add data paths for the secondary copy so that any Auxiliary Copy operations can be performed using a LAN-free data path.

As with the primary copy, additional data paths for the secondary copy can also be defined from the Data Paths tab of the **Copy Properties** dialog box. (See [Add a Data Path to a Storage Policy Copy](#) for step-by-step instructions.)

Note that although the **Use preferred datapaths** option is selected, the LAN free Auxiliary Copy operations on the copy is *not* performed until the alternate data paths are selected.

When you add the data path for the secondary copy it is sufficient to add one path per MediaAgent-Library combination. The system automatically uses an available data path to perform LAN free Auxiliary Copy operations. Keep in mind, that when you add data paths in the secondary copies, the system automatically tries to perform a LAN-free read operation. (This is opposed to the primary copies, where the system strives to perform both the read and write operations when the LAN-free option is selected.)

See also:

Although common data paths are defined in primary and secondary copies, another data path is being used for Auxiliary Copy operations.

EXAMPLES

Alternate data paths on Secondary Copies can be used to perform LAN free Auxiliary Copy operations as follows:

- Using disk as primary and a tape/optical library for secondary copies. See [Example 1](#) for more information.
- Using a tape/optical library for both the primary and secondary copies. See [Example 2](#) for more information.

CONFIGURING ALTERNATE DATA PATHS FOR SUBCLIENTS

Each subclient can be configured with a subset of data paths from the data paths available in the storage policy associated with the subclient. The following options are provided while defining the data paths for a subclient:

- Facility to select a subset of data paths from the list of available data paths.
- Facility to assign a priority for the selected data paths.
- If necessary, facility to override the default data path on storage policy and use the other data path from the subset of data paths available for the subclient.

Note that **Override Datapaths** option is not supported if the subclient is associated with an Incremental Storage Policy.

Note that the data paths and the priority established at the subclient level takes precedence over the data paths defined at the storage policy copy.

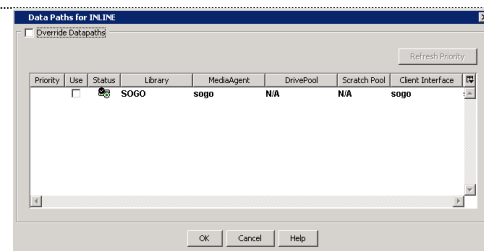
ADDING DATA PATHS TO SUBCLIENTS

By default, the system uses the data path associations defined in the primary copy of the storage policy to perform data protection operations. (This is depicted in the sample image shown on the right. Note that the **Override Datapaths** option is not selected and the default data path is displayed using a bold font-face and a special icon.) If necessary you can perform the following operations:

- Select a subset of the available data paths for the subclient.
- Set a priority for the selected data paths.

See the following procedures for step-by-step instructions:

- [Configure Data Paths for Subclients](#)
- [Assign Priorities for Subclient Data Paths](#)



POINTS TO REMEMBER

Consider the following for configuring data paths at the subclient level:

- Subclient data paths are supported by all agents that require an iDataAgent Backup Storage Policy.
 - If necessary, different data path subsets can be selected for database agents that use different storage policies for data and log files. (See, [Classification of Agents based on Index Usage](#) for a definition of database agents.)
- When a secondary (storage policy) copy is promoted as the primary copy, the data paths defined in the secondary copy is automatically used by the subclient. If necessary, you must establish the default data path and set the priority once the secondary copy is promoted.
- When a data path is deleted from the storage policy (or a library is deconfigured) the data path is automatically removed from the subclient.
- Subclient data paths are not supported by Subclient Policies.
- Subclient data paths cannot be configured using the Command Line interface.
- In the case of Incremental Storage Policies, which uses two different storage policy copies for full and non-full backups, different data path subsets can be

selected for full or non-full backups using the same or a different storage policy. In such a situation, make sure that the selected data paths share the index.

EXAMPLES

The subclient data paths can be used effectively in the following situations:

- To configure subclients to use certain data paths, and minimize media utilization. See Example 1 for information on how this works.
- Restrict some subclients to use only a subset of data paths and at the same time reduce media utilization. See Example 2 for information on how this works.

DATA PROTECTION OPERATIONS USING ALTERNATE DATA PATHS

When a data protection operation is initiated, the storage policy copy attempts to write the data using the default data path. If the default data path is not available, an alternate data path is automatically used to perform the data protection operation. If more than one alternate data path is defined, the first data path listed in the Data Paths tab of the **Copy Properties** dialog box is selected, followed by the second and so on until a data path is available.

MEDIA USAGE

If both the default and alternate data paths are configured to use the same library, as a result of a shared library configuration (configured as a SAN DDS library or direct-attached shared library) the MediaAgent will automatically use the appropriate **Assigned** media for the data protection operation.

If the default and alternate data paths are configured to use different libraries, the MediaAgent, marks the previously used **Assigned** media as **Appendable** and uses a new media from the library associated with the alternate data path.

Such **Appendable** media can be re-used in the library by enabling the **Use Appendable Media** option in the Library Properties dialog box associated with the library.

DATA RECOVERY OPERATIONS USING ALTERNATE DATA PATHS

Data can be restored/recovered from any compatible library and drive type in the CommCell.

WHEN MEDIA IS AVAILABLE IN A LIBRARY

When a Data Recovery operation is initiated, and if the media is not exported, the software attempts to restore/recover data using the appropriate data path associated with that library, instead of the default data path in the following order:

- The first priority is provided to the path which results in LAN-free restore/recover to the client computer from which the restore/recover operation was initiated. LAN-free operation is possible only when the client initiating the restore/recover operation and MediaAgent are on the same computer.
- If the LAN-free operation is not possible, then the Data Recovery operation attempts to restore/recover data using the default data path.
- If the appropriate media is not available in all these data paths, the software automatically identifies the media in which the data resides and performs the restore/recover operation from that library.

WHEN MEDIA IS EXPORTED

When a Data Recovery operation is initiated, and if the media is exported, the software will prompt you to import the media in the appropriate MediaAgent computer. This is done as follows:

If a LAN-free restore/recover is possible, the restore/recover operation would prompt you to import the media in the appropriate library from which the LAN-free restore is possible. (LAN-free restore will be possible only when the client initiating the restore/recover operation and MediaAgent are on the same computer.)

If the LAN-free restore/recover operation is not possible, then the operation would prompt you to import the media in the library which was last used to write to the media.

If the resources in that library are offline, the restore/recover operation would prompt you to import the media in the library associated with the default data path.

If the resources associated with the default data path are offline, then the restore/recover operation identifies a library from an alternate data path which are assigned in the data path list, to import the media.

See Also:

- Restore From Anywhere

IMPORTANT CONSIDERATIONS

Consider the following information when using alternate data paths:

GENERAL CONSIDERATIONS

- Job Preemption is supported on Default/LAN-free backups (i.e., if GridStor is configured for User Preferred Datapath). It is not supported for the jobs that are run using data paths with the Round Robin configuration.
- Change Data Path (right-click option) should not be performed on Storage Policies with Storage Policy Copies that have Alternate Data Paths (GridStor). If Change Data Path is performed on such a setup, data recovery operations can be performed from the media. However, subsequent data protection operations will not re-use the migrated media.

CLUSTERED ENVIRONMENT

- On clustered computers the system automatically performs LAN free operations for Agents installed on the virtual machines with the storage policy copy (attached to the subclient) pointing to the MediaAgent on the physical node. Consider the following example:

A file system *iDataAgent* is installed on Virtual Machine (VM1) and can be controlled by Node 1 or Node 2 at any given time.

The subclient (subclient1) associated with this file system *iDataAgent* on VM1 points to a Storage Policy Copy (SP1) which in turn uses the following data paths:

- default data path using MediaAgent (Node1) and Library 1
- alternate data path MediaAgent (Node2) and Library 1

When a backup is run on subclient1, the system automatically figures out the node controlling VM1 and will use the appropriate MediaAgent. For example if VM1 is controlled by Node 2 at the time of the backup, the system automatically uses the MediaAgent on Node2 to perform the LAN free backup.

This capability allows you to install the MediaAgent on the physical node of a cluster. (Instead of multiple instances if installed in the cluster group.) However you will need GridStor® to provide failover capabilities.

CONSIDERATIONS FOR NAS ATTACHED LIBRARIES

- Data paths for NAS attached libraries can only be added if the MediaAgent used in that data path also has the File System *iDataAgent* installed on that computer. This is applicable only for Windows MediaAgents.
- For NAS environments, refer to Storage Policy Considerations for additional information.

CONSIDERATIONS FOR BACKING UP THE MICROSOFT VIRTUAL SERVER

- If the MediaAgent software is installed in the cluster server, configure a disk library to backup the data.
- If you wish to configure a tape/optical library, install the MediaAgent software on the physical computer.

Add a data path which uses this MediaAgent, Library, Drive Pool and Scratch Pool combination to the Storage Policy used to backup the cluster server. (See Add a Data Path to a Storage Policy Copy for step-by-step instructions.)

Assign this as a high priority data path in the subclient(s) used to backup the cluster server. (See Assign Priorities for Subclient Data Paths for step-by-step instructions.)

CONFIGURING ROUND ROBIN OF HBA CARDS

When the devices are configured from different HBA cards on the same host as distinct drive pools, each of these drive pools can be added as data paths on the storage policy. For LAN storage policies, these data paths can be added as additional data paths with the **Round-Robin between Data Paths** option enabled. This will automatically round robin the data protection jobs between these HBA cards.

For LAN free Storage Policies, the additional LAN free data paths for the secondary HBA cards can be added as data paths and the software will automatically pick the least used LAN free data path.

(See Configuring Dual Host Bus Adaptors (HBA) for information on configuring HBA cards.)

ROUND ROBIN WITH MULTIPLEXING

When a storage policy is configured for multiplexing and contains data paths to be used in round-robin fashion, then the round-robin option is completely utilized before using multiplexing.

For example, consider a storage policy with 3 data paths configured in the round robin mode and multiplexing set to 2. If 4 backup jobs kick off simultaneously, then the three available data paths are utilized first and multiplexing is applied for the fourth job only.

BEST PRACTICES

Consider the following information and recommendations, while creating and using alternate data paths:

- For LAN-free clients do not enable the **When Resources are Busy** option to choose an alternate data path. This will ensure LAN free operations, wherever

possible.

- It is not necessary to share the index on MediaAgents with LAN-free data paths. However, even if one additional alternate data path on the LAN is added to the storage policy, you must share the index for all the MediaAgents in the data path list.
 - Create and use less number of storage policies, as large number of storage policies will result in the fragmentation of data on media. Consider the following:
 - Control data retention by creating copies within the Storage Policies. (As opposed to creating many storage policies with different retention periods.)
 - Consolidate each Client's data by creating Subclient-Based Storage Policy Copies.
 - Before you deconfigure a library, verify and ensure that none of the Storage Policy Copy's default data path points to the library. (See View the Storage Policies Accessing a Library for step-by-step instructions on how to view the storage policies associated with a library.) If necessary, set an alternate data path as the default data path before deconfiguring the library.
- If you have a storage policy copy with no default data path, use **Change Data Path** option to migrate the storage policy to point to another data path. See Change Data Path for more information.
- NAS Load-Balancing - in addition to the resource load balancing that the Alternate Data Paths feature provides, NAS can be configured to load balance the processing tasks associated with backup, restore, and auxiliary copy jobs, which normally run on a single client machine, to spread the processing among different MediaAgent.

[Back to Top](#)

Alternate Data Paths (GridStor) - How To

[Topics](#) | [How To](#) | [Troubleshoot](#) | [Examples](#) | [Support](#) | [Related Topics](#)

Configure Data Paths for Storage Policies

- [Configure Multiple Data Paths for a Storage Policy Copy](#)
- [Select the Criteria for using an Alternate Data Path](#)
- [Add a Data Path to a Storage Policy Copy](#)
- [Delete a Data Path from a Storage Policy Copy](#)
- [Set a Data Path as the Default Data Path](#)
- [View Data Paths Associated With a Subclient](#)

Configure Data Paths for Subclients

- [Configure Data Paths for Subclients](#)
- [Assign Priorities for Subclient Data Paths](#)

CONFIGURE MULTIPLE DATA PATHS FOR A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To configure multiple data paths for a storage policy copy:

1. Select the criteria under which a storage policy copy must use an alternate data path, as described in [Select the Criteria for using an Alternate Data Path](#).
2. Depending on the criteria selected for using an alternate data path, you may have to share the indexes.
3. Add the data paths to storage policy copies for which you wish to add multiple data paths, as described in [Add a Data Path to a Storage Policy Copy](#).

The storage policy copy will automatically switch to an alternate data path, when the preferred data path is either offline or busy, as established in the criteria for using an alternate data path.

SELECT THE CRITERIA FOR USING AN ALTERNATE DATA PATH

Required Capability: See Capabilities and Permitted Actions

▶ To select the criteria for using an alternate data path for a storage policy copy:

1. From the CommCell Browser, right-click the storage policy copy for which you select the criteria for using an alternate data path, then click **Properties**.
2. Click the Data Path configuration tab.
3. Select the **Automatically add datapaths for existing library** option, if you are using shared libraries.
4. Choose from the following options:

Choose the **Use Alternate Data Paths only when** option to indicate that alternate data paths must be used only when resources are busy and/or resources are offline. If you wish to choose this option, and wish to use some or all available resources in the CommCell, you must first share the index cache.

- Select the **When Resources are Offline** checkbox, to indicate that the storage policy copy must use an alternate data path, when resources are offline.

Resources are MediaAgent, Library, Master Drive Pool, Drive Pool, Drives in the drive pool and spare media in the scratch pool associated with this data path.

- Select **Immediately** to use an alternate data path at once, when resources are offline.
- Select **After** and type the minimum number of hours and minutes after which an alternate data path must be used when resources are offline

- Select the **When Resources are Busy** checkbox, to indicate that the storage policy copy must use an alternate data path when resources are busy.

Resources are all the drives in the library attached to the preferred MediaAgent.

- Select **Immediately** to use an alternate data path at once, when resources are busy.
- Select **After** and type the number of hours and minutes after which an alternate data path must be used, when resources are busy.

Choose the **Round-Robin between Data Paths** option to automatically fail over between all the available data paths. If you wish to choose this option, you must first share the index cache.

Choose the **Use preferred datapath** option to automatically perform LAN-free backups, wherever possible.

5. You can now add the appropriate data paths as described in *Add a Data Path to a Storage Policy Copy*.

ADD A DATA PATH TO A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To add a data path to a storage policy copy:

1. From the CommCell Browser, right-click the storage policy copy for which you wish to add the data paths, then click **Properties**.
2. Click the Data Paths tab. Note that depending on the criteria selected for using an alternate data path, you may have to share the indexes.
3. Click **Add**.
4. From the Copy Data Path Candidates dialog box, select the data path candidates that you wish to add.

You can select multiple candidates by holding down the CTRL key and clicking on each of the data path candidates that you wish to select.

5. Click **Add**.
6. Click **OK**.
7. Click **OK** in the **Data Paths** tab to save the information.

DELETE A DATA PATH FROM A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To delete a data path from a storage policy copy:

1. From the CommCell Browser, right-click the storage policy copy for which you wish to delete a data path, then click **Properties**.
2. Click the Data Paths tab.
3. Click the data path you wish to delete from the list.
4. Click **Delete**. The data path is deleted.
5. Click **OK** to save the information.

- You cannot delete a data path that is set as the default data path.
- You can delete a data path when the associated storage policy is reserved for data protection operations.

SET A DATA PATH AS THE DEFAULT DATA PATH

Required Capability: See Capabilities and Permitted Actions

▶ To set a data path as the default data path from a storage policy copy:

1. From the CommCell Browser, right-click the storage policy copy for which you wish to set as the preferred data path, then click **Properties**.
2. Click the Data Paths tab.
3. Click the data path you wish to set as the preferred data path from the list.
4. Click **Set Default**.

The data path is set as the default data path. Notice the tick mark in the icon displayed in the **Status** column.

5. Click **OK** to save the information.
-

VIEW DATA PATHS ASSOCIATED WITH A SUBCLIENT

Required Capability: See Capabilities and Permitted Actions

▶ To view data paths:

1. From the CommCell Browser, right-click the subclient whose data paths you want to view, then click **Properties** from the shortcut menu.
 2. Click the Storage Device tab of the Subclient Properties dialog box.
 3. From the **Data [or Logs] Storage Policy** tab, click **Show Data Paths** to view the data paths used by the subclient to access the storage media for data protection operations. Click **Close** to exit the Data Paths dialog box.
 4. Click **OK** to exit the Subclient Properties Storage Device tab.
-

CONFIGURE DATA PATHS FOR SUBCLIENTS

Required Capability: See Capabilities and Permitted Actions

▶ To configure data paths for subclients:

1. From the CommCell Browser, right-click the subclient for which you wish to create the data paths, and then click **Properties**.
2. Click the Storage Device tab.
3. Click **Data Paths**.
4. From the Data Paths for <Storage Policy Name> dialog box, select the **Override DataPaths** option. This will allow you to define the necessary data paths at the subclient level.
5. From the list of data paths displayed in the bottom pane, select the **Use** option to choose a data path for the subclient.
6. If necessary assign a priority as described in Assign Priorities for Subclient Data Paths.
7. Click **OK** to save the changes.

The selected data paths will be used by the subclient for subsequent data protection operations.

ASSIGN PRIORITIES FOR SUBCLIENT DATA PATHS

Required Capability: See Capabilities and Permitted Actions

▶ To assign priorities for subclient data paths:

1. Follow the steps described in Configure Data Paths for Subclients.
2. From the Data Paths for <Storage Policy Name> dialog box, after selecting the data paths for the subclient by clicking the **Use** option, click **Priority** and type a number as priority.
3. If necessary, click the **Refresh Priority** button to sort the display based on the established priority.
4. Click **OK** to save the changes.

The data path with the smallest number will be established as a high priority data path, while data paths with bigger numbers will be established as low priority data paths.

Data Multiplexing

Topics | How To | Support | Related Topics

Overview

How Data Multiplexing Works

Configure for Data Multiplexing

Determining the Multiplexing Factor

Perform a Multiplexed Data Protection Operation

Impact of Data Multiplexing on Data Recovery Operations

Best Practices

License Requirement

Support Information - Storage Policy Copy

OVERVIEW

In a typical storage policy configuration, many clients/subclients can point to the same storage policy. Each storage policy copy has one or more streams related to the number of drives in a drive pool. On a particular stream, only one subclient can perform a data protection operation at any one time. The limit for the number of data protection operations that can go to any one stream is one. Therefore, only one data protection operation can be sent to a media/drive at any one time.

This limitation has its disadvantages. Backing up one client/subclient to a single piece of media does not fully utilize the drive's throughput, as the backing up of client data can be much slower than actual speeds of the tape.

In a large enterprise with many clients, many data protection operations may need to be performed within a fixed backup window. This may lead to high hardware requirement costs if the drive or media used for those data protection operations is being under utilized.

To optimally use the high speed tape drives available today, data from several clients/subclients can be multiplexed and written to media.

CHUNK SIZE OF DATA THAT IS MULTIPLEXED

Multiplexed data chunk sizes are determined by the type of data that is being multiplexed; file system data and database data.

- If the first backup is a file system type backup, all other backups joining multiplexing will have a chunk size of 4 GB.
- If the first backup is a database type backup, all other backups joining multiplexing will have a chunk size of 16 GB.

Multiplexed data is aged when all jobs (multiplexed) on a single chunk have met the defined retention rules of their associated storage policy copy. For more information, see Data Aging.

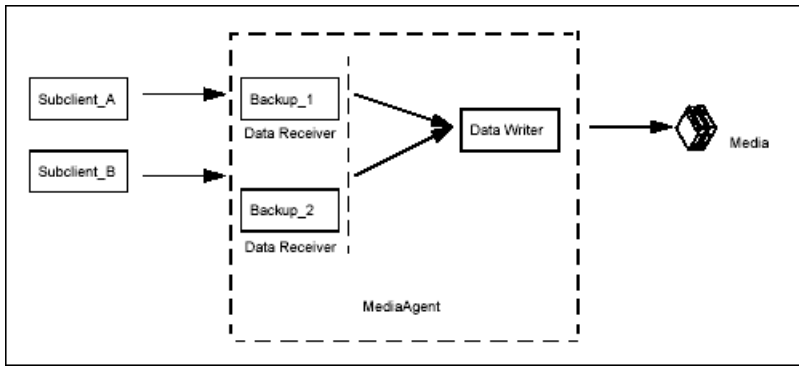
- Data in a storage policy copy enabled for Deduplication can not be multiplexed. Therefore, Data Multiplexing is not supported if the storage policy copy is enabled with Deduplication. However, a SILO copy supports Data Multiplexing even if the storage policy copy is enabled with Deduplication.
 - Multiplexed data cannot be copied to a storage policy copy enabled for Deduplication. Therefore, a storage policy copy enabled for Deduplication can not have a direct or indirect source copy enabled for Data Multiplexing.
 - An Auxiliary Copy can be configured with Data Multiplexing when the source copy is enabled for Deduplication.
-

HOW DATA MULTIPLEXING WORKS

During a data protection operation, agent data is transferred to media over a data pipeline. This data is transferred by data movers that read agent data then write the data to the media.

During data multiplexing, many such data movers must read and write data to the same piece of media. To achieve this, these data movers are comprised of two components, data receivers and data writers. During data multiplexing, one data receiver per backup stream reads the data coming through the data pipeline. One data writer per media receives data from multiple data receivers then writes data to the media.

In the sample image that follows, `Subclient_A` and `Subclient_B` are being backed up at the same time and their data is being multiplexed. Multiple data receivers read the data and then one data writer writes the data to a single piece of media.



CONFIGURING FOR DATA MULTIPLEXING

To configure your subclients to use this feature, data multiplexing must be enabled from the **Media** tab of the **Copy Properties** dialog box of the primary copy.

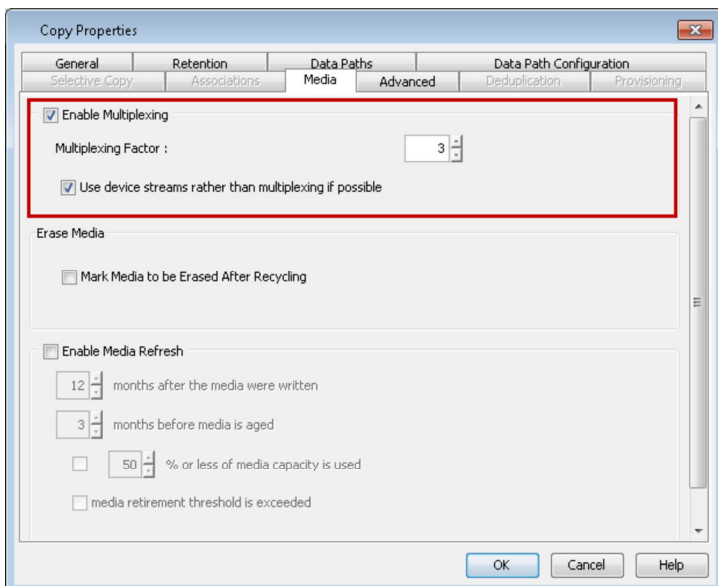
For example, if three subclients of this storage policy are to be backed up in a multiplexed manner, then the multiplexing factor would be set to three.

You can enable multiplexing for the copy as follows:

1. From the CommCell Browser, navigate to **Policies | Storage Policies | <Storage_Policy>**.
2. Right-click **<Storage Policy Copy>** and click **Properties**.
3. Click the **Media** tab.
4. Select the **Enable Multiplexing** check box and select the **Multiplexing Factor**.
5. Select the **Use device streams rather than multiplexing if possible** checkbox.

The data streams are copied to each available drives first and then fills up the used up drives (spill and fill). If disabled, all the data streams are copied to one drive and once it is filled up, moves to the next drive (fill and spill).

5. Click **OK**.



DETERMINING THE MULTIPLEXING FACTOR

The multiplexing factor should be determined by analyzing your network configuration and by examining your needs for maximizing disk throughput to decrease the total amount of time it takes to protect your data. The multiplexing factor is determined by the following:

- Network card speed
- Network switch speed

- Drive speed

The following examples will help you determine the multiplexing factor. Keep in mind that these are only hypothetical examples.

1. Let's analyze a network configuration that involves three clients, without and with multiplexing.
2. What happens when a fourth client is added to the example and the multiplexing factor is set to four.
3. A fifth client is added, and the multiplexing factor is set to five, is this over-multiplexing?
4. If you have over-multiplexed, either set the multiplexing factor lower and multiplex less clients, or add some gigabit Ethernet switches to your network.
5. In another example, client disk speeds are fast and they become slower after multiplexing.

Note that the maximum multiplexing factor that can be set from the CommCell Console is 10 and the system displays a warning message when the multiplexing factor is set to 5 or above.

PERFORM A MULTIPLEXED DATA PROTECTION OPERATION

Once the multiplexing factor is set on the primary copy of the storage policy whose subclients are to be backed up, all data protection operations of the storage policy can run at the same time, to the same piece of media.

In the sample image that follows, Job IDs 142, 140, and 141 are all backing up to Lib_Drive1.

Job ID	Operation	Client Computer	Agent Type	Subclient	Backup Type	Storage Poli...	Media Agent	Status	Progress	Drives/Mount Paths
142	Backup	purple	Windows 20...	multiplex_3	Full	sp_multiplexi...	purple	Running	■■	Lib2_Drive1
140	Backup	purple	Windows 20...	multiplexing_2	Full	sp_multiplexi...	purple	Running	■■	Lib2_Drive1
141	Backup	purple	Windows 20...	multiplex_1	Full	sp_multiplexi...	purple	Running	■■	Lib2_Drive1

Running: 0, Pending: 0, Queued: 0, Waiting: 0, Suspended: 0

PERFORM DATA MULTIPLEXING USING A DISK LIBRARY

Data Multiplexing can be performed on a disk library by setting the maximum number of streams on the disk storage policy to a value equal to the number of data protection operations that are to be performed simultaneously. For more information on setting the number of data streams, see Storage Policy Copy Properties.

DE-MULTIPLEXING MULTIPLEXED DATA

De-multiplexing segregates/de-multiplexes the data for selected clients/subclients from the larger list of clients. The software does not require de-multiplexing; however, if you want to de-multiplex the data that you have multiplexed, you can create a subclient-based storage policy copy for each subclient within the original storage policy copy, and then perform an auxiliary copy operation on that copy.

Be sure to adhere to Best Practices when using the data multiplexing feature.

MULTIPLEXING AND DATA STREAMS

Data Multiplexing is performed differently based on whether or not you are performing multiple stream data protection operations.

DATA MULTIPLEXING WITH SINGLE STREAM DATA PROTECTION OPERATIONS

In the following example, J_1 , J_2 , J_3 , and J_4 have been run as single stream data protection operations. There are two drives available, D_1 , and D_2 .

If there is no data multiplexing:

J_1 will use D_1 , J_2 will use D_2 , J_3 , and J_4 will go into a waiting state until J_1 and J_2 have completed.

If data multiplexing was used with a multiplexing factor of two:

J_1 and J_2 will use D_1 , J_3 and J_4 will use D_2 .

DATA MULTIPLEXING WITH MULTIPLE STREAM DATA PROTECTION OPERATIONS

The following examples illustrate data multiplexing with data protection operations that use multiple streams.

DATA MULTIPLEXING WITH FILE SYSTEM MULTIPLE STREAM DATA PROTECTION OPERATIONS

In the following example, there are two jobs, J_1 and J_2 . Each job was run with three streams. There are two drives, D_1 and D_2 .

If there is no data multiplexing:

J_1 has three streams, and each stream uses D_1 , but they run one after another.

J_2 also has three streams, and each stream uses D_2 , and they also run one after another.

If there is data multiplexing with a multiplexing factor of three:

The three streams of J_1 can run concurrently to D_1 .

The three streams of J_2 can run concurrently to D_2 .

DATA MULTIPLEXING WITH DATABASE MULTI STREAMING

In the following example, a three stream database data protection operation is performed with a multiplexing factor of three. J_1 , J_2 , and J_3 are database data protection operations, and each used three streams. There are three drives available, D_1 , D_2 , and D_3 .

If there is no data multiplexing:

$D_1 - J_1$

$D_2 - J_1$

$D_3 - J_1$

The second and third job (J_2 and J_3) must wait for the necessary resources.

If there is data multiplexing with a multiplexing factor of three.

The first job (J_1) uses three drives, D_1 , D_2 , and D_3 :

$D_1 - J_1$

$D_2 - J_1$

$D_3 - J_1$

The second and third job (J_2 and J_3) are multiplexed and use the same drives as J_1 :

$D_1 - J_1, J_2, J_3$

$D_2 - J_1, J_2, J_3$

$D_3 - J_1, J_2, J_3$

Therefore, J_1 , J_2 , and J_3 use D_1 , D_2 , and D_3 in parallel.

DATA MULTIPLEXING WITH MULTI STREAMING FOR ORACLE JOBS

The Oracle *iDataAgent* applies multiplexing rule as any other database *iDataAgent* for multiple jobs. Also, when you have multiplexing enabled for an Oracle job with multiple streams, all the streams of the job can be made to use the available drives sequentially (i.e., fills one drive and then moves to the next) by enabling the **Enable Multiplexing for Oracle** option in the **Job Management** window from the **Control Panel**. For step-by-step instructions on enabling multiplexing for Oracle, see [Enable Data Multiplexing](#).

However, note that this option can be used only for Oracle jobs from the CommCell Console and from third party command line. This can also be used when initiating the job using `qoperation backup` command.

In the case of on demand Oracle jobs, data multiplexing is enabled by default with/without this parameter. You can disable this feature using the `QB_NO_MULTIPLEX_STREAM` option.

IMPACT OF DATA MULTIPLEXING ON DATA RECOVERY OPERATIONS

The following data recovery operations can be performed on multiplexed data without significant degradation of performance:

- Data recovery operations using CommCell Console
- Data recovery operations using Media Explorer

BEST PRACTICES

It is recommended that you keep the following in mind when performing data multiplexing:

- Use different storage policies for file system and database type data before performing data multiplexing. Therefore, there will not be differences in the chunk sizes of the different types of data.
- If possible use the Restore by Jobs option to restore multiplexed data, especially when restoring large amount of data. This will provide the optimum performance during the restore operation as there are fewer tape rewinds to secure the data.
- It is recommended that you perform data multiplexing for jobs that have similar speeds (i.e. two database jobs), instead of mixing faster jobs (i.e. file systems) with slower jobs (i.e. databases). Mixing faster and slower jobs results in data stored on media that is not uniform.. Hence, data recovery operations of slower clients will have added performance penalty.
- Multiplexing is recommended if you are planning to recover:
 - Individual items, files and folders.
 - Entire computers or databases.
- It is not recommended under following conditions:
 - If you are planning to recover scattered folders as multiplexing will further scatter the data. Also it adds to up to extra tape mounts and rewinding/forwarding on the media.
 - Clients which undergo very frequent restore requests.
- The multiplexing factor is determined based on the ratio of how fast the tape drive is compared to the disk. For example, consider the following ratios:
 - Tape write speed = 80 GB per hour
 - Disk read speed (backup) = 25 GB per hour
 - Tape read speed = 80 GB per hour
 - Disk write speed (restore) = 60 GB per hour

Tape write speed/disk read speed (backup) = $80/25 = 3.2$ GB per hour

Tape read speed/disk write speed (restore) = $80/60 = 1.33$ GB per hour

It is recommended that the lower of the two ratios as the multiplexing factor if you want no-penalty data recovery operations.

LICENSE REQUIREMENT

This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

[Back to Top](#)

Data Multiplexing - How To

[Topics](#) | [How To](#) | [Support](#) | [Related Topics](#)

[Enable Data Multiplexing](#)

ENABLE DATA MULTIPLEXING

Before You Begin

Data Multiplexing cannot be enabled on a secondary copy, a copy of a disk library, or on a Disaster Recovery Backup storage policy.

Required Capability: Capabilities and Permitted Actions

▶ To enable data multiplexing:

1. From the CommCell Browser, right click the storage policy copy whose storage policy you want to enable data multiplexing, then click **Properties**.
2. From the Media tab of the **Copy Properties** dialog box, select **Enable Multiplexing**.
3. Select the number of subclients whose data will be multiplexed to the same media from the **Multiplexing Factor** list box.
4. Click **OK** to save your changes.

▶ To enable data multiplexing for Oracle jobs:

1. From the CommCell Browser, click **Job Management** from the **Control Panel** window.
2. From the Job Management (General) tab, select **Enable Multiplexing for Oracle**.

3. Click **OK** to save your changes.

[Back to Top](#)

User Administration and Security

[Topics](#) | [How To](#) | [Troubleshoot](#) | [Support](#) | [Related Topics](#)

Overview

[Enable Users to Perform CommCell Functions](#)

[Enable Users to View All Objects in the CommCell Console](#)

[Restrict Visibility in the CommCell Console](#)

[Users Logged In](#)

[Single Sign On](#)

[Authentication for Agent Installs](#)

[Capabilities and Permitted Actions](#)

[Audit Trail](#)

[Related Reports](#)

OVERVIEW

Users have access to the resources and features of the CommCell based on the following:

- CommCell user accounts
- CommCell user groups
- User group capabilities
- User group object associations

Using this approach, a CommCell administrator can provide users with the exact capabilities they are required. These requirements can vary, depending on the tasks each user needs to perform. A CommCell administrator can also restrict the CommCell objects that a user can view, by restricting the CommCell objects that a user's member user group has an association with.

COMMCELL USER ACCOUNTS

All users that perform functions within the CommCell must have a CommCell user account. This user account contains information about each user. A user can have a unique account, or use another account.

By default, a CommCell administrator user is established during the installation of the software. The user defined as the CommCell administrator user is permanent and cannot be deleted.

COMMCELL USER GROUPS

User Groups are named logical entities; containers to which capabilities, CommCell objects, and users are assigned. Users that are assigned to a group are granted the group's privileges as well as access to the group's object associations. The following user groups are automatically created by the installation of the software:

MASTER USER GROUP

By default, the Master user group is automatically created during the installation of the software. This user group is assigned all available capabilities as system resources. The user you created during the installation of the software is automatically assigned to this user group. Users that are members of this user group have all available rights within the CommCell.

VIEW ALL USER GROUP

The `View All` user group allows a user to see all CommCell entities and associated schedules, regardless of the associations of the user groups to which that user has an association. Note that users cannot modify the schedules unless they created them. For more information, see [Enable Users to View All Objects in the CommCell Console](#).

NAME SERVERS

Name Servers comprises of external domains and external user groups to which CommServe user groups can be associated in order to utilize the Single Sign On feature and/or to use external domain user account credentials for logging in. For more information, see [Single Sign On](#).

You can also create Name Servers for Domino Directory Services in order to enable end-user search for Lotus Notes Domino users. However, note that Single Sign On is not supported for Domino Name Servers. For step-by-step instructions, see [Add a Domain Controller for Domino Directory Services](#).

- When adding domain controllers, note that no two domain controllers can have the same domain name. In other words, you cannot register duplicate domain controllers with the CommServe.
- Whenever you register a new domain controller with the CommServe, make sure to restart the IIS services on the Web Search Server in order to enable logging to the Search Console using the new domain.

CAPABILITIES AND COMMCELL OBJECTS

Each user group must be assigned capabilities and objects so that its member users can perform functions within the CommCell. A user group can be assigned all capabilities and/or all associations, or individual associations and capabilities.

Capabilities are privileges that allow users to perform a variety of functions within a CommCell. These functions include performing data protection, data recovery, and administration operations, such as license administration and administering user accounts.

CommCell Objects are levels in the CommCell that a user group can be associated with. User groups must be given permissions to these objects.

If a user is not part of the `View All` user group, then that user will not see CommCell objects for which the user's member user group(s) does not have associations. Furthermore, users will not be able to view the Job Controller or Event Viewer details associated with the CommCell objects for which they do not have permissions. Note that a user will not be able to view these CommCell objects upon logging onto the CommCell Console after the restrictions have been set.

- Similar to the CommCell Console, the Command Line Interface also has the ability to restrict user access for performing various operations. For example, if a user with limited permissions uses the command to obtain the list of all CommCell clients, then only the clients that the user has access to will be displayed.
- An alert can be configured to notify users of multiple failed login attempts, which may signify that a non-registered user is trying to gain unauthorized access to the CommCell. This alert can assist in securing your CommCell environment. To configure this alert, see CommCell alert.

ENABLE USERS TO PERFORM COMMCELL FUNCTIONS

A user will be able to perform functions within the CommCell after the following steps are completed:

1. Create a user account. See [Create a User Account](#).
2. Create a user group. See [Create a User Group](#).
3. Assign that user group with a particular capability. See [Assign Capabilities to a User Group](#).
4. Make the user a member of the user group you created. See [Assign A User To a User Group](#).
5. Associate the group with a CommCell object. See [Associate CommCell Objects to a User Group](#).

Once the above steps are completed, the user assigned to the created user group will be able to perform the functions available from the capabilities and objects the user group is associated with. See [Capabilities and Permitted Actions](#) for a list of the specific functions a user group can perform based on capabilities and associated objects.

CREATE A USER ACCOUNT

User accounts are created for users who need to access the system. When you create a user account, you can immediately assign the account to the available user groups or leave the account unassigned.

In the sample image, the user `Technician` was created from the General tab of the `New User Properties` dialog box. This user was given a password, user name, description and e-mail address.

The screenshot shows the 'New User Properties' dialog box with the 'General' tab selected. The fields are filled with the following information:

- User Name: Technician
- Password: *****
- Confirm Password: *****
- Full Name: Computer Technician
- Description: This technician fixes computer problems.
- E-Mail: tech@company.com
- Enabled:
- Age Password in: 0 Days

Buttons for OK, Cancel, and Help are visible at the bottom of the dialog.

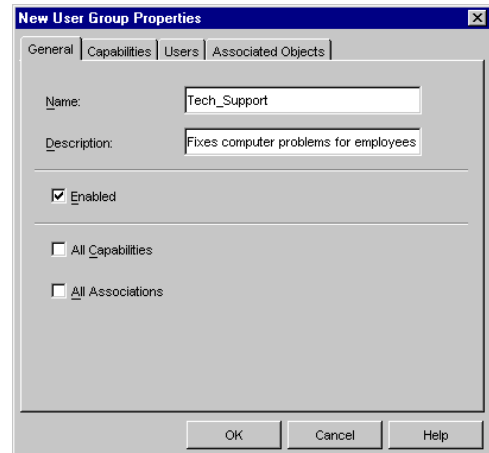
CREATE A USER GROUP

User groups must be created for users who require access to the system. Each user group represents a distinct set of users, capabilities, and CommCell objects. You can create any number of user groups, each having any combination of assigned capabilities.

When planning your user group strategy, decide:

- Who needs access to the system?
- What tasks will each CommCell user need to perform?
- As an administrator, what are your security needs?

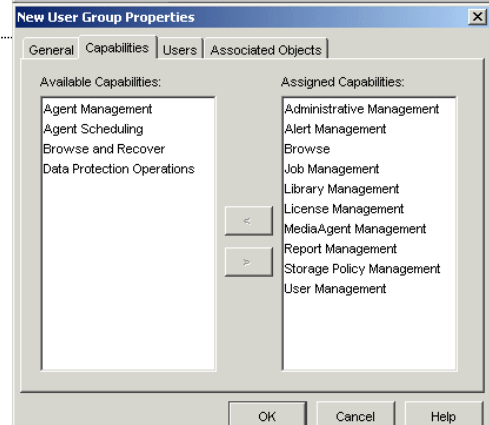
In the sample image, the user group `Tech_Support` was created from the `General` tab of the `New User Group Properties` dialog box. This user group was given a name and description.



ASSIGN CAPABILITIES TO A USER GROUP

When assigning capabilities to a user group, the capabilities you assign should match the functions you want the users of that user group to perform within the CommCell. For a complete list of capabilities, see `Capabilities and Permitted Actions`.

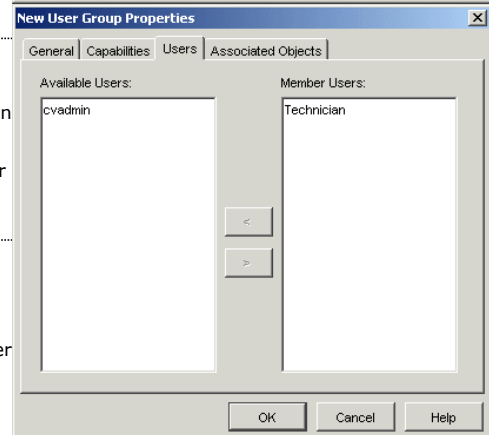
In the sample image, the user group `Tech_Support` was assigned capabilities from the `Capabilities` tab of the `New User Group Properties` dialog box.



ASSIGN A USER TO A USER GROUP

A user can obtain the functionality of a user group by being assigned to that group. You can assign individual users or groups of users to user groups. A user can be a member of more than one group (and have all of the capabilities from each of those groups).

In the sample image that follows, the user `Technician` was assigned to the `Tech_Support` user group from the `Users` tab of the `New User Group Properties` dialog box.



ASSOCIATE COMMCELL OBJECTS TO A USER GROUP

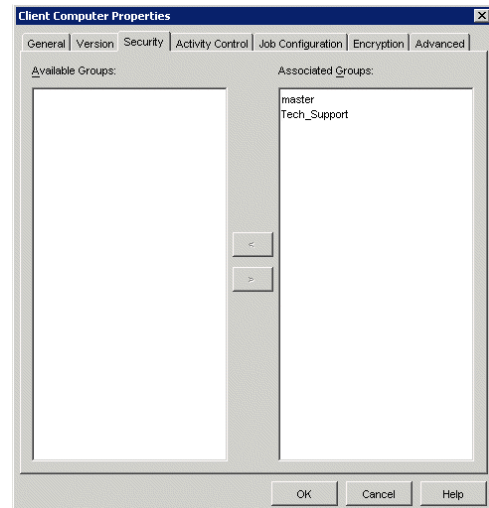
CommCell object associations enable members of a group to perform operations on a specific object. The nature of those operations depends on the capabilities assigned to the group.

If an object, such as a client computer or higher level object, is not associated with a given user group, then the users of that group cannot perform any operations involving that client computer. The following objects can be associated with a user group:

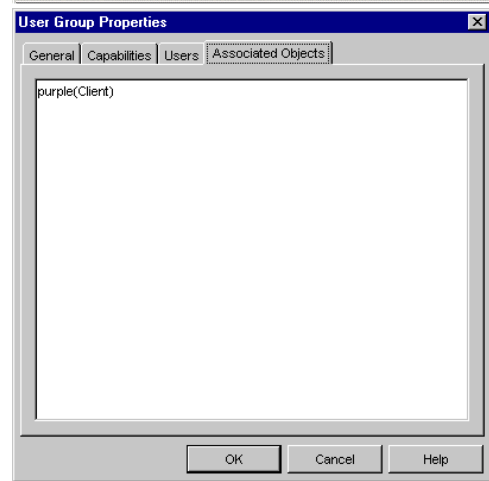
- The CommServe
- Client Computer Group
- Client Computer
- Agent
- Backup set
- Subclient
- MediaAgent
- Library
- Storage policy

Each of these objects supports specific functions within the CommCell. For a summary of these functions, see `Capabilities and Permitted Actions`.

In the sample image, the `Tech_Support` user group was associated at the Client level from the `Security` tab of the `Client Computer Properties` dialog box.



Once the `Tech_Support` user group is given association at the client level, the client level is displayed in the `Associated Objects` tab of the `User Group Properties` dialog box.

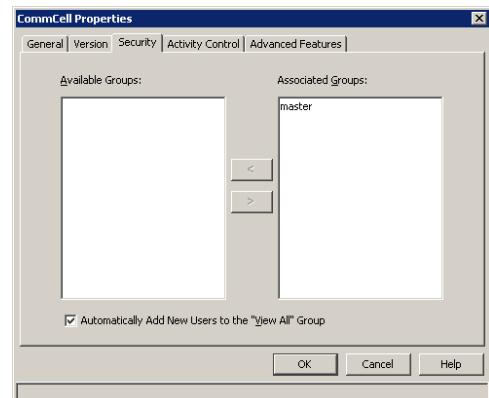


ENABLE USERS TO VIEW ALL OBJECTS IN THE COMMCELL CONSOLE

The `View All` user group allows members of that group to see all entities in the CommCell Console as well as associated job schedules, regardless of the associations of their member user groups. By default, the `Automatically Add New Users to the View All Group` option on the `Security` tab at the CommCell level is enabled, allowing all newly created users membership with this group.

Users can also be added to this group individually.

Though users within this group can view all schedules associated with all CommCell entities, they can only modify those schedules which they have created.



RESTRICT VISIBILITY IN THE COMMCELL CONSOLE

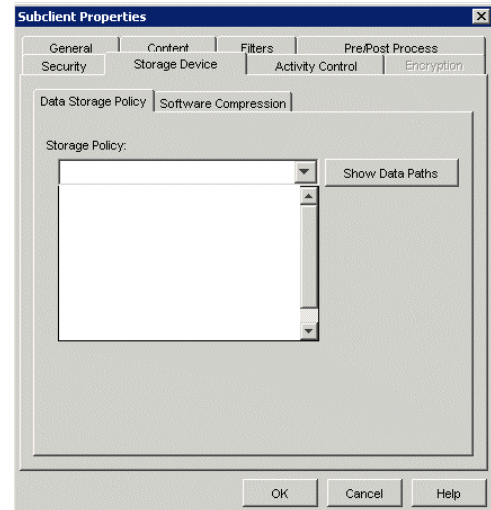
If a user is not part of the `View All` user group, the user can only see objects in the CommCell Console for which their member user group(s) has association with.

For example, if a user is not a member of the `View All` user group, and user `Technician` of the `Tech_Support` user group is associated at a particular client, this user will only be able to see that client upon logging on to the CommCell Console.

If this user then wants to change the storage policy of a subclient, then `Tech_Support` must have association at both the subclient and storage policy levels.

In the sample image that follows, `Tech_Support` does not have association at the storage policy level. User `Technician` of that user group cannot select a storage policy, as the storage policies are not visible.

- When a user belongs to a user group with restricted access, the restrictions extend to the Job Controller and the Event Viewer; they will not be able to view the Job Controller or Event Viewer details associated with the clients or objects for which they do not have permissions. Once a user is added to a user group with restricted access, the restrictions will take place upon the user logging into the CommCell Console after the restrictions are set. They will only be able to view Job Controller or Event Viewer details with which they are associated and have permissions.
- You can create a user group with the **View** capability, which can be associated with specific entities within the CommCell. Members of this user group will only be able to view those entities associated with the user group.



USERS LOGGED IN

You can view the users currently logged on to the CommCell Console via the CommCell Console or Command Line Interface. Through the Users Logged In dialog box, you can obtain the log on name of the user that is currently logged on, the host name the user logged on from, the date and time the user logged on to the CommCell Console, and the amount of time the CommCell Console has been inactive. For more information, see View Users Logged In.

If you want the CommCell Console to disconnect after being inactive for a certain amount of time, you can enable the Allow GUI connections to timeout option on the System dialog box. You can define the timeout in minutes for the inactive CommCell Console to disconnect.

For more information, see View Users Logged In.

SINGLE SIGN ON

The Single Sign On (SSO) feature enables users to login to the CommServe using their user-account credentials from the Active Directory service provider, inheriting capabilities on the CommServe based on their Active Directory group membership mapping on the CommServe user groups, which must include the *Browse* capabilities.

If the Single Sign On feature is enabled for this Active Directory domain, the login/password entry screen is bypassed, and the user is authenticated without them having to enter any login/password information. Users can also launch the CommCell Console and select **Cancel** before the application initiates the login process. The username field is pre-populated if the user is connecting to the CommServe, and the Active Directory domain they are currently logged into has been configured on the CommServe. Users also have the option to overwrite this username with other Active Directory user account credentials; the username must be entered in the following format: `<domain name>\<user name>`. When a username is entered with a domain name, the CommServe Server automatically recognizes that the password information must be authenticated by the external domain server.

Prior to enabling Single Sign On on a Name Server, note the following:

- Ensure that a Web Client package is installed on at least one of the clients in the domain.
- Ensure that Java 6 is installed (1.6.x and above)
- Single Sign On works only on Intranet based sites.
- The CommServe must be a member of an Active Directory domain in order to support Single Sign On logins. SSO logins are not supported if the CommServe is part of a workgroup.

ADD A NEW DOMAIN CONTROLLER

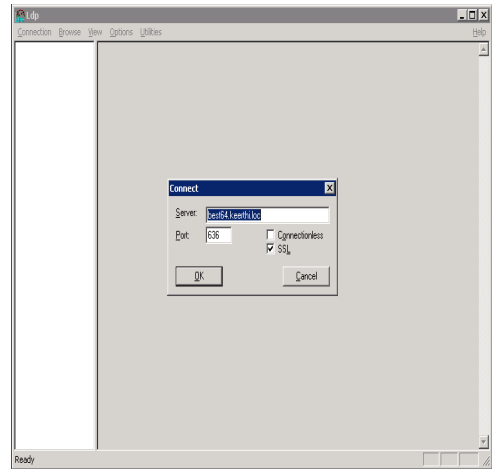
In order to enable Single Sign On, you need to first add the external domain with the CommServe for authentication purposes. When adding the domain controller, you will provide the required information to communicate with the Active Directory service provider (such as domain name, hostname of directory server, directory service type, username and password).

Note the following when adding domain controllers:

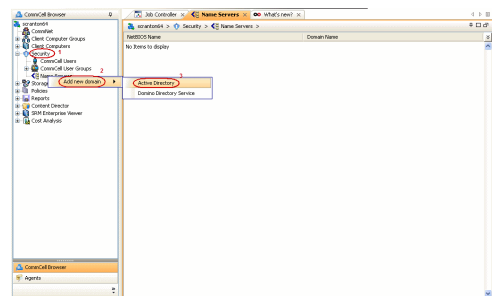
- The CommServe must have LDAP, DNS and Kerberos connectivity to each domain that you wish to register for Single Sign On. If firewalls exist between the CommServe and domain controllers, these services must be able to traverse the firewall in order for Single Sign On to function.
- When using trusted domains, make sure to add both the domains with the CommServe so that users from the trusted domains can login using Single Sign On.
- Make sure no two domain controllers have the same domain name. In other words, you cannot register duplicate domain controllers with the CommServe.

Use the following steps to add a domain controller:

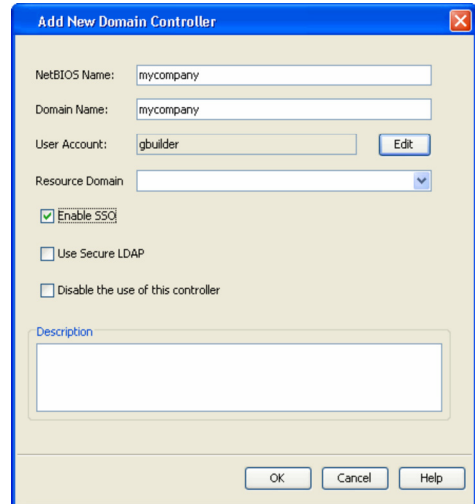
1. Obtain the domain name and fully qualified domain name of the Active Directory server.
2. Ensure that LDAP is configured on the AD server:
 - From the Active Directory Server, select **Start | Run**.
 - Type **ldp** on the **Run** dialog box and click **OK**.
 - Click the **Connections** menu option, and select **Connect**.
 - From the **Connect** dialog box, enter the following information:
 - **Server:** Enter the name of the external domain server, e.g., `computer.domain.com`.
 - **Port:** Enter 636 as the port number for the external domain server.
 - **SSL:** Mark this checkbox to check for the proper certificate.
 - Click **OK**. If properly configured for LDAP, the external domain server details will be displayed in the LDP windowpane. If not configured for use with LDAP, an error message will appear indicating that a connection cannot be made using this feature.



3. From the CommCell Browser, expand the **Security** node, right-click **Name Servers | Add New Domain** and click **Active Directory**.

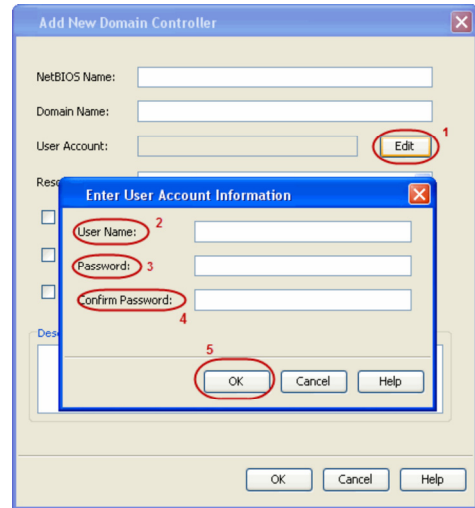


4.
 - Enter the domain name in **NetBIOS Name** text box, e.g., `mydomain`.
 - Enter the Fully Qualified Domain Name (FQDN), e.g., `mydomain.mycompany.com` in the **Domain Name** text box.

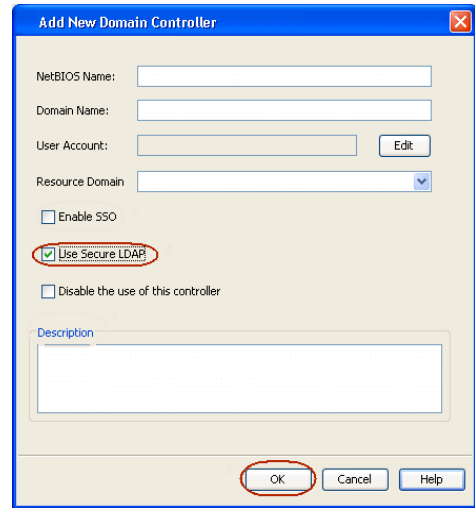


5.
 - Click **Edit** to enter the user account information for the domain.
 - Type **Username** and **Password** in **Enter User Account Information**.
 - Click **OK**.

6.
 - Select **Use Secure LDAP** to enable the secure Lightweight Directory Access Protocol (LDAP) with the external domain.
 - Click **OK**.



7. Once you have registered the Domain Controller, restart the IIS services on the Web Search Server.
 - From your **CommServe** computer, click the **Start** button on the Windows task bar and then click **Administrative Tools**.
 - Click **Services**.
 - In the **Services** window, select and right-click **IIS Admin Service** and click **Restart**.
 - **Restart Other Services** dialog will be displayed, click **Yes**.



ADD A NEW EXTERNAL GROUP

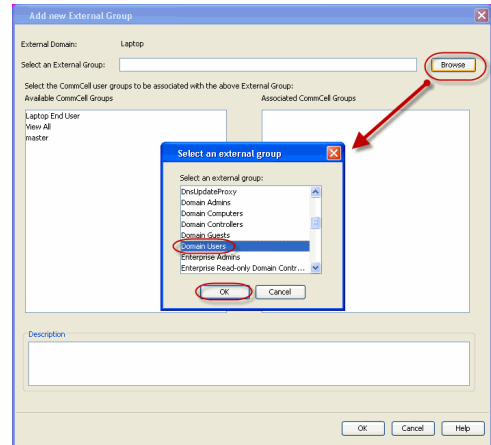
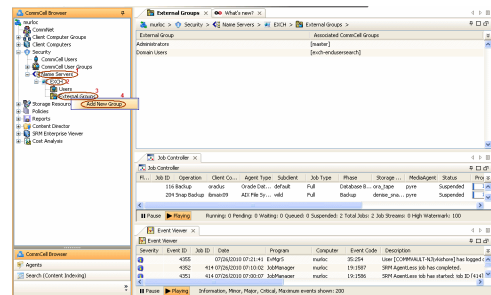
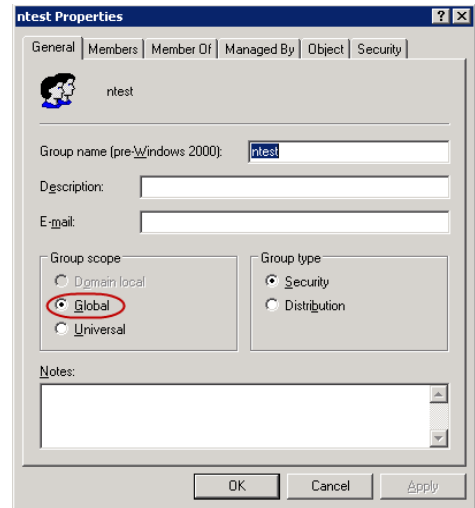
Once you have added the domain controller, associate certain external domain user groups (domain name\user group) with a user group defined in the CommServe. This will provide the external domain users access to the CommCell entities. Note that the CommServe user group must have Browse capabilities in order for the Single Sign On feature to work properly.

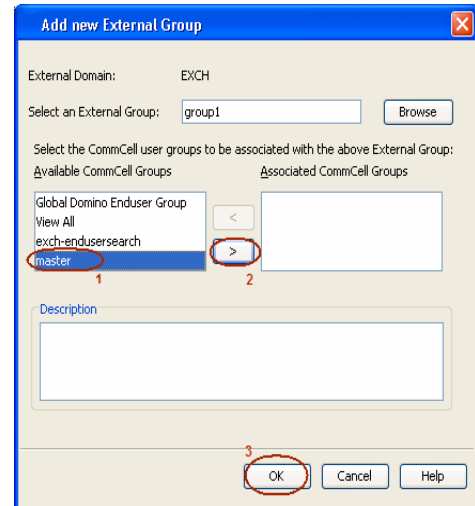
15.
 1. Ensure that the specific external user group in which the user belongs has Group Scope defined as `Global` on the Active Directory Domain:
 - Navigate to **Start | Administrative Tools | Active Directory Users and Computers**.
 - Right-click the external group and select **Properties**.
 - Select **Group** from **Group Scope** and click **OK**.

2. From the CommCell Browser, navigate to **Security | Name Server | <Domain Name>**, right-click **External Groups** and select **Add New Group**.

3.
 - Click **Browse**.
 - Select the **<external user group name>** in which the user belongs.

4.
 - Select the **CommCell User Group** to associate with the specified external user group.
 - Click **OK**.

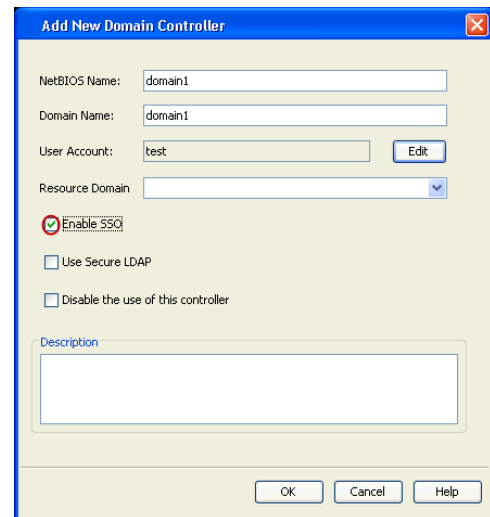




ENABLE SINGLE SIGN ON

Use the following steps to enable Single Sign On:

1. From the CommCell Browser, click the **Security** icon, and right-click on the **Name Servers** icon.
2. Right click on the domain for which you wish to enable/disable the feature, and select **Properties** from the popup menu.
3. Enable or disable the **Enable SSO** option.



CONFIGURATION

Once you have enabled Single Sign On on the Name Server , do the following:

- Restart the Web Server (IIS) since the domain information is cached in the server.
- Ensure that you have administrative permissions for the domain.
- Open the command prompt and execute `cvspn.bat` located in the Base folder of the web client.

- `cvspn.bat -A domainName\userName` (adds a Service Principal Name)
- `cvspn.bat -D domainName\userName` (deletes a Service Principal Name)

Here the `userName` must match with the Name Server registration done in the Commcell GUI.

- Configure your browser to include the site in the Intranet zone in case of Internet Explorer.

Once configured, if necessary, users can temporarily disable the Single Sign On feature or change user credentials. For more information, see [Disable Single Sign On/Change the Target CommCell from a Specific Console](#).

ADMIN AND RESOURCE DOMAINS

You can also register Active Directory Admin domains and Resource domains with the CommServe. Admin domain contains the user credentials of all the users. The Resource domain includes the resources or applications that can be accessed by each user in the admin domain. In order to enable the users in the admin domain to access the resources in the resource domain, you need to associate the admin domain with the resource domain when adding a new domain controller.

For step-by-step instructions on mapping an admin domain with the resource domain, see Associate Admin Domain with Resource Domain.

ALERTS

An alert can be configured to send e-mail notifications to user groups created from within the CommCell Console as well as external domain user groups. However, individual external domain users will not receive the alert notification e-mail if they have not previously logged on to the CommCell Console. Users (from the user groups created from within the CommCell Console) will receive the alert e-mail notification regardless of their login status.

REPORTS

A scheduled report can be configured to be sent via e-mail to user groups created from within the CommCell Console as well as external domain user groups. However, individual external domain users will not receive the report via e-mail if they have not previously logged on to the CommCell Console. Users (from the user groups created from within the CommCell Console) will receive the report e-mail regardless of their login status.

LICENSE REQUIREMENT

This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

ADDITIONAL FEATURES SUPPORTED BY SINGLE SIGN ON

Single Sign On configuration can also be used for the following:

- Content Indexing: For more information, see Configuration - Content Indexing and Search.
- DataArchiver Outlook Add-In: For more information, see Getting Started - Outlook Add-In - Administrator.

AUTHENTICATION FOR AGENT INSTALLS

CommCell environments can be secured by limiting agent installations to those users belonging to the following user group:

- A user group assigned with Installation capabilities for the CommCell, or
- A user group assigned with Administrative Management capabilities for the CommCell or an existing client computer within the CommCell

This feature, disabled by default, can be enabled in the CommCell Properties (Security) dialog. When enabled, during the installation of an Agent, you will be prompted with the **Account Information for Agents Authentication** dialog where you must enter the **username** and **password** credentials for an external domain user account or a CommCell user account. This authorizes the installation of the agent on the CommCell. If you attempt to install an agent without the proper credentials, the installation process will abort.

To enable this feature, see Require Authentication for Agent Installation.

- If Single Sign On is enabled together with this feature, then during the installation of an Agent, the user's credentials will be verified automatically, and if they are assigned with Administrative Management capabilities, the Agent Authentication dialog will not be displayed during install.
- If this feature is enabled, and you want to install an Agent on a client not yet associated to the CommCell, you must have Administrative Management capabilities for the entire CommCell to add the new client computer. However, if executing a decoupled install where the client computer is registered in the CommServe database prior to the installation and you are assigned Administrative Management capabilities for that client, you can still install this first Agent on the CommCell.
- If this feature is enabled, uninstalling an agent will require you to have Administrative Management capabilities.
- This feature is not available for Express versions of the software.

CAPABILITIES AND PERMITTED ACTIONS

Any operation performed by a user in the CommCell Console requires the user to have the appropriate security.

A user group given association to the CommCell level will be able to perform all actions on the CommCell. In this case all functions in the Control Panel will be available to them.

User groups who do not have association to the CommCell level but instead have associations to entities at lower levels will be able to perform all actions limited to the associated entities. These users will be able to perform functions in the Control Panel that do not affect the CommCell globally. This non-global permission model can be useful for Multi Tenancy CommServe.

See Control Panel for detailed information on the available Dialogs for each user group association.

The restricted view of Control Panel will be available to users if the `allowAdminUserCapabilities` parameter is set up in the Global Parameters. Use the steps below to setup this global parameter:

1. Log on to the CommServe computer.
2. From the command prompt, navigate to `<software_installation_path>\base`.
3. Run the following command:

```
goperation execscript -sn SetKeyIntoGlobalParamTbl.sql -si allowAdminUserCapabilities -si y -si 1
```

A user who belongs to a user group that has a particular capability must also be given an association at a particular level in the CommCell Console.

See Capabilities and Permitted Actions to view a list of operations that are available to a user who belongs to a user group that has a particular capability.

See the Capabilities and Permitted Actions (by Feature) to view a list of features with their required capability and the required association in the CommCell Console.

- The following types of operations do not require security:
 - Modifying the default display of the CommCell Console.
 - Set the maximum number of events to be retained in the Event Viewer.
- For information about User Capabilities required for Recovery Director, see Overview - Recovery Director - User Capability Requirements.

AUDIT TRAIL

Operations performed with this feature are recorded in the Audit Trail. See Audit Trail for more information.

RELATED REPORTS

USER CAPABILITY REPORT

The User Capability Report displays the user groups and users within a CommCell.

[Back To Top](#)

User Administration and Security - How To

[Topics](#) | [How To](#) | [Troubleshoot](#) | [Support](#) | [Related Topics](#)

<ul style="list-style-type: none"> Create a User Account Delete a User Change the Name of a User Change a User Password Change the Expiration Date of a User Password Change the Description of a User Disable a User Create a User Group Delete a User Group Change a User Group Description Disable a User Group Re-Assign the Capabilities of a User Group Associating or Disassociating a User Group to a CommCell Object View Users Logged In Require Authentication for Agent Installation Add a New Domain Controller for Domino Directory Services Single Sign On Add a New Domain Controller for Active Directory Edit/View Properties of an External Domain Enable/Disable Single Sign On 	<ul style="list-style-type: none"> Command Line Operations for Managing Users <ul style="list-style-type: none"> • Creating a User • Modifying a User • Getting User Properties • Deleting a User • Available Command Parameters Command Line Operations for Managing User Groups <ul style="list-style-type: none"> • Creating a User Group • Modifying a User Group • Getting User Group Properties • Listing All User Groups • Deleting a User Group • Assigning Capabilities to a User Group • Assigning a User to a User Group • Assigning CommCell Objects to a User Group • Available Command Parameters
---	---

Delete a Domain Controller Add a New External User Group Disable Single Sign On/Change the Target CommCell from a Specific Console Associate Admin Domain with Resource Domain	
---	--

CREATE A USER ACCOUNT

Required Capability: See Capabilities and Permitted Actions

▶ To create a user account:

1. From the CommCell Browser, click the **Security** icon, right-click the CommCell Users icon, and then click **New User**.
2. From the General tab of the **User Properties** dialog box type the **User Name** and **Password**. Then confirm the Password.
3. Optionally you can enter a full Name, description, and e-mail or pager address.
4. If you want to enable the user account immediately, select the **Enabled** check box. If you want to create the account but leave it inactive until some later time, then clear the Enabled option (this option is selected by default).
5. If you want the user's password to expire on a periodic basis, select the **Age Password** check box and then select the number of days for which the password is to remain valid.
6. To assign the new user to a user group, from the User Groups tab select a user group from the **Available Groups** pane and then move the group to the **Member Groups** pane. Note that unless you assign the user account to a user group, the user will not have any capabilities after logging on.
7. Click **Create New User Group** to create a user group to which this user can be associated. For more information, see Create a User Group.
8. Click **OK**.

DELETE A USER

Before You Begin

- You cannot delete the user that you defined as the CommCell administrator user during the installation of software. This user remains enabled at all times.
- Deletions are effective immediately, and once a user is deleted, the user will immediately not be able to perform functions within the CommCell Console.

Required Capability: See Capabilities and Permitted Actions

▶ To delete a user:

1. From the CommCell Browser, click the **Security** icon and then the **CommCell Users** icon.
2. From the right pane of the CommCell Browser, right-click the user you want to delete, and then click **Delete** from the short-cut menu.
3. Click **Yes** to the confirmation prompt that appears delete the user.

If this user account was used to create a schedule policy or schedule a report, upon deletion of the account, you will be prompted to transfer ownership of the schedule policy or report schedule to another user.

CHANGE THE NAME OF A USER

Required Capability: See Capabilities and Permitted Actions

▶ To change the name of a user:

1. From the CommCell Browser, click the **Security** icon and then the **CommCell Users** icon.
2. From the right pane of the CommCell Browser, right-click the user whose name you want to change, then select **Properties**.
3. From the General tab of the **User Properties** dialog box, type a new user name in the **User Name** field.
4. When you are finished, click **OK**.
5. You are prompted to enter your user login password in the **Enter Password** dialog box. Type your password and click **OK**.

CHANGE A USER PASSWORD

Required Capability: See Capabilities and Permitted Actions

▶ To change password of a user:

1. From the CommCell Browser, click the **Security** icon and then the **CommCell Users** icon.
 2. From the right pane of the CommCell Browser, right-click the user whose password you want to change, then click **Properties**.
 3. From the General tab of the **User Properties** dialog box, select the **Change Password** check box.
 4. Type the new user password in the **Password** field, and re-type it in the **Confirm Password** box.
 5. When you are finished, click **OK**.
 6. You are prompted to enter your user login password in the **Enter Password** dialog box. Type your password and click **OK**.
-

CHANGE THE EXPIRATION DATE OF A USER PASSWORD

Required Capability: See Capabilities and Permitted Actions

▶ To change the expiration date for a user password:

1. From the CommCell Browser, click the **Security** icon and then the **CommCell Users** icon.
 2. From the right pane of the CommCell Browser, right-click the user whose password expiration date you want to change, then click **Properties**.
 3. From the General tab of the **User Properties** dialog box, select a new number of days from the **Age Password** list box.
 4. Click **OK**.
-

CHANGE THE DESCRIPTION OF A USER

Required Capability: See Capabilities and Permitted Actions

▶ To change the description of a user::

1. From the CommCell Browser, click the **Security** icon and then the **CommCell Users** icon.
 2. From the right pane of the CommCell Browser, right-click the user whose description you want to change, then select **Properties**.
 3. To change the full name, type the name in the **Full Name** box.
 4. To change the description, change the description in the **Description** box.
 5. To change the e-mail or pager address of the user, type the e-mail or pager address in the **E-mail** box.
 6. When you are finished, click **OK**.
-

DISABLE A USER

Before You Begin

If you disable an existing user account, this user will immediately not be able to create or receive scheduled reports or alerts. However, this disabled user will retain all assigned rights within the CommCell until the user has logged off. Once this disabled user has logged off, the user cannot log on to the CommCell.

Required Capability: See Capabilities and Permitted Actions

▶ To disable a user:

1. From the CommCell Browser, click the **Security** icon and then the **CommCell Users** icon.
 2. From the right pane of the CommCell Browser, right click an existing user and select **Properties**.
 3. Deselect the **Enabled** field of the **General** tab of the **User Properties** dialog box to disable the user.
 4. Click **OK**.
-

CREATE A USER GROUP

Required Capability: See Capabilities and Permitted Actions

▶ To create a user group:

1. From the CommCell Browser, click the **Security** icon, right-click the CommCell User Groups icon, and then click **New User Group**.
2. From the General tab of the User Group Properties dialog box, type the name you want to assign to the user group (up to 32 characters; do not include trailing spaces) and some descriptive information that characterizes the user group.
3. If you want this user group to be disabled, de-select the **Enabled** check box (this option is selected by default).
4. If you want the user group to possess all capabilities select **All Capabilities**. If you want this user to possess only certain capabilities, click the Capabilities tab, and then perform the following:
 - Assign capabilities to a user group by moving capabilities from the **Available Capabilities** pane to the **Assigned Capabilities** pane.
 - When you are finished, click **OK**.
5. If you want the user group to be associated with all CommCell resources, select **All Associations**. If you want the user group to only be associated with specific objects, click the Associated Entities tab, and follow the procedure in Associating or Disassociating a User Group to a CommCell Object.

Do not select the **All Capabilities** and **All Associations** check boxes if you do not want to risk exposing all CommCell features and resources to users that may not have adequate training or knowledge. For this reason, these options are cleared by default.

6. To assign users to a users group, click the Users tab, and then assign users to the group, as necessary.
7. Click **Create New User** to create a user to be associated with this user group. For more information, see Create a User Account.
8. Click **OK**.

DELETE A USER GROUP

Before You Begin

You cannot delete the **master** user group. The master user group is the primary CommCell administrator group and remains available at all times.

Required Capability: See Capabilities and Permitted Actions

▶ To delete a user group:

1. From the CommCell Browser, click the **Security** icon and then the **CommCell User Groups** icon.
2. From the right-hand pane of the CommCell Browser, right-click the user group you want to delete, and then click **Delete** from the short-cut menu.
3. A confirmation prompt appears, asking if you are sure that you want to delete this user group. Click **Yes** to delete.

CHANGE A USER GROUP DESCRIPTION

Required Capability: See Capabilities and Permitted Actions

▶ To change the description of a user group:

1. From the CommCell Browser, click the **Security** icon and then the **CommCell User Groups** icon.
2. From the right-hand pane of the CommCell Browser, right-click the user group whose description you want to change, and then click **Properties**.
3. From the User Group Properties dialog box, type a new description in the **Description** field.
4. When you are finished, click **OK**.

DISABLE A USER GROUP

Before You Begin

If you disable an existing user group account, this user group will immediately not be able to create or receive scheduled reports or alerts.

Required Capability: See Capabilities and Permitted Actions

▶ To disable a user group:

1. From the CommCell Browser, click the **Security** icon and then the **CommCell User Groups** icon.
2. From the right-hand pane of the CommCell Browser, right-click the user group that you want to enable or disable, and then click **Properties**.
3. From the **User Group Properties** dialog box, deselect the **Enabled** check box (is enabled by default).
4. When you are finished, click **OK**.

REASSIGN THE CAPABILITIES OF A USER GROUP

Required Capability: See Capabilities and Permitted Actions

▶ To reassign the capabilities to a user group:

1. From the CommCell Browser, click the **Security** icon and then the **CommCell User Groups** icon.
 2. From the right-hand pane of the CommCell Browser, right-click the user group whose capabilities you want to re-assign, then click **Properties** from the short-cut menu.
 3. From the Capabilities tab of the **User Group Properties** dialog box, re-assign the capabilities to the user group, as necessary.
 4. When you are finished, click **OK**.
-

ASSOCIATE OR DISASSOCIATE A USER GROUP TO A COMMCELL OBJECT

Required Capability: See Capabilities and Permitted Actions

▶ To associate or disassociate a user group to a CommCell entity:

1. From the CommCell Browser, click the CommServe, client computer group, client computer, agent, MediaAgent, Library, Storage Policy, backup set, subclient, or Shelf media, and then select **Properties**.
 2. From the **Security** tab, select the appropriate user groups to which you want to associate to the CommCell object from the **Available Groups** pane, and then move the user group to the **Associated Groups** pane.
 3. Click **OK**.
-

VIEW USERS LOGGED IN

Required Capability: See Capabilities and Permitted Actions

▶ To view the users that are currently logged in to the CommCell Console:

1. From the CommCell Browser, right-click the CommServe, then select **View->Users Logged In**.
 2. The Users Logged In dialog box displays the user's login name, host name, time logged in, and idle time.
 3. Click **OK**.
-

REQUIRE AUTHENTICATION FOR AGENT INSTALLATION

Before You Begin

- Enabling this feature will prevent any unauthorized users from installing agents on the CommCell. Authorized users include those with Installation or Administrative Management capabilities.

Required Capability: See Capabilities and Permitted Actions

▶ To enable authentication for agent installs:

1. From the CommCell Browser, right click on the CommCell, and select **Properties** from the popup menu.
 2. Select the CommCell Properties (Security) tab.
 3. Select the **Require Authentication for Agent Installation** option to enable the feature.
 4. Click **OK**.
-

ADD A NEW DOMAIN CONTROLLER FOR DOMINO DIRECTORY SERVICES

Required Capability: See Capabilities and Permitted Actions

Before You Begin

- Make sure that Web Access is enabled for the Domino Server and the users have an Internet Password set from the Domino Server.
 - When adding domain controllers, note that no two domain controllers can have the same domain name. In other words, you cannot register duplicate domain controllers with the CommServe.

- Whenever you register a new domain controller with the CommServe, make sure to restart the IIS services on the Web Search Server in order to enable logging to the Search Console using the new domain.

▶ To add a new domain controller for Domino Directory Services:

1. From the CommCell Browser, expand the Security icon, and right-click on the Name Servers icon. From the popup menu, select **Add New Domain**.
2. Enable the secure Lightweight Directory Access Protocol (LDAP) for additional network security with the external domain. Remember that this can only be enabled when the external domain has been configured to use the secure LDAP (with the proper SSL certificate). If this protocol is enabled from the **Add New Domain Controller** dialog box, but not configured from the external domain; the feature is not enabled. To verify whether the external domain client has been configured for LDAP, see Verify LDAP configuration on External Domain.

Note that setting up the secure LDAP environment is required for the feature to work properly. It involves the following steps:

- setting up certificate servers
- importing of the same SSL certificates on both the CommServe and the external domain
- setting up the proper DNS (very important especially when the external domain client and the CommServe computer are in two different domains, etc.).

After completing these steps, you can verify if your environment is set up correctly by checking if the external domain is accessible. This ensures the DNS is set up properly. Then follow the steps in the Verify LDAP configuration on External Domain to see if the certificates are set up properly for secure communication to take place.

3. From the Add a New Domain Controller dialog, enter the following information:
 - **Domino Organization** - Specifies the top most level in the domino server hierarchy.
 - **Domino Server Host Name** - Client name in which the Domino Server resides.
 - **Domino LDAP Port** - port used by Lightweight Directory Access Protocol (LDAP) to communicate to the Domino Server. The default value is 389.
 - **User Account** - Domino administrator user account used to connect to the Domino Server. Click **Edit** to enter the user account information.
4. Click **OK**.

ADD A NEW DOMAIN CONTROLLER FOR ACTIVE DIRECTORY

Required Capability: See Capabilities and Permitted Actions

Before You Begin

- When adding domain controllers, note that no two domain controllers can have the same domain name. In other words, you cannot register duplicate domain controllers with the CommServe.
- Whenever you register a new domain controller with the CommServe, make sure to restart the IIS services on the Web Search Server in order to enable logging to the Search Console using the new domain.

▶ To add a new domain controller:

1. From the CommCell Browser, click the **Security** icon, and right-click on the **Name Servers** icon. From the popup menu, select **Add New Domain**.
2. Enable the secure Lightweight Directory Access Protocol (LDAP) for additional network security with the external domain. Remember that this can only be enabled when the external domain has been configured to use the secure LDAP (with the proper SSL certificate). If this protocol is enabled from the **Add New Domain Controller** dialog box, but not configured from the external domain; the feature is not enabled. To verify whether the external domain client has been configured for LDAP, see Verify LDAP configuration on External Domain.

Note that setting up the secure LDAP environment is required for the feature to work properly. It involves the following steps:

- setting up certificate servers
- importing of the same SSL certificates on both the CommServe and the external domain
- setting up the proper DNS (very important especially when the external domain client and the CommServe computer are in two different domains, etc.).

After completing these steps, you can verify if your environment is set up correctly by checking if the external domain is accessible. This ensures the DNS is set up properly. Then follow the steps in the Verify LDAP configuration on External Domain to see if the certificates are set up properly for secure communication to take place.

3. Enter the appropriate information in the Add New Domain Controller dialog box. You will need to enter the following information:
 - **NetBIOS Name:** Enter the NetBIOS name (IP address) of the external domain.
Note that different domains have different NetBIOS names. If you do not know the NetBIOS name of your domain, you can retrieve it using the LDP utility and searching the sub-tree of configuration naming context for the NetBIOS name attribute using the following filter:

```
( &(objectCategory=crossRef)(SystemFlags=3)(dnsroot=%s) )
```

Replace `dnsroot` with your domain, e.g., `gp.cv.company.com` (i.e., the Fully Qualified Host Name) based on your Active Directory configuration.

- Domain Name: Enter the Fully Qualified Domain Name (FQDN), e.g., `company.com`.
- User Account: Click **Edit** to enter the user account information for the external domain.
- Optional: Enable the domain controller for the SSO feature (Single Sign On).
- Optional: Enable/Disable the use of this controller.
- Click **OK**.

You can also access the **Add New Domain Controller** dialog box from the CommCell Console's **Action** dropdown menu.

EDIT/VIEW PROPERTIES OF AN EXTERNAL DOMAIN

Required Capability: See Capabilities and Permitted Actions

▶ To edit/view the properties of an external domain:

1. From the CommCell Browser, click the **Security** icon, and right-click on the **Name Servers** icon.
 2. Right click on the domain for which you wish to view the properties, and select **Properties** from the popup menu.
-

ENABLE/DISABLE SINGLE SIGN ON

Required Capability: See Capabilities and Permitted Actions

▶ To enable/disable Single Sign On:

1. From the CommCell Browser, click the **Security** icon, and right-click on the **Name Servers** icon.
 2. Right click on the domain for which you wish to enable/disable the feature, and select **Properties** from the popup menu.
 3. Enable or disable the **Enable SSO** option.
-

DELETE AN EXTERNAL DOMAIN

Required Capability: See Capabilities and Permitted Actions

▶ To delete an external domain:

1. From the CommCell Browser, click the **Security** icon, and right-click on the **Name Servers** icon.
 2. Right click on the domain for which you wish to view the properties, and select **Delete** from the popup menu.
-

ADD A NEW EXTERNAL USER GROUP

Required Capability: See Capabilities and Permitted Actions

▶ To add a new external user group:

1. From the CommCell Browser, click the **Security** icon and expand all the nodes.
 2. Click on the external domain for which you want to add an external user group, and right click on the **External Group** icon.
 3. From the Add New External Group dialog box, select the external user group for which you want to associate the CommCell user groups. Note that the external user group that you select must have their Group Scope defined as `Global`. This can be verified in the external domain's interface; check the external user group's properties. This will prevent any conflicts that may arise during Single Sign On login for an external domain user when this user and corresponding external domain user groups reside in child and parent domains.
 4. Select the CommCell user groups to associate with the specified external user group.
 5. Click **OK**.
-

DISABLE SINGLE SIGN ON/CHANGE THE TARGET COMMCELL FROM A SPECIFIC CONSOLE

Required Capability: See Capabilities and Permitted Actions

▶ To disable Single Sign On for a specific console:

1. Right-click on the application icon, and select **Properties**.

- From the **Console Properties** dialog box, select the **Shortcut** tab.
- In the **Target** field, add the following command `-sso=disabled`, and click **OK**. When launching the application from this application icon, the Single Sign On feature will be disabled, and users can enter alternate login information.

This method disables the Single Sign On feature for this application shortcut. To re-enable the feature, simply remove the `-sso=disabled` command.

▶ To temporarily disable Single Sign On:

- Launch the application using the application icon.
- When prompted with the **Connect to CommCell** login box, click **Cancel**. This will allow users to enter different login credentials.

This method allows the user to enter alternate login information once. The next time a user launches the application using the same application shortcut; it will once again use the single sign on feature.

▶ To add another target CommCell for Single Sign On:

- Create another application shortcut.
 - Right-click on current application icon.
 - Select **Create Shortcut**.
- Right-click on the new application shortcut, and select **Properties**.
- From the **Console Properties** dialog box, select the **Shortcut** tab.
- In the **Target** field, change the name of the CommServe, and click **OK**. This method adds another shortcut with a different target CommCell

This method adds another application shortcut with a different target CommCell. When this new application shortcut is used to launch application, it will automatically access the new CommCell.

▶ To change the target CommCell for Single Sign On:

- Right-click on the application shortcut, and select **Properties**.
- From the **Console Properties** dialog box, select the **Shortcut** tab.
- In the **Target** field, change the name of the CommServe, and click **OK**.

This method changes the target CommCell for the Single Sign On feature. When this application shortcut is used to launch application, it will automatically access the new CommCell.

ASSOCIATE ADMIN DOMAIN WITH RESOURCE DOMAIN

Required Capability: See Capabilities and Permitted Actions

▶ To associate an admin domain with the resource domain,

- From the CommCell Browser, expand the **Name Servers** icon under **Security** node.
- Right click on the admin domain for which you wish to enable/disable the feature, and select **Properties** from the popup menu.
- From the Edit Domain Controller Details dialog, select the **Resource Domain** from the drop-down list.
- Click **OK**.

COMMAND LINE OPERATIONS FOR MANAGING USERS

The following sections describe the steps to manage users from the command line.

Before running command line operations, you must first login to the CommServe. From the Command prompt, navigate to `<Software_Installation_Directory>/Base` and run the following command:

```
glogin -cs <commserve name> -u <user name>
```

CREATING A USER

- Download the `create_user_template.xml` file and save it on the computer from where the command will be executed.

- Execute the following command from the <Software_Installation_Directory>/Base folder after substituting the parameter values below using the Available Command Parameters table for reference.

```
qoperation execute -af create_user_template.xml -userName myuser -password plaintextpassword -fullName 'User Full Name' -
userGroupName myusergroup -email myemail -description 'account description'
```

MODIFYING A USER

- Download the modify_user_template.xml file and save it on the computer from where the command will be executed.
- Execute the following command from the <Software_Installation_Directory>/Base folder after substituting the parameter values below using the Available Command Parameters table for reference.

```
qoperation execute -af modify_user_template.xml -userName myuser -enableUser true -agePasswordDays 30 -password plaintextpassword
-fullName 'User Full Name' -userGroupName myusergroup -email myemail -description 'account description'
```

Example

To disassociate an user group, execute the following command after substituting the parameters below with the correct values.

```
qoperation execute -af modify_user_template.xml -userName myuser -associatedUserGroupsOperationType DELETE -userGroupName
usergroup
```

GETTING USER PROPERTIES

- Download the get_user_template.xml file and save it on the computer from where the command will be executed.
- Execute the following command from the <Software_Installation_Directory>/Base folder after substituting the parameter values below.

```
qoperation execute -af get_user_template.xml -userName myuser
```

DELETING A USER

- Download the delete_user.xml file and save it on the computer from where the command will be executed.
- Execute the following command from the <Software_Installation_Directory>/Base folder after substituting the parameter values below.

```
qoperation execute -af delete_user.xml -userName myuser
```

AVAILABLE COMMAND PARAMETERS

The following table displays all the parameters you can use with the commands mentioned in the sections above.

PARAMETER	DESCRIPTION AND PARAMETER VALUES
agePassword	Number of days to keep the password active
associatedUserGroupsOperationType	Modification type. Valid values are: <ul style="list-style-type: none"> • ADD, to associate new user groups. • OVERWRITE, to overwrite the existing user groups with new use groups. • DELETE, to delete one or more user groups.
description	A general description of the user account
email	Email of the user
enableUser	Option to enable/disable the user. Valid values are True/False.
fullName	Full name of the user
password	A plain text password to access the user account
userGroupName	Name of the user group to be associated. If you plan to associate more than one user group, add the following line in the XML file to specify each user group: <userGroupName>user_group</userGroupName>
userName	Name of the user

COMMAND LINE OPERATIONS FOR MANAGING USER GROUPS

The following sections describe the steps to manage user groups from the command line.

Before running command line operations, you must first login to the CommServe. From the Command prompt, navigate to <Software_Installation_Directory>/Base and run the following command:

```
qlogin -cs <commserve name> -u <user name>
```

CREATING A USER GROUP

1. Download the create_usergroup.xml file and save it on the computer from where the command will be executed.
2. Open the .xml file and update the XML parameters using the Available Command Parameters table for reference.
3. Execute the following command from the <Software_Installation_Directory>/Base folder after updating the XML parameters.

```
qoperation execute -af create_usergroup.xml
```

MODIFYING A USER GROUP

1. Download the modify_usergroup.xml file and save it on the computer from where the command will be executed.
2. Open the .xml file and update the XML parameters using the Available Command Parameters table for reference. You can remove XML parameters such as *users*, *capabilities* or *associations* from the .xml file if you do not plan to modify them.
3. Execute the following command from the <Software_Installation_Directory>/Base folder after updating the XML parameters.

```
qoperation execute -af modify_usergroup.xml
```

GETTING USER GROUP PROPERTIES

1. Download the get_usergroup_template.xml file and save it on the computer from where the command will be executed.
2. Execute the following command from the <Software_Installation_Directory>/Base folder after substituting the parameter values below.

```
qoperation execute -af get_usergroup_template.xml -userGroupName myUserGroup
```

If you want to adjust the amount of property information being displayed, use the 'level' parameter to specify the property level (see Available Command Parameters table for reference). For example, if you want to list only basic properties, execute the following command:

```
qoperation execute -af get_usergroup_template.xml -userGroupName myUserGroup -level BasicProperties
```

LISTING ALL USER GROUPS

1. Download the list_usergroup_template.xml file and save it on the computer from where the command will be executed.
2. Execute the following command from the <Software_Installation_Directory>/Base folder to list all user groups.

```
qoperation execute -af list_usergroup_template.xml
```

If you also want to list the user group properties, use the 'level' parameter to specify the property level (see Available Command Parameters table for reference). For example, if you want to list all properties, execute the following command:

```
qoperation execute -af list_usergroup_template.xml -level AllProperties
```

DELETING A USER GROUP

1. Download the delete_usergroup.xml file and save it on the computer from where the command will be executed.
2. Execute the following command from the <Software_Installation_Directory>/Base folder after substituting the parameter values below.

```
qoperation execute -af delete_usergroup.xml -userGroupName myUserGroup
```

ASSIGNING CAPABILITIES TO A USER GROUP

1. Download the associate_capability_usergroup.xml file and save it on the computer from where the command will be executed.
2. Open the .xml file and specify the capabilities that you want to add. Refer to the Available Command Parameters table for a list of valid capability values.
3. Execute the following command from the <Software_Installation_Directory>/Base folder after updating the XML parameters.

```
qoperation execute -af associate_capability_usergroup.xml
```

ASSIGNING A USER TO A USER GROUP

1. Download the associate_user_to_usergroup.xml file and save it on the computer from where the command will be executed.
2. Open the .xml file and specify the user that you want to associate. Refer to the Available Command Parameters table for information on adding multiple users.
3. Execute the following command from the <Software_Installation_Directory>/Base folder after updating the XML parameters.

```
qoperation execute -af associate_user_to_usergroup.xml
```

ASSIGNING COMMCELL OBJECTS TO A USER GROUP

1. Download the associate_entity_to_usergroup.xml file and save it on the computer from where the command will be executed.

- Open the .xml file and specify the CommCell entity that you want to associate. Refer to the Available Command Parameters table for information on the entities that you can add.
- Execute the following command from the <Software_Installation_Directory>/Base folder after updating the XML parameters.

```
goperation execute -af associate_entity_to_usergroup.xml
```

AVAILABLE COMMAND PARAMETERS

The following table displays all the parameters you can use with the commands mentioned in the sections above.

PARAMETER	DESCRIPTION
allCapabilities	Option to assign all capabilities to the user group. Valid values are True/False.
allAssociations	Option to associate all CommCell objects (such as clients, libraries, storage policies, etc) to the user group. Valid values are True/False.
associations/<entity>	Name of the CommCell entity to be associated with the user group. The XML files in the above sections define the client computer association. If you want to associate a different entity, add the following lines for the entity you want to associate: FOR MEDIAAGENTS <associations mediaAgentName="name" /> FOR LIBRARIES <associations libraryName="name" /> FOR STORAGE POLICIES <associations storagePolicyName="name" /> FOR CLIENT GROUPS <associations clientGroupName="name" />
associationsOperationType	Modification type. Valid values are: <ul style="list-style-type: none"> • ADD, to associate new CommCell entities. • OVERWRITE, to overwrite the existing CommCell entities with the new CommCell entities. • DELETE, to delete one or more CommCell entities.
capability	Name of the function which the users will be performing within the CommCell. To add more than one capability, add the following line in the XML file to specify each capability: <capabilities capability="capability name"/> The following are valid capability values: <ul style="list-style-type: none"> • ADMINISTRATIVE_MANAGEMENT • AGENT_MANAGEMENT • AGENT_SCHEDULING • ALERT_MANAGEMENT • ANNOTATION_MANAGEMENT • BROWSE • BROWSE_AND_IN_PLACE_RECOVER • BROWSE_AND_OUT_OF_PLACE_RECOVER • COMPLIANCE_SEARCH • CONTENT_DIRECTORY_POLICY_MANAGEMENT • DATA_PROTECTION_OPERATIONS • ENDUSER_SEARCH • INSTALLATION • JOB_MANAGEMENT • LEGAL_HOLD_MANAGEMENT • LIBRARY_ADMINISTRATION • LIBRARY_MANAGEMENT • LICENSE_MANAGEMENT • MEDIAAGENT_MANAGEMENT • OBJECT_STORE_UPLOAD • OBJECT_STORE_DOWNLOAD • REPORT_MANAGEMENT • STORAGE_POLICY_MANAGEMENT • TAG_MANAGEMENT • USER_MANAGEMENT • VIEW For information on the supported operations/tasks for the above capabilities, see Capabilities and Permitted Actions.
capabilitiesOperationType	Modification type. Valid values are: <ul style="list-style-type: none"> • ADD, to associate new capabilities. • OVERWRITE, to overwrite the existing capabilities with the new capabilities. • DELETE, to delete one or more capabilities.
description	A general description of the user group
enabled	Option to enable/disable the user group. Valid values are True/False.
level	The property level information that you want to display when listing user groups. Valid values are: <ul style="list-style-type: none"> • ListOnly, to list the user group name without its property information. • BasicProperties, to list the user group name along with its basic properties.

	<ul style="list-style-type: none"> ExtendedProperties, to list the user group name along with its basic and extended properties. AllProperties, to list the user group name along with all its properties.
userGroupName	Name of the user group
userName	Name of the user to be associated with the user group. If you plan to associate more than one user, add the following line in the XML file to specify each user: <users userName="user x"></users>
usersOperationType	Modification type. Valid values are: <ul style="list-style-type: none"> ADD, to associate new users. OVERWRITE, to overwrite the existing users with the new users. DELETE, to delete one or more users.

EXAMPLES

Delete a Specific Capability	To delete a specific capability for a user group, execute the following command after substituting the parameter below with the correct values. <pre>qoperation execute -af associate_capability_usergroup.xml -userGroupName myUserGroup - capabilitiesOperationType DELETE -capability capability_name</pre>
Associate a Storage Policy	To add a storage policy to a user group, open the .xml file and remove the client association line. Then, execute the following command after substituting the parameters below with the correct values. <pre>qoperation execute -af associate_entity_to_usergroup.xml -userGroupName myUserGroup - storagePolicyName sp_name</pre>

[Back to Top](#)

License Administration

Topics | How To | How Do I | Related Topics

Overview

- Permanent License Expiration
- Evaluation License Expiration
- Permanent License Release
- Licensing and Disaster Recovery

Feature Licenses

- VaultTracker Licenses

Product Licenses

License Usage by Capacity

License Administration

- Activate Permanent Licenses
- Extend the Expiry Date for CommServe Licenses
- Convert Evaluation Licenses to Permanent Licenses
- Validate License After Changing the CommServe IP Address
- Anticipate License Expiration
- Respond to License Expiration

What Happens When a License Expires

- CommServe or Agent Licenses
- Feature Licenses

Number of Supported Components within a CommCell

Best Practices

Related Alerts

Related Reports

OVERVIEW

Every component in the system (MediaAgents, libraries, and agents), CommNet products and certain CommCell features, require a product license or feature license for use. The following types of licenses are available:

Evaluation License	A temporary license provided in the software installation discs that can be used to initially install a CommCell and use CommCell features. You can continue to use the software for evaluation purposes for the duration of this license. Erase data license is not part of the Evaluation license. You need to add it separately.
Permanent License	A permanent license used for new CommCell installations and CommCell features that require this type of license for use. Permanent licenses are applied to every configured entity within the CommCell.

Evaluation and permanent licenses for the same license type can co-exist within the same CommCell. When components are initially installed, the software will first consume any available permanent licenses before consuming evaluation licenses. The License Summary Report and `License Administration` dialog box will show the numbers of evaluation and permanent licenses available and consumed within the CommCell. To access this dialog box, use the CommCell Console Control Panel. See `View All Licenses` for step-by-step instructions.

PERMANENT LICENSE EXPIRATION

When a permanent license for the CommServe is bought or activated, depending on the type of license purchased, an expiry date will be set by your software provider. If necessary, the expiry date for a permanent CommServe license can be extended by purchasing new licenses. Contact your software provider for more information.

The `License Administration` dialog box provides information on the CommServe expiry date. Additionally, the CommCell Console displays a dialog box during login if the license expiry date is 60 days or less from the current date. See `View the License Expiration Date for the CommServe` for step-by-step instructions.

EVALUATION LICENSE EXPIRATION

For evaluation licenses, the expiration clock begins from the moment the license is consumed, not the time the CommServe is installed or the evaluation license

is generated. The expiration period for evaluation licenses is usually 60 days following the date the license was consumed, although the expiration period may vary depending on the license purchased.

Evaluation licenses that were consumed on different days will have different expiration dates. For example, a license consumed on the 20th of October will expire on the 19th of December, whereas a license consumed on the 30th of October will expire on the 29th of December.

The `License Administration` dialog box provides two methods of viewing evaluation license usage:

- The `General` tab provides information on all existing permanent and evaluation licenses, including license types, the number of licenses used, the number of licenses available, and the expiration dates for evaluation licenses. See `View All Licenses` for step-by-step instructions.
- The `Evaluation Usage` dialog box provides information specific to the existing evaluation licenses, including the client name, license type, install date, and expiration date. See `View Evaluation Usage` for step-by-step instructions.

PERMANENT LICENSE RELEASE

Permanent licenses can be released when any of the following operations are performed:

- Uninstall a MediaAgent or Agent
- Deconfigure a MediaAgent or Agent
- Deconfigure a library
- For a Windows or UNIX Cluster, when MediaAgent or Agent software is uninstalled from the cluster server and from every node where the binaries were installed to host the cluster server.
- For a NetWare cluster, when the MediaAgent or Agent software is uninstalled from the cluster server.

When a permanent license is released, the license will remain available for use at a later time should the component be reinstalled or reconfigured.

LICENSING AND DISASTER RECOVERY

The CommServe license can have two IP addresses, a primary IP address for a CommServe host computer, and an IP address for a CommServe hosted in the disaster recovery site. This provides the system with the capability to automatically identify the appropriate CommServe when the CommServe meta data is restored in the disaster recovery site. See `Disaster Recovery Using a Hotsite - Planning` for an overview of planning for disaster recovery.

Contact your software provider to obtain a copy of the Dual IP License before building the disaster recovery site.

FEATURE LICENSES

For each CommCell feature that is installed, a license is consumed. While some features have their own unique license, other features share the same license type.

The Oracle RAC `iDataAgent` does not consume a license. However, an Oracle `iDataAgent` license is required for each Oracle RAC node on which you configure Oracle `iDataAgent` instances.

You can view the available feature licenses using the `License Administration` dialog box. Licenses can be sorted by license type, group, usage, or total number of licenses available. The following table lists the feature licenses as they are displayed in the `License Administration` dialog box and the `License Summary Report`, as well as how each license is consumed:

FEATURE	LICENSE TYPE (AS DISPLAYED IN THE LICENSE ADMINISTRATION DIALOG BOX AND LICENSE DETAILS)	LICENSE CONSUMPTION
AGENT - RELATED FEATURE LICENSES		
Automatic File System Multi-Streaming	Advanced File System iDA Options	1 license per CommCell
Restore By Jobs		
On Demand Backups		
Restore Data Using a Map File		
Erase Data by Browsing	Erase Data	1 license per CommCell
Erase Stubs		
Recovery Points	Recovery Points	1 license per Snapshot
Proxy Stub Subclient	DataArchiver for Files - Network Shares	1 license per Agent
SnapProtect Backup	Hardware Snapshot Enabler	1 license per client
Copy Managers	Hardware Copy Manager	1 license per CommCell
1-Touch for UNIX	1-Touch Server (Boot Server) on Unix	1 license per CommCell
1-Touch for Windows	1-Touch Server for MS Windows	1 license per Agent
COMMSERVE - RELATED FEATURE LICENSES		
CommCell Migration	CommCell Migration	1 license per CommCell

CommCell Readiness Check	CommCell Readiness Check	1 license per CommCell
Data Encryption	Data Encryption	1 license per CommCell
Data Multiplexing	Data Multiplexing	1 license per CommCell
Data Verification	Data Verification	1 license per CommCell
EZ Browse	EZ Browse	1 license per CommCell
Client Computer Groups	Client Groups	1 license per CommCell
Deferred Auxiliary Copy	Advanced Copy Features	1 license per CommCell
Inline Copy		
Office Communications Server	Office Communications Server	1 license per CommCell
System Recovery Server	System Recovery Server on Windows	1 license per CommCell
Boot Server	Boot Server on Windows	1 license per CommCell
MEDIA MANAGEMENT - RELATED FEATURE LICENSES		
Auxiliary Copy Data Encryption	Auxiliary Copy Encryption	1 license per MediaAgent
Centera Clusters	Centerra Mount Path	1 license per library
Cloud Storage	Cloud Storage	1 license per MediaAgent
Hardware Single Instancing of Data	Content Addressed Storage	1 license per CommCell
Object Level Data Deduplication on Disk Media (license available on upgraded MediaAgents)	Data De-Duplication Enabler	1 license per MediaAgent hosting the Deduplication Store.
Block Level Data Deduplication on Disk Media	Block Level Deduplication	1 license per MediaAgent hosting the Deduplication Store.
Data Deduplication on Secondary Media	Tape Deduplication	
Direct-Attached Libraries	Library Control Module	1 license per library
PnP Disk Libraries		
Stand-Alone Drives	MediaAgent Direct to Disk Option (DDO)	1 license per library
Removable Disk Drives		
DVD Media	DVD Support	1 license per CommCell
Unbuffered I/O	Advanced Media Management Features	1 license per CommCell
Libraries with Mixed Drive Types		
SCSI-3 reserve/release resource reservation		
USB, FireWire and IP Libraries (Like libraries attached to ACSLS Server)		
Disk Libraries	MediaAgent Direct to Disk Option (DDO)	1 license per library
Shared Disk Libraries With Static Mount Paths		
HDS DRU		
Shared Library Support	Shared Storage License	1 license per library
	Library Sharing Across CommCells	1 license per library
UDO Media	UDO Support	1 license per CommCell
Vault Tracker Enterprise	Vault Tracker Enterprise	1 license per CommCell
Vault Tracker	Vault Tracker	1 license per CommCell
WORM Media Support	WORM Media Support	1 license per CommCell
CONTENT INDEXING AND SEARCH - RELATED FEATURE LICENSES		
Offline Content Indexing	Content Indexing Engine Content Indexing	1 license per Agent
Search Console	Web Search Server Compliance Search	1 license per Agent
Automated Content Classification	Automated Content Classification Compliance Director	1 license per CommCell 1 license per CommCell
Tagging	Data Tagging	1 license per CommCell
ERM Connector	ERM Connector	1 license per CommCell
Legal Hold	Legal Hold	1 license per CommCell
	Advance File System iDataAgent Options	1 license per CommCell

VAULTTRACKER LICENSES

The **VaultTracker** license provides the capability to track media movement between two locations. It is also used to export media.

The **VaultTracker Enterprise** license provides the capability to track media movement between several locations. In addition to the standard VaultTracker features, it also provides several advanced capabilities.

- If both VaultTracker and VaultTracker Enterprise licenses are available, the VaultTracker Enterprise license will take effect.
- If the VaultTracker Enterprise license expires and the VaultTracker license is upgraded to a permanent license, only VaultTracker options will appear in the CommCell Console.

See Also:

- VaultTracker
- VaultTracker Enterprise

PRODUCT LICENSES

For most CommCell components or agents, and CommNet products that are installed, a license is consumed.

While some agents have their own unique license, other agents share the same license type.

The Oracle RAC *iDataAgent* does not consume a license. However, an Oracle *iDataAgent* license is required for each Oracle RAC node on which you configure Oracle *iDataAgent* instances.

Also, the Data Classification Enabler does not consume a license.

You can view the available product licenses using the *License Administration* dialog box. Licenses can be sorted by license type, group, usage, or total number of licenses available.. The following table lists the product licenses as they are displayed in the *License Administration* dialog box and the *License Summary Report*, as well as how each license is consumed:

AGENT/COMPONENT	LICENSE TYPE (AS DISPLAYED IN THE LICENSE ADMINISTRATION DIALOG BOX AND LICENSE DETAILS)	LICENSE CONSUMPTION
ACTIVE DIRECTORY		
Active Directory	<i>iDataAgent for Active Directory</i>	1 license per installed instance of the component
Active Directory Offline Mining Enabler	<i>Offline Mining Enabler for Active Directory</i>	1 license per installed instance of the component
AIX		
IBM AIX File System	<i>iDataAgent for IBM AIX File System</i>	1 license per installed instance of the component
COMMNET		
CommNet Server	<i>CommNet Server</i>	1 license per CommNet Server
CommNet Agent	<i>CommNet Agent</i>	1 license per CommServe
CommNet Advanced Reporting	<i>CommNet Advanced Reporting</i>	1 CELL Level license on Associated CommServe
CONTENT STORE		
Content Store	<i>Content Store</i>	1 license per installed instance of the component
CONTINUOUSDATAREPLICATOR		
ContinuousDataReplicator	<i>ContinuousDataReplicator</i>	1 license per installed instance of the component
ContinuousDataReplicator for Windows	<i>ContinuousDataReplicator for MS Windows</i>	1 license per installed instance of the component
ContinuousDataReplicator for Unix	<i>ContinuousDataReplicator for Unix</i>	1 license per installed instance of the component
DATA PROTECTION MANAGER		
Data Protection Manager	<i>Data Protection Manager</i>	1 license per installed instance of the component
Data Protection Manager for Windows	<i>iDataAgent for MS Data Protection Manager</i>	1 license per installed instance of the component
DATAARCHIVER		
Exchange Compliance Archiver	<i>Data Archiver Compliance for MS Exchange</i>	1 license per installed instance of the component
File Archiver for Windows	<i>Data Archiver for Files - MS Windows</i>	1 license per installed instance

	DataArchiver for Files - Network Storage	of the component This license is consumed when an instance is created for Celerra or Network Share/FPolicy. Note the following: <ul style="list-style-type: none"> • More than one instance for Celerra can be created by consuming one license. • More than one instance for Network Share/FPolicy can be created by consuming one license.
Exchange Mailbox Archiver	DataArchiver for MS Exchange Mailbox	1 license per installed instance of the component
Exchange Public Folder Archiver	DataArchiver for MS Exchange Public Folder	1 license per installed instance of the component
Domino Mailbox Archiver	Domino Mailbox Archiver	1 license per installed instance of the component
File Archiver for NetWare	DataArchiver for Files - NetWare	1 license per installed instance of the component
SharePoint Archiver	DataArchiver for MS SharePoint	1 license per installed instance of the component
Lotus Notes Document	DataArchiver for Lotus Notes Document	1 license per installed instance of the component
	DataArchiver for Lotus Notes Document for Unix	1 license per installed instance of the component
File Archiver for Unix	Data Archiver for Files - Unix	1 license per installed instance of the component
OWA Proxy Enabler	MS Outlook Web Access Proxy	1 license per installed instance of the component
DB2		
DB2 Database on Windows	iDataAgent for DB2 Database on MS Windows	1 license per installed instance of the component
DB2 Database on UNIX	iDataAgent for DB2 Database on UNIX	1 license per installed instance of the component
DB2 DPF	DB2 DPF	1 license per client. The license is consumed when this component is configured on the client computer.
DOCUMENTUM		
Documentum	Documentum	1 license per installed instance of the component
EXCHANGE		
Exchange Database	iDataAgent for Exchange Database	1 license per installed instance of the component
Exchange Mailbox	iDataAgent for Exchange Mailbox	1 license per installed instance of the component
Exchange Public Folder	iDataAgent for MS Exchange Public Folder	1 license per installed instance of the component
Exchange Offline Mining Enabler	Offline Mining Enabler for Exchange	1 license per installed instance of the component
EXTERNAL DATA CONNECTOR		
External Data Connector	External Data Connector	1 license per installed instance of the component
FREEBSD		
Free BSD File System	iDataAgent for FreeBSD	1 license per installed instance of the component
HP-UX		
HP-UX File System	iDataAgent for Hewlett Packard HP-UX File System	1 license per installed instance of the component
HP-UX Cluster	Virtual File System	1 license per installed instance of the component

IMAGE		
Image Level	iDataAgent for Image Level on Windows	1 license per installed instance of the component
Image Level on Solaris	iDataAgent for Image Level on Unix	1 license per installed instance of the component
Image Level on Linux		
Image Level ProxyHost (Windows)	iDataAgent for ProxyHost for Image Level on Windows	1 license per installed instance of the component
Image Level ProxyHost (Unix)	iDataAgent for ProxyHost for Image Level on Unix	1 license per installed instance of the component
INFORMIX		
Informix on Unix	iDataAgent for Informix Database on Unix	1 license per installed instance of the component
Informix on Windows	iDataAgent for Informix Database on Windows	1 license per installed instance of the component
IRIX		
Irix File System	iDataAgent for SGI Irix File System	1 license per installed instance of the component
	iDataAgent for Irix File System	1 license per installed instance of the component
LINUX		
Linux File System	iDataAgent for Linux File System	1 license per installed instance of the component
Red Hat Linux Cluster	Virtual File System	1 license per installed instance of the component
LOTUS NOTES		
Lotus Notes Database on Windows	iDataAgent for Lotus Notes Database on MS Windows	1 license per installed instance of the component
Lotus Notes Document on Windows	iDataAgent for Lotus Notes Document on MS Windows	1 license per installed instance of the component
Lotus Notes Database on Unix	iDataAgent for Lotus Notes Database on Unix	1 license per installed instance of the component
Lotus Notes Document on Unix	iDataAgent for Lotus Notes Document on Unix	1 license per installed instance of the component
MEDIAAGENT		
MediaAgent for Novell NetWare	MediaAgent for Novell NetWare	1 license per MediaAgent
MediaAgent for Microsoft Windows	MediaAgent for Microsoft Windows	1 license per MediaAgent
MediaAgent for Hewlett Packard HP-UX	MediaAgent for Hewlett Packard HP-UX	1 license per MediaAgent
MediaAgent for Sun Solaris	MediaAgent for Sun Solaris	1 license per MediaAgent
MediaAgent for IBM AIX	MediaAgent for IBM AIX	1 license per MediaAgent
MediaAgent for Linux	MediaAgent for Linux	1 license per MediaAgent
MediaAgent for Unix	MediaAgent for Unix	1 license per MediaAgent
MediaAgent for Tru64	MediaAgent for Tru64	1 license per MediaAgent
MACINTOSH		
Macintosh File System	iDataAgent for Apple Macintosh File System	1 license per installed instance of the component
MYSQL		
MySQL on Unix	MySQL	1 license per installed instance of the component
NAS		
BlueArc NAS NDMP	iDataAgent for BlueArc NAS NDMP	1 license per client. The license is consumed when this component is configured on the client computer.
NetApp NAS NDMP	iDataAgent for NetApp NAS NDMP	1 license per client. The license is consumed when this component is configured on the client computer.

EMC Celerra NAS NDMP	iDataAgent for EMC Celerra NAS NDMP	1 license per client. The license is consumed when this component is configured on the client computer.
Hitachi NAS NDMP	iDataAgent for Hitachi NAS NDMP	1 license per client. The license is consumed when this component is configured on the client computer.
NDMP Remote Server on Windows	iDataAgent for NDMP Remote Server on MS Windows	1 license per client. The license is consumed when this component is configured on the client computer.
NDMP Remote Server on UNIX	iDataAgent for NDMP Remote Server on Unix	1 license per client. The license is consumed when this component is configured on the client computer.
NDMP Restore Enabler	iDataAgent for NDMP Restore Enabler	1 license per client. The license is consumed when this component is configured on the client computer.
Mutli Vendor NAS NDMP	iDataAgent for Multi Vendor NAS NDMP	1 license per client. The license is consumed when this component is configured on the client computer.
NETWARE		
NetWare File System	iDataAgent for Novell NetWare File System	1 license per installed instance of the component
NetWare with Cluster Service enabled	Virtual File System	1 license per installed instance of the component
Novell Directory Services	iDataAgent for Novell Directory Services	1 license per installed instance of the component
NOVELL GROUPWISE		
Novell GroupWise	iDataAgent for Novell GroupWise Database	1 license per installed instance of the component
OES FILE SYSTEM		
OES File System	iDataAgent for OES File System	1 license per installed instance of the component
ORACLE		
Oracle on Unix	iDataAgent for Oracle Database on Unix	1 license per installed instance of the component
Oracle on Microsoft Windows	iDataAgent for Oracle Database on Windows	1 license per installed instance of the component
	iDataAgent for Oracle on MS Windows	1 license per installed instance of the component
Oracle RAC	iDataAgent for Oracle Database on Unix	1 Oracle iDataAgent license per RAC instance is required.
	iDataAgent for Oracle Database on Windows	
OSSV PLUG-IN		
OSSV Plug-In on Windows	QR Enabler for OSSV	1 license per client. The license is consumed when this component is configured on the client computer.
	QR Enabler for Windows Volume Shadow Service	
	Quick Recovery Agent for MS Windows	
OSSV Plug-In on Unix	QR Enabler for OSSV	1 license per client. The license is consumed when this component is configured on the client computer.
	QR Enabler for Windows Volume Shadow Service	
	Quick Recovery Agent for Unix	
QSnap on Unix	QSnap on Unix	1 license per client. The license is consumed when this component is configured on the client computer.
POSTGRESQL		
PostgreSQL on Unix	Postgress	1 license per installed instance of the component
PROXYHOST		

ProxyHost on Windows	iDataAgent for ProxyHost on MS Windows	1 license per installed instance of the component
ProxyHost on Unix	iDataAgent for ProxyHost on Unix	1 license per installed instance of the component
QUICK RECOVERY AGENT		
Quick Recovery on Windows	Quick Recovery Agent for Windows	1 license per installed instance of the component
Quick Recovery on Unix	Quick Recovery Agent for Unix	1 license per installed instance of the component
QR Enabler for EMC SnapView	QR Enabler for SnapView	1 license per enabler
QR Enabler for Microsoft VSS	QR Enabler for Windows Volume Shadow Service	1 license per enabler
QR Enabler for ONTAP SnapVault and SnapMirror	QR Enabler for ONTAP	1 license per enabler
QR Enabler for Open Systems SnapVault	QR Enabler for OSSV	1 license per enabler
QR Enabler for Echo View	QR Enabler for Echo View	1 license per enabler
NetApp Snapshot Enabler	NetApp Snapshot Enabler	1 license per enabler
OSSV SnapVault for the Quick Recovery Agent	Software Copy Manager	1 license per installed instance of the component
For detailed configuration and license information, see License and Package Requirements for the Quick Recovery Agent.		
RECOVERY DIRECTOR		
Recovery Director	iDataAgent for Recovery Directory	1 license per installed instance of the component
SAP		
SAP using MAXDB on Windows	iDataAgent for SAP using MAXDB on Windows	1 license per installed instance of the component
SAP using MAXDB on Unix	iDataAgent for SAP using MAXDB on Unix	1 license per installed instance of the component
SAP using Oracle on Unix	iDataAgent for SAP using Oracle on Unix	1 license per installed instance of the component
SAP using Oracle on Windows	iDataAgent for SAP using Oracle on Windows	1 license per installed instance of the component
SERVERLESS DATA MANAGER		
Serverless Data Manager on Windows	iDataAgent for Serverless Data Manager on MS Windows	1 license per installed instance of the component
Serverless Data Manager on Unix	iDataAgent for Serverless Data Manager on Unix	1 license per installed instance of the component
SHAREPOINT		
Microsoft SharePoint Server	iDataAgent for MS SharePoint Database	1 license per installed instance of the component
	iDataAgent for MS SharePoint Document	1 license per installed instance of the component
SharePoint Offline Mining	Offline Mining Enabler for SharePoint	1 license per installed instance of the component
SNAPSHOT		
QSnap on Windows	QSnap on MS Windows	1 license per installed instance of the component
QSnap on Unix	QSnap on Unix	1 license per installed instance of the component
SNMP ENABLER		
CommCell SNMP Enabler	CommCell SNMP Enabler	1 license per enabler
SOLARIS		
Sun Solaris File System	iDataAgent for Sun Solaris File System	1 license per installed instance of the component
Virtual Server for the following: • Solaris Sun Cluster • VERITAS Cluster for Solaris	Virtual File System	1 license per installed instance of the component
SRM (STORAGE RESOURCE MANAGER)		
SRM Server	SRM Services	1 license per installed instance

		of the component
SRM Exchange Agent	SRM for Exchange	1 license per installed instance of the component
SRM NAS Agent	SRM for Network Attached Storage	1 license per client. The license is consumed when this component is configured on the client computer.
SRM NetWare Agent	SRM for NetWare	1 license per client. The license is consumed when this component is configured on the client computer.
SRM Oracle Agent	SRM for Oracle	1 license per client. The license is consumed when this component is configured on the client computer.
SRM SharePoint Agent	SRM for SharePoint	1 license per installed instance of the component
SRM SQL Agent	SRM for SQL Server	1 license per installed instance of the component
SRM Domino Server Agent	SRM for Lotus Notes	1 license per installed instance of the component
SRM UNIX File System Agent	SRM for UNIX File Systems	1 license per installed instance of the component
SRM Virtual Server Agent	SRM for Virtual Server	1 license per Agent. The license is consumed when "Enable SRM Data Collection" checkbox is selected on the Virtual Server iDataAgent properties dialog box.
SRM Windows File System Agent	SRM for Windows File Systems	1 license per installed instance of the component
SYBASE		
Sybase Database on HP	iDataAgent for Sybase Database on Unix	1 license per installed instance of the component
Sybase Database on Solaris		
Sybase Database on Windows	iDataAgent for Sybase Database on Windows	1 license per installed instance of the component
SQL		
Microsoft SQL Server	iDataAgent for Microsoft SQL Server	1 license per installed instance of the component
TRU64		
TRU64 File System	iDataAgent for TRU64 File System	1 license per installed instance of the component
WINDOWS		
Microsoft Windows File System (Desktop Class)	iDataAgent for Windows Desktop Class File System	1 license per installed instance of the component
Microsoft Windows File System (Server Class)	iDataAgent for Windows Server Class File System	1 license per installed instance of the component
Microsoft Windows File System (Cluster)	Virtual File System	1 license per installed instance of the component
* Server computer requires server license and desktop computer requires desktop license for the Windows File System iDataAgent.		
Run the systeminfo command using the command prompt and check the OS Name of your computer. If it contains the word Server then it is a server machine and will require a server license; if not, then it is a desktop machine and will require a desktop license.		
WORKSTATION BACKUP AGENT		
Workstation Backup Agent on Windows	Workstation Backup	1 license per installed instance of the component
VIRTUAL SERVER		
Virtual Server Agent	Virtual Server	1 license per installed instance of the component

LICENSE USAGE BY CAPACITY

License Usage by Capacity is a licensing mechanism that allows you to obtain licenses based on the amount of data you back up. It lets you purchase licenses

based on your data protection needs.

See License Usage by Capacity for comprehensive information on what this license is and how to use this license.

LICENSE ADMINISTRATION

The `License Administration` dialog box in the CommCell Console allows you to examine and update the existing licenses in your entire CommCell. When a component is installed or uninstalled, the license type count is updated to reflect the new configuration. Note that the CommServe component does not contain a separate license type and count; it is automatically included in the CommCell configuration. This dialog box displays:

- The license type for the product, platforms, and components installed in the CommCell, in addition to the feature licenses that are available.
- The total number of available evaluation and permanent licenses for each license type.
- The number of evaluation and permanent licenses actually used.
- The expiration date for the CommServe and each of the product/feature licenses if the license is an evaluation copy.

ACTIVATE PERMANENT LICENSES

Permanent licenses can be activated from the `License Administration` dialog box. Licenses must be activated in the following situations:

- To add permanent licenses for additional components in the CommCell.
- To update the IP address of the CommServe computer.
- To add additional evaluation licenses.

To obtain additional licenses, contact your software provider.

See `Activate Licenses` for step-by-step instructions on how to activate permanent licenses.

EXTEND THE EXPIRY DATE FOR COMMSERVE LICENSES

If you wish to extend the expiry date of the CommServe you must obtain a new license file and then extend the expiry date by applying the new license on the CommServe. Contact your software provider for more information.

The expiry date of the CommServe license can be extended using the `License Administration` dialog box. This enables all operations to continue uninterrupted beyond the expiration date. See `Activate Licenses` for step-by-step instructions on how to extend the expiry date of the CommServe license.

CONVERT EVALUATION LICENSES TO PERMANENT LICENSES

Evaluation licenses may be converted to permanent licenses using the `License Administration` dialog box. This enables all operations to continue uninterrupted beyond the expiration date of the evaluation license.

When converting permanent licenses for a given product or feature, all evaluation licenses of that type are automatically converted without further user intervention required as long as the number obtained is equal to or greater than the number of existing evaluation licenses.

If the total number of permanent licenses available is less than the total number of consumed evaluation licenses, you must manually convert each evaluation license individually. You may convert as many consumed evaluation licenses to permanent licenses as you wish, provided you have sufficient permanent licenses available. See `Convert Evaluation Licenses to Permanent Licenses` for step-by-step instructions on how to convert evaluation licenses to permanent licenses.

When an evaluation license is converted to a permanent license, the following changes can be observed in the `License Administration` dialog box:

- The CommCell ID is updated with a serial number.
- The CommServe ID is updated with the IP address of the CommServe computer.

To obtain additional permanent licenses, contact your software provider.

VALIDATE LICENSE AFTER CHANGING THE COMMSERVE IP ADDRESS

After installing the software, if you change the CommServe's IP address, the existing CommCell license becomes invalid. This may render the software inoperable until you update the license with the new IP address. To update the license you must obtain an IP Address Change license from your software provider.

ANTICIPATE LICENSE EXPIRATION

If you have not converted the CommCell evaluation license to a permanent license, and you are concerned as to when the evaluation license will expire, you can check the expiration date from the CommCell Console as follows:

- From the `License Administration` dialog box by clicking on the `Evaluation Usage` tab. For information on viewing evaluation license usage using this tab, see `View Evaluation Usage`.
- From the `Event Viewer`. The `Event Viewer` displays license expiration information at a set time before the actual license expiration. If your license is due to

expire within 10 days or less, this information is displayed as a major event in the Event Viewer. This event message is triggered by any type of data protection operation, including Synthetic Full backups. For information on events, see Event Viewer.

RESPOND TO LICENSE EXPIRATION

When your license expires, you may have to either purchase a new license or extend the existing license. Contact your software provider for more information.

WHAT HAPPENS WHEN A LICENSE EXPIRES

COMMSERVE OR AGENT LICENSES

The following list identifies some common problems that may be encountered when the CommServe or an Agent license expires. You can determine whether these specific problems are caused by license expiration by checking the messages in the *Event Viewer* or the appropriate log file as indicated in the following sections. (Log files are found in the `<software installation path>\Log Files` folder.)

DATA PROTECTION OPERATIONS DO NOT RUN

Check the license information of the associated agent. Data protection operations may not run if the license for the associated agent has expired. You will also see the following error messages:

CHECK THIS...	FOR THE FOLLOWING:
Event Viewer	Failed to initialize backup request Invalid or No license for application type <app_type> Application name: <app_name>
JobManager.log file	The application license evaluation date has expired.

MEDIAAGENT WILL NOT RESTART

Check the license information of the associated MediaAgent. A MediaAgent that is installed on the same computer as the CommServe may not restart if the license for the MediaAgent has expired. You will also see the following error messages:

CHECK THIS...	FOR THE FOLLOWING:
Event Viewer	The application license evaluation date has expired Application name: <MediaAgent_name>
cvd.log file	The application license evaluation date has expired.

YOU CANNOT PERFORM DATA PROTECTION AND RECOVERY OPERATIONS

All data protection and recovery operations will become unavailable when the CommServe license expires.

Certain data protection and recovery operations will become unavailable if the corresponding evaluation license for that feature or product has expired.

In this situation, you must obtain the necessary permanent license for that feature or product by contacting your software provider. You must then activate the license using the *License Administration* dialog box.

See *Activate Licenses* for step-by-step instructions on how to activate permanent licenses.

NEW COMPONENTS CANNOT BE INSTALLED

You cannot install new components in the CommCell when the CommServe license expires.

FEATURE LICENSES

The following table describes what happens to specific features when the evaluation license expires:

FEATURE	BEHAVIOR WHEN LICENSE IS ABSENT	BEHAVIOR WHEN LICENSE IS EXPIRED	PERFORM THESE TASKS BEFORE REMOVING A FEATURE LICENSE
Auxiliary Copy Data Encryption	A secondary storage policy copy cannot be configured for data encryption.	A secondary storage policy copy cannot be configured for data encryption.	N/A
Centera Clusters	A Centera library cannot be configured.	<ul style="list-style-type: none"> Data protection operations and auxiliary copy operations to Centera libraries will stop running. New Centera libraries cannot be 	Before the application of a permanent license: <ul style="list-style-type: none"> Check if the number of Centera licenses available in the permanent license

		<p>configured.</p> <p>The following will continue to work:</p> <ul style="list-style-type: none"> • Data recovery operations from Centera libraries and storage policy copies created on media from Centera libraries. • Data Aging of data from Centera libraries. • Deconfiguration of Centera libraries. 	<p>is less than the number of evaluation Centera licenses in use.</p> <ul style="list-style-type: none"> • If so, the number of Centera libraries that make up the difference must be deconfigured first.
CommCell Migration	CommCell Migration data captures and merges cannot be performed on the CommCell.	CommCell Migration data captures and merges cannot be performed on the CommCell.	N/A
Data Verification	The Data Verification option is not available in the CommCell Console.	A Data Verification job will fail.	N/A
VaultTracker VaultTracker Enterprise	The VaultTracker node is not available from the CommCell Console.	<ul style="list-style-type: none"> • New VaultTracker Policies cannot be created. • VaultTracker policies cannot run. • VaultTracker Policies can be deleted. • VaultTracker policy schedules cannot be created. • Scheduled Data Protection or Auxiliary Copy jobs that already have the Vault Tracker option enabled will continue to run, but Export jobs will fail. • The VaultTracker node and all VaultTracker policies will continue to be displayed in the CommCell Console. • Existing Vault Tracker schedules can be deleted. • Reports will continue to function. 	<p>Delete any existing VaultTracker policies.</p> <p>Ensure that the job level Export option is not enabled.</p> <p>Disable any VaultTracker options that are enabled in scheduled jobs.</p>
Disk Libraries Shared Disk Libraries With Static Mount Paths HDS DRU	A disk library with mount paths cannot be configured.	<ul style="list-style-type: none"> • Data protection operations and auxiliary copy operations to disk libraries will stop working. • New disk libraries cannot be configured. <p>The following will continue to work:</p> <ul style="list-style-type: none"> • Data recovery operations from disk libraries and storage policy copies created on media from disk libraries. • Data Aging of data from disk libraries. • Deconfiguration of disk libraries. 	<p>Before the application of a permanent license:</p> <ul style="list-style-type: none"> • Check if the number of Disk Library Support (DDO) licenses available in the permanent license is less than the number of evaluation DDO licenses in use. • If so, the number of disk libraries that make up the difference must be deconfigured first.
Data Encryption	The Data Encryption is not available in the CommCell Console at the client and subclient levels.	<ul style="list-style-type: none"> • The Data Encryption option from the properties of a client computer or a subclient is still available. • Data Protection operations of encrypted data will not run. These operations will resume functioning once the Data Encryption option is disabled. • Schedules of data protection operations of encrypted data cannot be saved or the jobs of the schedule cannot be run immediately. • Data recovery operations of encrypted data can be performed. 	The Data Encryption from the properties of all clients and subclients must first be disabled.
Data Multiplexing	The Data Multiplexing option is not available in the CommCell Console.	<ul style="list-style-type: none"> • The Data Multiplexing option on a storage policy copy is still available. • Data Protection operations that are multiplexed cannot run. Disabling the Data Multiplexing option on the appropriate storage policy copies will allow the operations to start running again. 	The Data Multiplexing option on all applicable storage policy copies within the CommCell must first be disabled.
GridStor	Alternate Data Paths (GridStor) cannot be configured.	<ul style="list-style-type: none"> • An operation that uses more than one data path cannot run. • Data recovery operations will still be able to run. 	Storage policy copies with more than one data path configured must first be configured with one data path.
Single Instancing of data (CAS - Content Addressed Storage)	The Single Instancing option is not available on a disk library or Centera Clusters.	<ul style="list-style-type: none"> • Data protection operations and auxiliary copy operations to libraries with the single instancing option enabled will stop running. • Libraries cannot be configured with the 	If any disk libraries has the single instancing option configured, disable the option from the library. If the single instancing option cannot be

		<p>single instancing option enabled.</p> <p>The following will continue to work from libraries:</p> <ul style="list-style-type: none"> • Data recovery operations from libraries with the single instancing option enabled. • Data Aging of data from libraries with the single instancing option enabled. • Deconfiguration of libraries with the single instancing option enabled. 	disabled on the library, the library must be deconfigured.
Block Level Data Deduplication on Disk Media	Cannot create storage policies/storage policy copies with Deduplication enabled. Note that the Subclient properties will still show the Deduplication option On.	Data Protection operations that are Deduplicated cannot run.	Delete all the Deduplication enabled Storage Policies before removing the feature license.
DVD Media UDO Media WORM Media	These media types are not available during or after library configuration.	<ul style="list-style-type: none"> • Data protection operations and auxiliary copy operations will fail. • Discovering these media types in the library or upon the configuration of a library will not work. <p>The following will continue to work:</p> <ul style="list-style-type: none"> • Data recovery operations from WORM/DVD/UDO media and storage policy copies created on WORM/DVD/UDO media. • Data Aging of data from WORM/DVD/UDO media. 	If any libraries have WORM, DVD, or UDO media configured, change the media type from the library properties first.
Erase Data by Browsing Erase Stubs	The Erase Data by Browsing and Erase Stubs options are not available in the CommCell Console.	<ul style="list-style-type: none"> • Items may be selected to be erased, but the list cannot be submitted from the Browse Options dialog box. • The Media password will be unavailable but can be reset. • Erase Data jobs cannot run. 	The media password can be set by a user.
Proxy Stub Subclient	<ul style="list-style-type: none"> • The Proxy Stub Subclient cannot be enabled. • The authentication credentials to access the filer for proxy stub recall capabilities cannot be configured. 	Recalling archived data from stubs will no longer be possible, however, you can still recover the data by performing a Browse and Recovery operation from the corresponding File Archiver for Windows Agent in the CommCell Console.	N/A
Client Computer Groups	The option to create a client computer group is not available in the CommCell Console.	<ul style="list-style-type: none"> • The Client Computer Groups that were already created will continue to exist and function. • Client Computer Groups can be removed, but new groups cannot be created. • A client cannot be added or removed from a client computer group. 	Delete all existing client computer groups.
CommCell Readiness Check	The CommCell Readiness Report is not available in the CommCell Console.	<ul style="list-style-type: none"> • If the CommCell Readiness Report is created, the report includes the message: License to run this report does not exist or has expired. • A schedule for the CommCell Readiness Report cannot be added. 	N/A
Single Sign On (SSO)	<ul style="list-style-type: none"> • Active Directory Service Provider credentials can be configured. • External user groups cannot be mapped to those created in the CommServe. • The CommServe cannot be accessed with the Active Directory credentials. 	<ul style="list-style-type: none"> • Active Directory Service Provider credentials can be configured. • External user groups cannot be mapped to those created in the CommServe. • The CommServe cannot be accessed with the Active Directory credentials. • Search or Content Indexing operations can be run. 	N/A
SnapProtect Backup	<ul style="list-style-type: none"> • The option to create a snapshot copy for a storage policy is not available. • The option to enable SnapProtect Backup for a client is not available. 	<p>SnapProtect Backup will fail.</p> <p>The following will continue to work:</p> <ul style="list-style-type: none"> • Data recovery operations from existing snapshots. 	N/A
ADVANCED FILE SYSTEM /DATAAGENT FEATURES			
Automatic File System Multi-Streaming	The option to select the number of readers (other than the default of 1) is unavailable	Scheduled Multi-stream File System backups cannot run.	No subclient should have the number of readers set to any

	in the CommCell Console.		other number than the default of 1.
Index Free Restores	A Restore by Job operation cannot be initiated.	Immediate or scheduled Restore by Job operations cannot run.	N/A
Restore Data Using a Mapped File	Data Recovery operations using mapped files cannot be initiated.	Immediate or scheduled data recovery operations using mapped files cannot run.	N/A
ADVANCED COPY FEATURES			
Inline Copy	The Inline Copy option is not available in the CommCell Console.	A data protection operation creating inline copies job will fail.	Disable the Inline Copy option on all applicable copies first.
Deferred Copy	The Deferred Copy option is not available in the CommCell Console.	Auxiliary Copy operations of Deferred copies will fail.	Disable the Deferred Copy option on all applicable copies first.
ADVANCED MEDIA MANAGEMENT FEATURES			
Unbuffered I/O	The Unbuffered I/O option is unavailable in the CommCell Console.	A job using unbuffered I/O will fail.	Disable the Unbuffered I/O option first (if it has been enabled).
Libraries with Mixed Drive Types	The option to create a drive pool with different drive types in the same library is unavailable in the Library and Drive Configuration window.	Operations using dissimilar drive types in the same library will fail. De-configure the dissimilar drive types to make sure that only homogenous drives are configured in the same library.	Deconfigure the dissimilar drive types to make sure that only homogenous drives are configured in the same library.
SCSI-3 Reserve/Release Resource Reservation	The option for SCSI-3 reservations is unavailable in the CommCell Console.	A job using a SCSI-3 reserve/release resource reservation will fail.	Disable the SCSI-3 option.
USB, FireWire and IP Libraries (Like libraries attached to ACSLS Server)	The option to configure these library types is unavailable in the Library and Drive Configuration window.	Jobs using these library types will fail. Redirect the subclients to different storage policies and run the jobs again.	De-configure any of these libraries (if these libraries are configured).
CONTENT INDEXING AND SEARCH			
Content Indexing and Search	The following packages cannot be installed: Offline Content Indexing Search Console	Content Indexing jobs will fail. Content Indexing searches can be performed. Data recovery operations of content indexing jobs can be performed.	Check if the number of permanent Content Indexing licenses is less than the number of evaluation licenses used. <ul style="list-style-type: none"> If so, the appropriate package must be uninstalled from the appropriate number of client computers to make up for the difference.

[Back To Top](#)

NUMBER OF SUPPORTED COMPONENTS WITHIN A COMMCELL

Each software license allows you to set up and configure the following components to a maximum limit within a CommCell:

EXPRESS COMMCELL	ENTERPRISE COMMCELL
25 Clients*	4000 Clients*
25 MediaAgents	4000 MediaAgents

* Maximum number of Client count is inclusive of MediaAgents.

BEST PRACTICES

It is recommended that your license file is kept in a safe place. This file is needed in case you need to recover your system, as described in Rebuild the CommServe.

RELATED ALERTS

JOB MANAGEMENT COMMCELL ALERT

The Job Management CommCell alert can be configured to notify users when the CommServe license will expire by enabling and configuring the **Alert**

CommServe License Expires With n Days criterion.

RELATED REPORTS

LICENSE SUMMARY REPORT

The License Summary Report provides information about the types of licenses in your CommCell.

[Back To Top](#)

License Administration - How To

[Topics](#) | [How To](#) | [How Do I](#) | [Related Topics](#)

[Update Licenses](#)

[Convert Evaluation Licenses to Permanent Licenses](#)

[View All Licenses](#)

[View Evaluation Usage](#)

[View the License Expiry Date for the CommServe](#)

[Configure Advanced Features - Express Version](#)

[Convert Evaluation Licenses to Permanent Licenses - Express Version](#)

[View All Licenses - Express Version](#)

[OEM Update License](#)

UPDATE LICENSES

Before you Begin

- If you are updating a feature license, you must re-login to the CommCell Console once the license is updated in order to see that feature.

Required Capability: See Capabilities and Permitted Actions

▶ To activate a license:

1. Obtain the necessary license disk from your software provider.
2. Insert the license disk into the CommServe computer or copy the license file to a network share.
3. From the CommCell Browser, right-click the CommServe icon, click **Control Panel**, and then click **License Administration**. This opens the License Administration window.
4. Select the Update License tab.
5. Specify the location of the license file and then click **Apply**.
6. The license is processed and the license information is updated in the License Administration dialog box.

If the operation is unsuccessful, a failure message is displayed in a pop-up window. Contact your software provider if the license update is unsuccessful.

CONVERT EVALUATION LICENSES TO PERMANENT LICENSES

Use this procedure if you wish to convert an evaluation license to a permanent license.

Before you Begin

- If you are converting a feature license, you must re-login to the CommCell Console once the license is updated in order to see that feature.

Required Capability: See Capabilities and Permitted Actions

▶ To convert a license:

1. From the CommCell Browser, right-click the CommServe icon, click **Control Panel**, and then click **License Administration**. This opens the License Administration window.

2. Select the Update License tab and then click **Convert**. The license type, client name, and license availability is displayed.
3. From the list of available licenses, check the box that corresponds to the evaluation license you would like to convert.
4. Click **Convert** to convert the license.
5. The license information is updated in the License Administration window.

If the operation is unsuccessful, a failure message is displayed in a pop-up window. Contact your software provider if the license update is unsuccessful.

VIEW ALL LICENSES

Required Capability: See Capabilities and Permitted Actions

▶ To view all licenses:

1. From the CommCell Browser, right-click the CommServe icon, click **Control Panel**, and then click **License Administration**. This opens the License Administration window.
 2. To view the license summary report, select the License Summary tab.

OR

To view specific details about each license in the CommCell, select the License Details tab. This information can be sorted, if desired, by clicking on the field name.
 3. Click **Close**.
-

VIEW EVALUATION USAGE

Required Capability: See Capabilities and Permitted Actions

▶ To view evaluation license usage:

1. From the CommCell Browser, right-click the CommServe icon, click **Control Panel**, and then click **License Administration**. This opens the License Administration window.
 2. Select the License Details tab and then click Evaluation Usage. The client name, license type, install date, and expiration date are displayed.
 3. Click **Close**.
-

VIEW THE LICENSE EXPIRATION DATE FOR THE COMMSERVE

Required Capability: See Capabilities and Permitted Actions

▶ To view the License Expiry Date for the CommServe:

1. From the CommCell Browser, right-click the CommServe icon, click **Control Panel**, and then click **License Administration**. This opens the License Administration window.
 2. Select the License Details tab. The **Expiration Date** field displays the expiration date for the CommServe.
 3. Click **Close** to close the dialog box.
-

CONFIGURE ADVANCED FEATURES - EXPRESS VERSION

Required Capability: See Capabilities and Permitted Actions

▶ To configure advanced features for Express versions of the software:

1. From the CommCell Console, right-click on the CommServe icon, click **Properties**, and then click the **Advanced Features** tab.
 2. Click the check box that corresponds to the feature you wish to configure.
 3. Click **OK**.
-

CONVERT EVALUATION LICENSES TO PERMANENT LICENSES - EXPRESS VERSION

The following procedure describes the steps involved in converting an evaluation license to a permanent license for Express versions of the software.

Before you Begin

- If you are converting a feature license, you must re-login to the CommCell Console once the license is updated in order to see that feature.

Required Capability: See Capabilities and Permitted Actions

▶ To convert a license:

1. From the CommCell Browser, right-click the CommServe icon, click **Control Panel**, and then click **License Administration**. This opens the License Administration window.
2. Select the Update License tab and then click **Convert**. The license type, client name, and license availability is displayed.
3. Click **Convert** for the license you wish to activate.
4. The license file is processed and the license information is updated in the License Administration window.

If the operation is unsuccessful, a failure message is displayed in a pop-up window. Contact your software provider if the license update is unsuccessful.

VIEW ALL LICENSES - EXPRESS VERSION

Required Capability: See Capabilities and Permitted Actions

▶ To view all licenses:

1. From the CommCell Browser, right-click the CommServe icon, click **Control Panel**, and then click **License Administration**. This opens the License Administration window.
 2. To view the license summary report, select the License Summary tab.
OR
To view specific details about each license in the CommCell, select the License Details tab. This information can be sorted, if desired, by clicking on the field name.
 3. Click **Close**.
-

OEM UPDATE LICENSE

The following procedure describes the steps to update OEM license from an Enterprise to Enterprise version or from an Express to Express version.

Required Capability: See Capabilities and Permitted Actions

▶ To update an OEM License:

1. Obtain the necessary licenses and the software discs (including the latest Service Packs) from your software provider.
 2. Follow the steps described in Update Licenses.
-

[Back To Top](#)

Disaster Recovery Backup

Topics | How To | Troubleshoot | Related Topics

Overview

- Types of Disaster Recovery Backups
- Phases of Disaster Recovery Backups
- Restore Disaster Recovery Backup Data

Disaster Recovery Backup Administration

- Change the Disaster Recovery Backup Destination
- Designate the Disaster Recovery User Account
- Retain Disaster Recovery Backups
- Run or Schedule a Disaster Recovery Backup
- View Disaster Recovery Backup History
- Job Restarts and Job Running Time

Best Practices

CommServe Disaster Recovery Tool

Related Reports

OVERVIEW

The software stores all information for the CommCell in a SQL database, and in the Windows registries. It is critical to be able to retrieve this information in the case of a disaster or system failure. This metadata and Windows registry data are backed up during a Disaster Recovery Backup. This data can be browsed and then restored using the CommServe Disaster Recovery Tool.

TYPES OF DISASTER RECOVERY BACKUPS

Disaster Recovery backs up the following types of data:

Metadata	Metadata includes the Microsoft SQL Server database that holds information about all CommCell and SRM database components (including clients , media configuration and Report Server for SRM).
Windows registry	The Windows registry is a central resource from which the Windows operating system obtains many of the system's operating parameters.
Firewall Configuration Files	The firewall configuration files (<code>FwPeers.txt</code> , <code>FwHosts.txt</code> and <code>FwPorts.txt</code>) are also included in the Disaster Recovery backup. If necessary, the entries associated with Clients/MediaAgents on the other side of the firewall from the CommServe can be restored in the event of a CommServe re-build. Note that a restore of the disaster recovery backup does not automatically restore the firewall files. To restore these files, manually select these files for restore from the CommServe Disaster Recovery Tool. See Restore a Disaster Recovery Backup for step-by-step instructions.

The following types of Disaster Recovery Backups are supported:

Full	Does a complete backup of CommServe and SRM database.
Differential	Backs up only that data in the CommServe and SRM database that has changed since the last full backup.

Regardless of the backup type, the registry hive is always fully backed up.

PHASES OF DISASTER RECOVERY BACKUPS

Disaster Recovery Backups are executed in two phases: Export and Backup. During the Export phase, Disaster Recovery Backup copies data to a local or network path. If necessary, a network path pointing to the hot-site can be established. The Backup phase scans the data for missing files, backs up data to media using a Disaster Recovery Backup storage policy, and then indexes and archives the data for long-term retention.

Disaster Recovery Backup will check the CommServe database for any type of corruption. If database corruption is detected, all CommServe job activities are disabled. Contact your software provider for assistance with database corruption.

By default, when a Disaster Recovery Backup detects database corruption, all CommServe job activities are disabled. To allow CommServe job activities to continue regardless of database corruption, use the `DisableActivityOnDbCorruption` registry key.

EXPORT PHASE - DISASTER RECOVERY BACKUP TO DISK

This phase does a Disaster Recovery Backup to the destination File System directory chosen during the installation of the CommServe (a local drive on the CommServe or a network destination). This directory can be changed from the DR Backup Settings (Export Settings) dialog box in the Control Panel of the CommCell Console. If a network destination is chosen, then an appropriate user account must also be specified, as described in Designate the Disaster Recovery User Account.

- The directory file path selected for this phase should not be located on a FAT drive. A FAT drive cannot be supported for this feature because it does not allow a temporary sparse file to be generated when creating the database snapshot, which is required for data verification; this may cause the phase to fail in its attempt to backup the database.
- If there is no MediaAgent configured, it is recommended that you specify a network share for the Disaster Recovery Backup destination folder.

SET_XXX directories are created under the specified destination. Each set holds information about the metadata and the registry. It contains the following files:

DISASTER RECOVERY BACKUP FILES

File	Description
commserv_FULL.dmp	This full .dmp file represents a full backup of the CommServe database. This full backup was backed up using Disaster Recovery backups.
commserv_DIFF_XXX.dmp	This differential .dmp file represents a differential backup of the CommServe database. This differential backup was backed up using Disaster Recovery backups. <i>xxx is a sequential number for the file. The highest number is associated with the latest Disaster Recovery backup.</i>
commserv_hive.reg	The CommServe registry full backup file.
commserv_hive_XXX.reg	The CommServe registry differential backup file. <i>xxx is a sequential number for the file. The highest number is associated with the latest Disaster Recovery backup.</i>
QNet_<cs_sitename>_FULL.dmp	This full .dmp file represents a full backup of the CommNet Server database. This full backup was backed up using Disaster Recovery backups.
QNet_<cs_sitename>_DIFF_XXX.dmp	This differential .dmp file represents a differential backup of the CommNet Server database. This differential backup was backed up using Disaster Recovery backups. <i>xxx is a sequential number for the file. The highest number is associated with the latest Disaster Recovery backup.</i>
SRM_<cs_sitename>_FULL.dmp	This full .dmp file represents a full backup of the SRM Server database. This full backup was backed up using Disaster Recovery backups.
SRM_<cs_sitename>_DIFF_XXX.dmp	This differential .dmp file represents a differential backup of the SRM Server database. This differential backup was backed up using Disaster Recovery backups. <i>xxx is a sequential number for the file. The highest number is associated with the latest Disaster Recovery backup.</i>
Other Files	Depends on the software module installed, e.g., firewall configuration files.

Data is backed up from the SQL server and is written to the user-defined destination. If this phase is unable to get a response from the SQL server, the software will retry up to 10 times at 30 minute intervals. If the software can get the data but cannot write to the user defined destination, it will retry the creation the directory structure specified for the Disaster Recovery Backup destination. If it cannot, then it will directly go to the second phase.

Disaster Recovery Backup files (.dmp) are portable between CommServe computers running Microsoft Windows Server 32-bit and x64 edition operating systems.

BACKUP PHASE - DISASTER RECOVERY BACKUPS TO MEDIA USING A DISASTER RECOVERY BACKUP STORAGE POLICY

In this phase, a copy of the data backed up in the Export phase as well as the non-active log files are first scanned for any additional system configuration files (not affiliated with the software) that should be included in the backup, and then written to media using a Disaster Recovery Backup or standard storage policy.

If configured to do so, this phase will also backup log files from selected clients. With log files providing the processing details of operations that have occurred on your system, this is especially useful for troubleshooting. For step-by-step instructions, see Schedule a Disaster Recovery Backup.

A default Disaster Recovery Backup storage policy [CommServeDR (host name)] is automatically created when the first library in the CommCell is configured. This type of storage policy is recommended because it only writes the Disaster Recovery Backup data to the media, and its default retention period is defined as 60 days and 60 cycles, which can be easily changed during configuration. The media being used for this storage policy should be removable to prevent accidental data loss due to system failure. If the first library configured is a disk library, change your Disaster Recovery Backup configuration to use a Disaster Recovery Backup storage policy associated with a tape library as soon as the first tape library is configured. You can create as many Disaster Recovery Backup storage policies as needed.

When there is no secondary copy using a tape library for the active disaster recovery storage policy, a secondary copy will be automatically created when you configure a tape library. Also, an automatic auxiliary copy schedule will be created, which will run every 15 minutes.

Though it is recommended to use a Disaster Recovery Backup storage policy in your configuration, standard storage policies can be used as well. If you select a standard storage policy for your configuration, the media will contain a mix of Disaster Recovery Backup data as well as standard backup data. This is not a recommended configuration because the retention rules of the standard storage policy will apply to all the data written to the media for that storage policy regardless of data type, standard backup versus Disaster Recovery Backup data. If the storage policy's retention rules are met, the data will be aged; and if this occurs prior to running another Disaster Recovery Backup, the Disaster Recovery Backup data will be lost.

If the software cannot write data to the media for any reason, it will retry up to ten times at 30 minute intervals. By default, Disaster Recovery Backup data written to media in the Backup phase is retained indefinitely, but can be changed from the DR Backup Settings dialog box.

For more information on Disaster Recovery Backup storage policies, see Storage Policies.

Once the data has been written to the media, it will be indexed for browsing and archived for long-term retention.

RESTORE DISASTER RECOVERY BACKUP DATA

Disaster Recovery Backup data can be restored at any production site or a hot-site any time using the CommServe Disaster Recovery Tool; however, the operation must be run on a CommServe machine that does not have any other platforms installed, e.g., MediaAgents, iDataAgents. Running the restore on a CommServe-only machine ensures that conflicts caused by mismatched product versions or dynamic-link library (DLL) files are avoided. The backup data can be restored from the Export Destination (Disaster Recovery Backups on disk) or the Backup Destination (Disaster Recovery Backups on media).

Disaster Recovery Backups of data can also be browsed and restored by using the DR Restore option. For more information, see Restore by Jobs and Browse and Recover Disaster Recovery Backup Data.

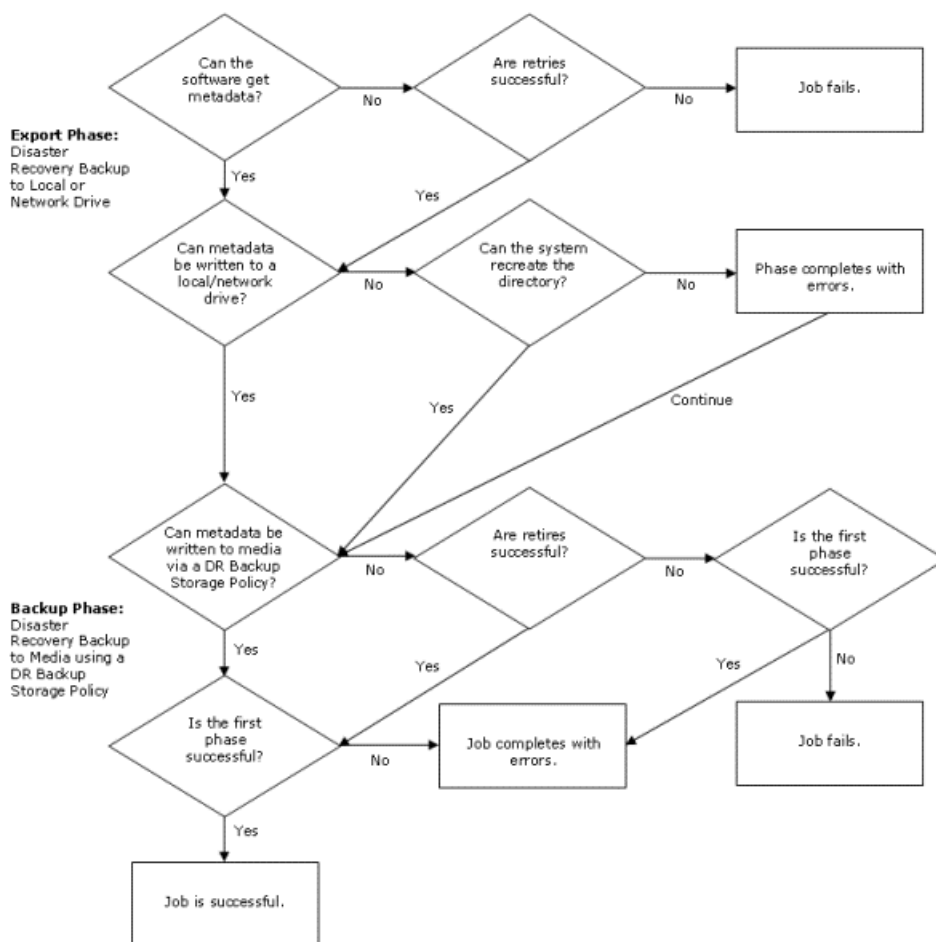
The browse option is only available for Disaster Recovery Backups executed in Release 7.0 and beyond.

Disaster Recovery backups are located on a disk drive (SET files), and can be restored using the CommServe Disaster Recovery Tool. If the destination of these Disaster Recovery Backups is on a network drive, the SET file must be copied to a local disk drive to the CommServe before using the CommServe Disaster Recovery Tool. See CommServe Disaster Recovery Tool for more information.

If Disaster Recovery backup data is located on media, you must first restore the data from media using Media Explorer. After Media Explorer restores the data to the local computer, you can use the CommServe Disaster Recovery Tool to restore the data. For information, see Recover CommServe Disaster Recovery Data Using Media Explorer.

STATUS OF DISASTER RECOVERY BACKUP JOBS

The status in which a Disaster Recovery Backup job can finish is explained in the following flowchart:



DISASTER RECOVERY BACKUP ADMINISTRATION

This section describes the following:

- Change the Disaster Recovery Backup destination.
- Designate the Disaster Recovery Backup user account.
- Retain Disaster Recovery Backups.
- Run or Schedule a Disaster Recovery Backup.
- View Disaster Recovery Backup history.

CHANGE THE DISASTER RECOVERY BACKUP DESTINATION

You can change either the Disaster Recovery Backup Export or Backup destination.

CHANGE THE DISASTER RECOVERY EXPORT DESTINATION

The Disaster Recovery Backup Export destination can be changed from the `Export` pane of the DR Backup Settings (Export Settings) dialog box.

CHANGE THE DISASTER RECOVERY BACKUP DESTINATION

The Disaster Recovery Backup Backup destination can be changed from the `Backup` pane of the DR Backup Settings (Export Settings) dialog box.

DESIGNATE THE DISASTER RECOVERY USER ACCOUNT

If backups are going to a remote location, after installing the CommServe software, you need to identify the Windows user account under which Disaster Recovery Backups are to be conducted. In order for Disaster Recovery Backups to work successfully on the network path, the specified Windows account must be a domain administrative account for the domain containing the Disaster Recovery backup destination directory.

You can designate the Disaster Recovery Backup user account from the `Change User Account` dialog box.

RETAIN DISASTER RECOVERY BACKUPS

You can determine the number of Disaster Recovery backups to retain on disk and media.

DETERMINE THE NUMBER OF DISASTER RECOVERY BACKUPS TO RETAIN ON DISK

When the metadata is backed up and archived, it remains valid (available for restoration) for a period of time determined by the number of backup sets to retain. The retention rule is determined by the number of successful full backup cycles to be maintained.

The number of Disaster Recovery backup sets is preset to five full backups during installation. This can be changed from the DR Backup Settings dialog box. This retention count refers to the number of backup sets created during the Export phase of the Disaster Recovery Backup. Retention time for copies written to media drives during Backup phase are determined by the characteristics of the Disaster Recovery Backup storage policy.

After each successful Disaster Recovery Backup, the system checks to see if the number of retained successful backup sets has exceeded the number of sets to retain. If expired data exists, it is automatically pruned. However, if the Disaster Recovery backup finished in the Backup phase with the status of Completed With One or More Errors, those backups sets that were not successfully copied to media will not be pruned from the disk.

If a Disaster Recovery Backup job returns with a status of Completed With One or More Errors, the data or partial sets will be kept for 90 days and removed when the next Disaster Recovery Backup is run. The number of days partial Disaster Recovery Backup data will be retained before it is aged can be changed from the default of 90 days using the `SetLifeSpanForFailedDR` registry key.

CYCLE

A cycle begins with the successful completion of a full backup and includes all differential backups up to the next full backup. A cycle is not complete until the full backup that follows it has successfully completed. A cycle is considered successful only if the last differential backup of the set succeeds.

The final differential backup must be successful in order to restore the CommServe database to the point at which the cycle completed, regardless of whether any intermediate differential backups failed. It is the final differential backup that includes all changes to the data since the time of the initial, full backup. However, if the final differential is unsuccessful, the CommServe cannot be restored to the point in time at which the cycle completed; therefore, if the final differential is unsuccessful, that cycle is not counted towards the retention rule.

DETERMINE THE NUMBER OF DISASTER RECOVERY BACKUPS TO RETAIN ON MEDIA

Disaster Recovery Backups are retained on media, depending on the retention rule of the Disaster Recovery Backup storage policy. After the retention rule of the storage policy has expired, the Disaster Recovery Backup data can be pruned using the data aging operation. See [Data Aging](#) for more information.

You can set the number of Disaster Recovery Backups to retain on media from the `Number of full Metadata Backups to be retained` field of the DR Backup Settings dialog box.

RUN OR SCHEDULE A DISASTER RECOVERY BACKUP

This section describes how to run or schedule a Disaster Recovery Backup, view backup history, and the related reports. By default, a full Disaster Recovery Backup is run every day at 10:00am.

Disaster Recovery Backups will run only when the SQL server is run as a system account (on a non-clustered computer). On a clustered computer, Disaster Recovery Backups will run only when the SQL server is run on a Windows account.

The number of times these full backups occur depend on the following:

- The number of clients in your CommCell.
- Complexity of your backup scheme.
- CommServe security requirements.
- Availability of CPU and network resources.

You can run or schedule a Disaster Recovery Backup from the Disaster Recovery Backup Options dialog box. From this dialog box, you can select the following type of backup operation:

- Full or Differential which will perform Full or Differential (data that is new or has changed since the last full backup) backups.
- **Shrink DB** option which will compress the database and database log file prior to the backup operation

Select this option only when no jobs are running in the CommCell Console. Enabling this option during the active jobs may affect other operations.

- **Enable database(s) backup compression** option which will compress the database backup file (*.dmp)

Shrink DB and **Enable database(s) backup compression** options are useful if free space on the CommServe computer is an issue. If space is not an issue, it is not necessary to select these options.

VIEW DISASTER RECOVERY BACKUP HISTORY

The history of Disaster Recovery Backups allows you to view the status of an Disaster Recovery Backup job and the time the job started and ended. You can also view the media that job used and the events of the job.

See Admin Job History for more information on Disaster Recovery Backup job history.

JOB RESTARTS AND JOB RUNNING TIME

You can click the **Job Retry** tab in the **Disaster Recovery Backup Options** dialog box to access the Job Retries and Job Running Time options, when you perform a Disaster Recovery Backup operation.

You can also specify the maximum number of allowed restart attempts and the interval between restart attempts for all Disaster Recovery Backup jobs. For procedures, see Specify Job Restartability for the CommCell.

For more information on these subjects, see Restarting Jobs and Job Running Time.

BEST PRACTICES

DISASTER RECOVERY BACKUP STORAGE POLICIES

- A default Disaster Recovery Backup storage policy [CommServeDR (host name)] is automatically created when the first library in the CommCell is configured. This type of storage policy is recommended because it only writes the Disaster Recovery Backup data to the media, and its default retention period is defined as 60 days and 60 cycles, which can be easily changed during configuration. The media being used for this storage policy should be removable to prevent accidental data loss due to system failure. If the first library configured is a disk library, change your Disaster Recovery Backup configuration to use a Disaster Recovery Backup storage policy associated with a tape library as soon as the first tape library is configured. You can create as many Disaster Recovery Backup storage policies as needed.

When there is no secondary copy using a tape library for the active disaster recovery storage policy, a secondary copy will be automatically created when you configure a tape library. Also, an automatic auxiliary copy schedule will be created, which will run every 15 minutes.

- By default, the retention period for Disaster Recovery Backup data is set to be retained for 60 days and 60 cycles. If you want to change the retention time for Disaster Recovery Backup data, it is recommended that you keep the default setting as the minimum with predefined extended retention rules defined as: weekly = 180 days, and monthly = infinite.

COMMSERVE DISASTER RECOVERY TOOL

The CommServe Disaster Recovery Tool restores the meta data (stored in the CommServe SQL database) from the Disaster Recovery Backup file. The Disaster Recovery Backup file gets created when a Disaster Recovery backup is performed from the CommCell Console. See CommServe Disaster Recovery Tool for more information.

RELATED REPORTS

ADMINISTRATIVE JOB SUMMARY REPORT

The Administrative Job Summary Report displays a summary of all or select Administrative jobs.

DISASTER RECOVER BACKUP JOB SUMMARY REPORT

The Disaster Recover Backup Job Report displays a list of Disaster Recovery backup jobs.

[Back To Top](#)

Disaster Recovery Backup - How To

[Topics](#) | [How To](#) | [Troubleshoot](#) | [Related Topics](#)

Designate the Disaster Recovery User Account

Select a Disaster Recovery Export Destination

Select a Disaster Recovery Backup Destination

Select the Number of Disaster Recovery Backups to Retain on Disk

Select the Number of Disaster Recovery Backups to Retain on Media

Schedule a Disaster Recovery Backup

Start a Disaster Recovery Backup

Browse and Recover Disaster Recovery Backup Data

Add Pre/Post Commands to Disaster Recovery Backup Settings

DESIGNATE THE DISASTER RECOVERY USER ACCOUNT

Before You Begin

For Disaster Recovery backups to work successfully for the new user, this user must have a minimum of read/write permissions to the Disaster Recovery backup destination directory.

Required Capability: Capabilities and Permitted Actions

▶ To designate the Disaster Recovery account:

1. In the CommCell Browser, right-click the CommServe, click **Control Panel**, and then click **DR Backup Settings**.
2. From the DR Backup Settings (Export Settings) dialog box, click the **Change** button associated with the **User Name** field.
3. In the Change User Account dialog box, type the user name and password of the Windows user account under which you want the Disaster Recovery backups conducted. Type the password a second time to confirm it, and click **OK**.
4. The Disaster Recovery program does not attempt to validate the user name and password at the time it is entered/modified through the DR Backup Settings (Export Settings) dialog box. To validate the user name and password, run an immediate Disaster Recovery backup.

SELECT A DISASTER RECOVERY BACKUP EXPORT DESTINATION

Before You Begin

- Network drives that are mapped to local drive letters must still be specified using the UNC network path. Mapped drive letters cannot be used because they are only valid for the currently logged in Windows user, who may not be logged in when the Disaster Recovery backup job is run. If you want to access a network path, the CommServe must be in the domain. If the network directory is going to another domain, this domain where the CommServe is must be the trusted domain.
- If you change the destination for the Disaster Recovery backup data, you will be prompted to enter the user name and password information required to access the network share or local directory in the Change User Account dialog box.

Required Capability: Capabilities and Permitted Actions

▶ To select an Disaster Recovery Backup Export destination:

1. In the CommCell Browser, right-click the CommServe, click **Control Panel**, and then click **DR Backup Settings**.
2. From the DR Backup Settings (Export Settings) dialog box, select either **Use Network Share** or **Use Local Drive** in the **Backup Metadata Destination Folder Type** field.
3. Enter or use the **Browse** button to specify a backup path in the **Back Up Metadata to this Folder** field.

NOTE

If you are backing up to a network drive, then this directory must be a valid UNC network path in the UNC format \\<server>\<share>\path. If you are backing up to a local drive, then this drive must be a local CommServe drive.

SELECT A DISASTER RECOVERY BACKUP DESTINATION

Before You Begin

- Network drives that are mapped to local drive letters must still be specified using the UNC network path. Mapped drive letters cannot be used because they are only valid for the currently logged in Windows user, who may not be logged in when the Disaster Recovery backup job is run. If you want to access a network path, the CommServe must be in the domain. If the network directory is going to another domain, this domain where the CommServe is must be the trusted domain.
- When specifying a network location:
 - The destination computer must either be in the same domain of the CommServe, or in a domain that has a proper two-way trust relationship with the CommServe.
 - A proper account (with enough rights to write to the destination computer) must be provided. This can be achieved by designating a proper Disaster Recovery user account.
 - If the network location is then changed to a (local) destination, it is recommended not to use the same account since write operations use local administrator security permissions.

Required Capability: Capabilities and Permitted Actions

▶ To select an Disaster Recovery Backup destination:

1. In the CommCell Browser, right-click the CommServe, click **Control Panel**, and then click **DR Backup Settings**.
2. From the DR Backup Settings (Export Settings) dialog box, select a storage policy from the **Back Up Metadata to this DR Storage Policy** dropdown list.
3. Click **OK**.

SELECT THE NUMBER OF DISASTER RECOVERY BACKUPS TO RETAIN ON DISK

Before You Begin

The number of Disaster Recovery backups you select to retain on disk refers to the number of backups created during the exporting of a Disaster Recovery backup. The number of Disaster Recovery backups created during the backup that are retained on media are determined by the retention criteria of the Disaster Recovery Backup storage policy.

Required Capability: Capabilities and Permitted Actions

▶ To select the number of Disaster Recovery backups to retain on disk:

1. In the CommCell Browser, right-click the CommServe, click **Control Panel**, and then click **DR Backup Settings**.
2. From the DR Backup Settings (Export Settings) dialog box, select a number from the **Number of Full Metadata Backups to be retained** field.
3. Click **OK**.

SELECT THE NUMBER OF DISASTER RECOVERY BACKUPS TO RETAIN ON MEDIA

Before You Begin

- The number of Disaster Recovery backups that are retained on media are determined by the retention rules of the Disaster Recovery backup storage policy.

Required Capability: Capabilities and Permitted Actions

▶ To select the number of Disaster Recovery backups to retain on media:

1. See Changing the Retention Rules of a Storage Policy Copy.

SCHEDULE A DISASTER RECOVERY BACKUP

Before You Begin

- Disaster Recovery Backups will run only when the SQL server is run as a System Account (on a non-clustered computer).
- Do not schedule many Backups while a Disaster Recovery Backup job is running. If you receive any timed out or failed events, run the Disaster Recovery Backup job again.
- A proper strategy should consist of at least one full backup performed every day and several differential backups performed during the day.
- A Disaster Recovery Backup job has the highest priority. Therefore, this job will interrupt other jobs, if needed.
- Once started, if a Disaster Recovery Backup job cannot be completed, the Job Manager will retry the job up to a total of five hours at 30-minute intervals for a maximum of 10 times.

Required Capability: Capabilities and Permitted Actions

▶ To schedule a Disaster Recovery Backup:

1. From the CommCell Browser, right-click the CommServe, click **All Tasks**, and then click **Disaster Recovery Backup**.
2. From the Disaster Recovery Backup Options (General) window, select the type of backup, **Full** or **Differential**. If necessary, select the option to **Shrink DB** and/or **Enable database(s) backup compression**.
 - Select **Shrink DB** option only when no jobs are running in the CommCell Console. Enabling this option during the active jobs may affect other operations.
 - If free space is not an issue on the CommServe computer, it is not necessary to select these (Shrink DB and/or Enable database(s) backup compression) options.
3. Select the Client Selection tab to backup up the log files from clients with your CommCell. Select the client(s) from the available list of clients. You can also back up the log files from MediaAgents. This is useful for troubleshooting purposes, especially in deduplication configurations.
4. Select the **Job Retry** tab to specify the job running time and the number of job retries. See Restarting Jobs and Job Running Time for more information. Note that the **Number of Retries** specified for this particular job will only be used by the system if Disaster Recovery Backup was configured as a **Restartable** job type in the Job Management Control Panel. For step-by-step instructions, see Specify Job Restartability for the CommCell.
5. Click **Schedule**.
6. From the Schedule Details tab, select the necessary scheduling options
7. To view the job summary for the Disaster Recovery Backup job that you have scheduled, click the Job Summary tab.
8. Click **OK** to save the schedule.

START A DISASTER RECOVERY BACKUP

Before You Begin

- Disaster Recovery Backups will run only when the SQL server is run as a System Account (on a non-clustered computer).
- Disaster Recovery Backup will check the CommServe database for any type of corruption. If database corruption is detected, all CommServe job activities are disabled. Contact your software provider for assistance with database corruption.
- Do not schedule many backups while a Disaster Recovery Backup job is running. If you receive any timed out or failed events, run the Disaster Recovery Backup job again.
- A proper strategy should consist of at least one full backup performed every day and several differential Backups performed during the day.
- A Disaster Recovery Backup job has the highest priority. Therefore, this job will interrupt other jobs, if needed.
- Once started, if a Disaster Recovery Backup job cannot be completed, the Job Manager will retry the job up to a total of five hours at 30-minute intervals for a maximum of 10 times.

Required Capability: Capabilities and Permitted Actions

▶ To start a Disaster Recovery Backup:

1. From the CommCell Browser, right-click the CommServe, click **All Tasks**, and then click **Disaster Recovery Backup**.
2. From the Disaster Recovery Backup Options (General) window, select the type of backup, **Full** or **Differential**. If necessary, select the option to **Shrink DB** and/or **Enable database(s) backup compression**.
 - Select **Shrink DB** option only when no jobs are running in the CommCell Console. Enabling this option during the active jobs may affect other operations.
 - If free space is not an issue on the CommServe computer, it is not necessary to select these (Shrink DB and/or Enable database(s) backup compression) options.
3. Select the Client Selection tab to backup up the log files from clients with your CommCell. Select the client(s) from the available list of clients. You can also

back up the log files from MediaAgents. This is useful for troubleshooting purposes, especially in deduplication configurations.

4. Select the **Job Retry** tab to specify the job running time and the number of job retries. See Restarting Jobs and Job Running Time for more information. Note that the **Number of Retries** specified for this particular job will only be used by the system if Disaster Recovery Backup was configured as a **Restartable** job type in the Job Management Control Panel. For step-by-step instructions, see Specify Job Restartability for the CommCell.
5. Click **Schedule** to schedule the backup at another time, or click **OK** to run it immediately. For more information on scheduling a back, see Scheduling a Disaster Recovery Backup.

BROWSE AND RECOVER DISASTER RECOVERY BACKUP DATA

Required Capability: Capabilities and Permitted Actions

▶ To start a Disaster Recovery Backup:

1. From the CommCell Browser, right-click the CommServe, click **All Tasks**, and then click **DR Restore** and **Browse and Recover**.
2. From the Browse Options dialog box, select the appropriate options for the disaster recovery backup data you wish to browse.
3. Click **OK**.
4. Select the data to be recovered from the **Client (Media Agent)** window, and then click **Recover All Selected...**
5. From the Restore Options from All Selected Options (General) dialog box, select the appropriate options for restoring the data.
6. Click the **Advanced** button for additional restore options, and click **OK**.
7. Click **OK**.

ADD PRE/POST COMMANDS TO DISASTER RECOVERY BACKUP SETTINGS

Required Capability: Capabilities and Permitted Actions

▶ To add pre/post commands to the Disaster Recovery Backup settings:

1. In the CommCell Browser, right-click the CommServe, click **Control Panel**, and then click **DR Backup Settings**.
2. From the DR Backup Settings (Pre/Post Process) dialog box, click inside the text box that corresponds to the phase that you want to start the process. Enter the full path of the process (i.e., batch file or shell script) that you want executed. Alternatively, use **Browse** to locate the process (applicable only for paths that do not contain any spaces).
3. If you want to run the *PostScan* or *PostBackup* processes for all attempts, then select the corresponding checkbox. (This will run both pre and post processes for all attempts.)
4. If no Pre/Post Impersonation account is currently selected, or if you want to change the account, select **Change**.
5. Select **Use Local System Account**, or select **Impersonate User** and enter a user name and password. Click **OK**.

NOTE

If you selected **Use Local System Account**, click **OK** to the message advising you that commands using this account have rights to access all data on the client computer.

6. Click **OK** to save your entries. This closes the Pre/Post commands dialog box.

[Back to Top](#)

CommServe Disaster Recovery Tool

Topics | How To

The CommServe Disaster Recovery Tool restores the metadata (stored in the CommServe SQL database or SRM Server database) from the Disaster Recovery Backup file. The Disaster Recovery Backup file gets created when a Disaster Recovery backup is performed from the CommCell Console.

The CommServe Disaster Recovery Tool can be used to restore data in the following situations:

- Rebuild the CommServe/CommNet/SRM on the same computer
- Rebuild the CommServe/CommNet/SRM on a different computer
- Change the name of the CommServe computer
- Create and maintain a CommServe in the hot-site
- Update license. (This involves using the Microsoft SQL Server (Enterprise Edition) instead of Microsoft SQL Server Desktop Engine (MSDE) as the database engine.)
- Migrate the CommServe database either from a clustered environment to a non-cluster environment, or from a non-clustered environment to a clustered environment.

If you change the name of the CommServe computer, be sure to Perform Post-Recovery Operations.

Disaster Recovery Backup files are located in the SET_XXX folders (where XXX is replaced by a sequential number and the folder with the highest number contains the latest Disaster Recovery Backup set). The SET_XXX folders, which are located in the File System directory chosen during the installation of the CommServe, contain a number of files, including a .dmp file. Refer to the following table for the types of .dmp files that can be restored using the CommServe Disaster Recovery Tool.

DISASTER RECOVERY BACKUP FILES

File	Description
commserv_FULLL.dmp	This full .dmp file represents a full backup of the CommServe database. This full backup was backed up using Disaster Recovery backups.
commserv_DIFF_xxx.dmp	This differential .dmp file represents a differential backup of the CommServe database. This differential backup was backed up using Disaster Recovery backups. <i>xxx is a sequential number for the file. The highest number is associated with the latest Disaster Recovery backup.</i>
commserv_hive.reg	The CommServe registry full backup file.
commserv_hive_xxx.reg	The CommServe registry differential backup file. <i>xxx is a sequential number for the file. The highest number is associated with the latest Disaster Recovery backup.</i>
QNet_<cs_sitename>_FULLL.dmp	This full .dmp file represents a full backup of the CommNet Server database. This full backup was backed up using Disaster Recovery backups.
QNet_<cs_sitename>_DIFF_xxx.dmp	This differential .dmp file represents a differential backup of the CommNet Server database. This differential backup was backed up using Disaster Recovery backups. <i>xxx is a sequential number for the file. The highest number is associated with the latest Disaster Recovery backup.</i>
SRM_<cs_sitename>_FULLL.dmp	This full .dmp file represents a full backup of the SRM Server database. This full backup was backed up using Disaster Recovery backups.
SRM_<cs_sitename>_DIFF_xxx.dmp	This differential .dmp file represents a differential backup of the SRM Server database. This differential backup was backed up using Disaster Recovery backups. <i>xxx is a sequential number for the file. The highest number is associated with the latest Disaster Recovery backup.</i>
Other Files	Depends on the software module installed, e.g., firewall configuration files.

You can also restore any other full backup that does not have the <cs_sitename>_FULLL.dmp naming convention. However, if you need to restore a differential file, then it must follow the above naming convention.

Before using the CommServe Disaster Recovery Tool, ensure that you have the correct version of the Disaster Recovery Backup files (SET_XXX), which you want to restore, on the local computer. You can find the Disaster Recovery Backup Job ID and the time when the backup job completed by viewing the version.txt file in the SET_XXX folder. It is also necessary to backup the CommServe database before using this tool; this will ensure no loss of current activity. Note that Disaster Recovery Backup files (.dmp) are portable between CommServe computers running Microsoft Windows Server 32-bit and x64 edition operating systems.

Disaster Recovery Backup data can be restored at any production site or a hot-site any time using the CommServe Disaster Recovery Tool; however, the operation must be run on a CommServe machine that does not have any other platforms installed, e.g., MediaAgents, iDataAgents. Running the restore on a CommServe-only machine ensures that conflicts caused by mismatched product versions or dynamic-link library (DLL) files are avoided. The backup data can be restored from the Export Destination (Disaster Recovery Backups on disk) or the Backup Destination (Disaster Recovery Backups on media).

Disaster Recovery Backup data can be restored to a disaster recovery server (or computer that has the disaster recovery server IP address.) Note that the reverse is not possible. e.g., you cannot perform a disaster recovery backup from the hot-site and restore it in the original production CommServe. To perform

this operation you must obtain a license and an IP Address Change license from your software provider.

Users can be notified via e-mail once the restore operation has completed. This must be set during the configuration of the restore operation. For more information, see [Restore a Disaster Recovery Backup](#).

Note that the CommServe Database can be restored with a different name for viewing purposes. Functionality of the database requires it to be restored with the same name. You can change the name of the database using the **Restore as DB** field in the SQL Restore tab.

- If you have the Disaster Recovery Backup files on the local disk, follow the procedure to [Restore a Disaster Recovery Backup](#).
- If you have the Disaster Recovery Backup files on the network drive, copy the files to the local disk and then follow the procedure to [Restore a Disaster Recovery Backup](#).
- If you have the Disaster Recovery Backup files on a media, use **Media Explorer** to retrieve the data from the media to the local disk and then follow the procedure to [Restore a Disaster Recovery Backup](#).

CommServe Disaster Recovery Tool - How To

Topics | [How To](#)

Start the CommServe Disaster Recovery Tool

Restore a Disaster Recovery Backup

- Restore the CommServe Database (Restore Database Tab)
- Change the Name of the CommServe (Name/License Change Tab)
- Activate the License (Name/License Change Tab)
- Perform Post-Recovery Operations (Post Recovery Tab)

Perform Cluster Migration

Start the CommServe Disaster Recovery Tool

To start the CommServe Disaster Recovery Tool:

1. From the Windows Explorer, navigate to the `<software installation path>\base` folder.
2. Double-click **CommserveDisasterRecoveryGUI.exe**.

If you run the restore on a CommServe machine with other platforms installed, e.g., MediaAgent, iDataAgents, you will be prompted with an error message. You must run the Disaster Recovery Backup Restore on a CommServe-only machine.

Restore a Disaster Recovery Backup

Before You Begin

- Apply the latest updates and service packs to the CommServe computer.
- Disaster Recovery Backup data can be restored at any production site or a hot-site any time using the CommServe Disaster Recovery Tool; however, the operation must be run on a CommServe machine that does not have any other platforms installed, e.g., MediaAgents, iDataAgents. Running the restore on a CommServe-only machine ensures that conflicts caused by mismatched product versions or dynamic-link library (DLL) files are avoided. The backup data can be restored from the Export Destination (Disaster Recovery Backups on disk) or the Backup Destination (Disaster Recovery Backups on media).
- Prior to running the CommServe Disaster Recovery Tool to restore your Disaster Recovery Backup Data, be sure to backup the CommServe, CommNet and/or SRM databases; this will ensure no loss of current activity.
- A SQL Server user account is required to perform Disaster Recovery operations.
- When restoring CommNet or SRM components, you must also restore the CommServe database. You can not restore CommNet or SRM components independently. Furthermore, the order in which the databases should be restored are as follows:
 - CommServe
 - CommNet
 - SRM

To restore a Disaster Recovery Backup:

RESTORE THE COMMSERVE DATABASE (RESTORE DATABASE TAB)

This section must be completed for all restore operations.

1. From the Windows Explorer, navigate to the `<software installation path>\base` folder.
2. Double-click **CommserveDisasterRecoveryGUI.exe**. This will launch the CommServe Disaster Recovery Tool.
3. In the Restore Database tab, click the **Restore DB** checkbox to enable the recovery.
4. Enter the SQL Server user account credentials in the **Destination SQL Server Info** fields.
5. Specify the restore options:
 - Select **Restore All Databases From Folder** to restore multiple databases from the specified folder containing the dump files.
 - Select **Restore Single Database** to restore a single dump file containing the database.
6. If necessary, click the Browse (...) button for **Restore Path** to change the target location of the files from the **Restore DR DB file as** dialog box. To change the target click a row in the **Physical File Name** column and type the new location and then click **Find and Replace**.

For more information, refer to Disaster Recovery Backup Files.
7. In the **Restore file** field, type or browse the name of the Disaster Recovery Backup file or folder where the dump files are located.

For more information, refer to Disaster Recovery Backup Files.

If necessary, enter another name for the database to be restored in the **Overwrite Database Name** field.

The CommServe Database can be restored with a different name for viewing purposes only. Functionality of the database requires it to be restored with the same name.

Note that when browsing for files, it may take a minute for the corresponding fields to be populated with the selected file path.
8. You can have an e-mail sent to a user indicating that the restore operation has completed. The mail server must be configured in this dialog box.
 - Specify a valid **Mail Server** to be used for e-mail messages.
 - Select the port number in the **Port** field. The default Mail Server port number is 25.
 - Specify a valid e-mail address in the **Sender** field. This e-mail address will be displayed in the mail generated from the software.
 - Specify a valid e-mail address in the **Recipients** field. This e-mail address is that of the recipient that will receive an e-mail message indicating that the restore operation has completed.
9. If only restoring the CommServe database, click **OK** to perform the restore.

The **CommserveDisasterRecoveryGUI** dialog box will display the restore event information logged in the bottom windowpane. This will include the restore operations for:

 - CommServe

If restoring the CommServe to another computer with a different name and IP address, go to Change the Name of the CommServe. If it is not necessary to change the name of the CommServe (and activate the license), go to Perform Post-Recovery Operations. If restoring SRM components, continue with the next step.

CHANGE THE NAME OF THE COMMSERVE (NAME/LICENSE CHANGE TAB)

This section is only applicable when restoring the CommServe to another computer with a different name and IP address.

10. Select the Name/License Change tab, and select the **CommServe Name Change** option. The system automatically displays the old and new names of the computer.

Continue with the next step.

ACTIVATE THE LICENSE (NAME/LICENSE CHANGE TAB)

This section is only applicable when restoring the CommServe to another computer with a different name and IP address.

11. From the Name/License Change tab, select the **Activate License** option, and then browse and select the appropriate license file.
12. Click **OK** to execute the restore operations.

The **CommserveDisasterRecoveryGUI** dialog box will display the restore event information logged in the bottom windowpane. This will include the restore operations for the:

 - CommServe
 - CommNet Server Database (if applicable)
 - SRM Server Database (if applicable)

PERFORM POST-RECOVERY OPERATIONS (POST RECOVERY TAB)

13. Select the Post Recovery tab, and select the one or more of the following options:
 - To mark your tapes exported after the recovery, click **Mark all tapes exported**.
 - To set a new email server for the new CommCell, click **Set new e-mail server**, and enter the email server. If you do not want to use an email server, click the option, then set the field to null.
 - To set a new email address for all CommCell users to use for the new CommCell, click **Change all user email address to**, and enter the new email address.
 - If you wish to disable the MediaAgent, click **Disable MediaAgent**.
 - To reset the index cache timestamps, click **Reset index cache timestamps**. This will reset all index cache timestamps, enabling the CommServe Disaster Recovery Tool to verify if an index cache label (ICL) file exists, and if not, automatically create one.
 - To use the same exact index when restoring the Disaster Recovery Backup data, click **Enable exact index restore**.
 - To update the CommServe database with the proper installation information, which will prevent conflicts with automatic updates and scheduling, click **Update Windows Version for CommServe**.
 - To disable all the scheduled tasks in the CommServe, click **Disable Schedules**.
 - Click **Disable Update Caches** so that all clients designated as update cache computers will no longer distribute update(s) to their associated clients. If configured for automatic updates, clients will receive their updates from the CommServe Update Cache.
 - To reset all update information for the CommServe Update Cache, click **Reset Update Info for CommServe**. This will remove leftover update and service pack information from the source database for the CommServe Update Cache, resetting the status of the baseline.
 - To reset the CommServe Cache location to the default location, click **Reset CommServe Cache Location to Default**. This will remove any specific path information added for the cache location, and revert to the default path directory.
 - After performing the CommServe database restore, the current deduplication store must be sealed. Select **Seal Dedupe Stores** check box to seal the deduplication store.

This will prevent any synchronization issues between deduplication database and CommServe database.
 - To create database objects in the CommServe database, click **Create CLR Functions**. This will re-create common language runtime (CLR) functions after the CommServe database is recovered.
 - To disable all activities at the CommCell level, click **Disable All Activity**.
 - To suspend all the jobs running in the CommServe, click **Suspend Running Jobs**.

14. Click **OK** to execute the post-recovery operations.

The **CommserveDisasterRecoveryGUI** dialog box will display the restore event information logged in the bottom windowpane. This will include the restore operations for the:

- Post-Recovery

15. If restoring CommNet or SRM Server Databases, skip this step.

Open the **Service Control Manager** on the CommServe computer and start the services.

To migrate to or from a clustered environment:

PERFORM CLUSTER MIGRATION

This section is only applicable when restoring the CommServe from or to a clustered environment.

1. From the Cluster/Non-Cluster CommServe DB Migration tab, select the Cluster/Non-Cluster CommServe DB Migration checkbox.
2. If restoring from a clustered environment to a non-clustered environment, select **Setup CommServe DB To Non-Cluster**.
3. If restoring from a non-clustered environment to a clustered environment, select **Setup CommServ DB To Cluster**. And then specify the names of the computers/nodes in the cluster.
4. Click **OK** to execute the cluster/non-cluster migration operations.

Data Encryption

[Topics](#) | [How To](#) | [Support](#) | [FAQ](#) | [Related Topics](#)

[Overview](#)

[FIPS Certification](#)

[Auxiliary Copy Operations and Encryption](#)

[Replication Encryption](#)

[Disable Encryption](#)

[Change Encryption Settings](#)

[Important Considerations](#)

[Verify Encryption](#)

[License Requirement](#)

OVERVIEW

The software allows encrypting data both for transmission over non-secure networks and for storage on media. The flexibility of key management schemes makes data encryption useful in a wide variety of configurations.

Encryption can be specified at three levels: client level (for backup), auxiliary copy level and hardware level. Client level encryption allows users to protect data prior to it leaving the computer. The data encryption keys are randomly generated per archive file. Additionally, they can be protected with a pass-phrase, which would be required for restoring the data. Auxiliary Copy level encryption encrypts data during auxiliary copy operations enabling backup operations to run at full speed. Here, data encryption keys are generated per storage policy copy of the archive file. Thus, if there are multiple copies in a storage policy, the same archive files in each copy gets a different encryption key. Individual archive files, however, will have different encryption keys. Note that the data encryption keys cannot be protected with a pass-phrase during auxiliary copy-level encryption. Hardware Encryption allows you to encrypt media used in drives with built-in encryption capabilities, which provides considerably faster performance than data or auxiliary copy encryption. The data encryption keys are generated per chunk on the media. Each chunk will have a different encryption key.

Data is encrypted according to the method you select when you Configure the Client for Data Encryption (client-level encryption) or Configure a Storage Policy Copy for Data Encryption (auxiliary copy-level encryption). You can select from several algorithms and key lengths, which are listed in the following table.

Data Encryption Algorithms

Cipher	Details	Block Size	Performance Rating*	Key Length Options
Blowfish	<ul style="list-style-type: none"> • Symmetric Key Block Cipher • Fast (fastest of the ciphers supported) • Secure • Finalist in the Advanced Encryption Standard Content 	64 bits	10	128, 256 bits
AES (Advanced Encryption Standard) or Rijndael	<ul style="list-style-type: none"> • Symmetric Key Block Cipher • Fast • Secure • Winner of the Advanced Encryption Standard Content • Adopted as the Government Standard (Only cipher approved by the National Security Agency to be used for top secret information.) 	128 bits	7	128, 256 bits
Serpent	<ul style="list-style-type: none"> • Symmetric Key Block Cipher • Fast • Very Secure (Considered more secure than AES) • Finalist in the Advanced Encryption Standard Content 	128 bits	8	128, 256 bits
Twofish	<ul style="list-style-type: none"> • Symmetric Key Block Cipher • Secure • Not standardized • Finalist in the Advanced Encryption Standard Content 	128 bits	4	128, 256 bits
3-DES (Triple Data Encryption Standard)	<ul style="list-style-type: none"> • Symmetric Key Block Cipher • Slow • May be susceptible to certain attacks 	64 bits	1.5	192 bits

*This performance rating is based on performance tests for the number of megabytes encrypted per second in a Windows environment with the CommServe software. The rating is on a scale of 1-10, 10 being the fastest. Results may vary depending on testing environment.

If you need network security only, configure encryption at the client level and select **Network Only**. The encryption keys are randomly chosen for every session. Data is encrypted on the Client and is decrypted on the MediaAgent and the keys are discarded at the end. The entire process is completely transparent. All you have to do is to enable encryption, and select the cipher and key length.

If you are concerned that media may be misplaced, data can be encrypted before writing it to the media and store the keys in the CommServe database. In this way, recovery of the data without the CommServe is impossible - not even with Media Explorer. This mode is also completely transparent. Once enabled, it will work requiring no additional activity on your part.

Additionally, encryption keys can be protected with your own pass-phrase before being stored in the database. If the database is accessed by unauthorized users, and the media is stolen, the data will still not be recoverable without the pass-phrase. This highest level of security comes at the price of having to enter the pass-phrase for every recovery operation and not being able to run synthetic full backups. But even this mode can further be customized to fit specific needs:

- By exporting a file that contains the scrambled pass-phrase of the client computer to a dedicated directory on another computer, the system can recover the client's data to that (and only that) computer without prompting you for the pass-phrase.
- Explicitly enabling synthetic full backups in the GUI will create a copy of unlocked encryption keys in the database, which will be accessible only to synthetic full data protection operations. In this case the regular data recovery operations will still prompt you for a pass-phrase, but synthetic full data protection operations will not.

FIPS CERTIFICATION

The Crypto Library module supports data encryption methods approved by the Federal Information Processing Standard (FIPS) as well as additional data encryption methods not approved by FIPS. To verify the method that the software is using, see Verify Data Encryption Method.

The National Institute of Standards and Technology has CommVault's certification under the list of Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules that have been tested using the cryptographic module validation program (CMVP).

AUXILIARY COPY OPERATIONS AND ENCRYPTION

Auxiliary copy operations can be configured for encryption when configuring a storage policy copy. This capability is useful in several scenarios:

- You are sending media to an off-site location and want to ensure the data on that media is not readable should the media be lost or stolen.
- You are performing a data protection operation to a disk library and wish to copy that data to a tape in encrypted form, but do not want to consume the time and resources required to encrypt the data during the data protection operation.
- You are protecting data from multiple organizations and want to ensure one organization cannot read the data from another.
- You wish to encrypt a portion of the source copy for off-site or long-term storage. For example, if you create a selective copy with a certain set of criteria established, the auxiliary copy encryption process will encrypt only the data satisfying that criteria.

When enabled, auxiliary copy encryption will encrypt any portion of the data that has not already been encrypted during a data protection operation. If any data on the source copy is already encrypted, the software will retain that data's existing encryption, unless configured to re-encrypt the data using a different data encryption algorithm.

The following table illustrates the data encrypted with auxiliary copy encryption:

The Storage Policy is:	Auxiliary Copy Encryption will:
Not encrypted	Encrypt all data.
Partially encrypted	Encrypt only the data that has not already been encrypted.
Fully encrypted	Retain existing encryption, unless configured to use a different algorithm.

All encryption keys are supported for auxiliary copy encryption and are created on an individual basis for each data protection operation. Refer to Data Encryption for more information on encryption keys.

In some cases, other encryption methods may be preferable to auxiliary copy encryption, such as:

- You are protecting data over an unsecured network (such as a Wide Area Network) and want to ensure the data is not readable while passing through the network. In this scenario, you can encrypt data at the client level.
- You wish to protect encryption keys with a pass-phrase. In this scenario, you can encrypt data at the client level..
- You have libraries or drives with built-in encryption capabilities and wish to encrypt the media used in those drives. In this scenario, you can encrypt data at the client level using Hardware Encryption. Note that hardware encryption provides considerably faster performance than data or auxiliary copy encryption.

CONFIGURING STORAGE POLICIES FOR AUXILIARY COPY ENCRYPTION

You can configure data encryption for an auxiliary copy operation by selecting the **Encrypt Data** option from the appropriate storage policy copy's **Properties** dialog box. The data will then be encrypted once the auxiliary copy process is initiated for that storage policy.

RE-ENCRYPTION DURING AUXILIARY COPY

During an auxiliary copy operation of encrypted data, you can also configure the copy to decrypt and re-encrypt the data. A different data encryption algorithm can be used when the data is re-encrypted. This is useful if data is compromised, company policy dictates it, data will be retained longer, thereby requiring a stronger encryption algorithm (more bits), or, on the contrary, the data will be retained for a shorter amount of time, thereby requiring a smaller algorithm (less bits).

For step-by-step instructions on configuring a storage policy for data encryption and starting the auxiliary copy, see the following:

- Configure a Storage Policy Copy for Data Encryption
- Start an Auxiliary Copy

RELATED REPORTS

The Auxiliary Copy Job Summary Report and Jobs in Storage Policy Copies Report will display the data that has been encrypted.

LICENSING

An Auxiliary Copy License is required for each MediaAgent.

REPLICATION ENCRYPTION

Data being replicated can be encrypted between the source and destination computers.

When encryption is enabled, data is encrypted on the source computer, replicated across the network to the destination computer, and decrypted on the destination computer. Encryption for replication is specified on the Replication Set level, and applies to all of its Replication Pairs. For a given Replication Set, you can enable or disable encryption between the source and destination machines. See [Configure the Replication Set for Data Encryption](#) for step-by-step instructions.

For data encryption during a copyback/restore operation, you have to enable encryption on the computer which initiates the copyback/restore operation, in addition to enabling the encryption for a replication set. See [Configure the Replication Set for Data Encryption](#) for step-by-step instructions.

CDR on UNIX only supports the Blowfish cipher, and only a 128-bit key length.

DISABLE ENCRYPTION

Once you have enabled encryption functionality at the client level, there are different approaches to backing out of the functionality. You need to be aware of the behaviors that result from each approach. Refer to [Change Encryption Settings](#).

If an exported pass-phrase was not synchronized with the last source client's pass-phrase at the time encryption was disabled (setting change from **With a Pass-Phrase** directly to **Disabled**), subsequent recovery operations may present an erroneous message "Invalid pass-phrase specified. Please check the spelling and try again". If the data you are recovering was not encrypted, this message can be ignored as the recovery will run successfully. If the data was encrypted with pass-phrase protection, you will need to provide the correct (last) source client's pass-phrase.

When you disable encryption after having exported a pass-phrase, the exported file is not deleted. To remove the file, locate the `<hostname>.pf` file in the `<software installation path>\PF` folder that is named for the source client.

- Do not delete the exported synched pass-phrase file when a Migration Archiver Agent is present on the client computer. If a migration archiving operation was done using encryption and the key is deleted, stub recoveries will not be possible. At that point, your remaining option would be to perform a browse/recovery and provide the correct Decryption key.
- Exchange data that has been archived with pass-phrase encryption cannot be recovered from Outlook or OWA, but can be recovered by performing a Browse and Recovery operation from the CommCell Console.

CHANGE ENCRYPTION SETTINGS

If you set up the following client and subclient encryption settings and never change them, the following chart indicates when a pass-phrase is required at recovery time:

	Subclient Encryption Settings			
Client Settings:	None	MediaAgent	Network and MediaAgent	Network
Restore Access		Only		Only

Disabled	N/A	N/A (except as noted) ^{1, 4, 5}	N/A (except as noted) ^{1, 4, 5}	N/A
Regular	N/A	Recoverable without pass-phrase ²	Recoverable without pass-phrase ²	Recoverable without pass-phrase
With a Pass-Phrase (exported to a client)	N/A	Recoverable without pass-phrase ³ (only to a client to which the pass-phrase has been exported)	Recoverable without pass-phrase ³ (only to a client to which the pass-phrase has been exported)	Recoverable without pass-phrase
With a Pass-Phrase (not exported to a client)	N/A	Pass-Phrase REQUIRED	Pass-Phrase REQUIRED	Recoverable without pass-phrase

Auxiliary copy operations support data encryption and can be configured when you Configure a Storage Policy Copy for Data Encryption. When storage policy copies are enabled for data encryption, the encryption takes place after the data protection operation during the auxiliary copy. If you do not configure the storage policy copy for data encryption, then when you run an auxiliary copy operation, the copy assumes the settings of the primary copy, which are set when you Configure the Client for Data Encryption. Therefore, if the primary copy data is encrypted, then the auxiliary copy data will be encrypted; and if the primary copy data is not encrypted, then the auxiliary copy data will not be encrypted.

Changing the client **Restore Access** settings, resetting a pass-phrase or changing export settings effects encryption behaviors as follow:

- At the time you change client properties from Restore Access **With a Pass-Phrase** directly to **Disabled** at the client level, the last pass-phrase is retained. When you run a recovery operation on those past backups 1) you will still have to enter the most recent pass-phrase, and 2) as long as the current pass-phrase had been exported, scheduled data recoveries for those past backups will run successfully. Subsequent data protection operations run after having disabled encryption and data recovery operations run on those subsequent data protection operations will not evidence any encryption behaviors. (SEE ALSO Notes ⁴ and ⁵ .)
- When you change client properties from Restore Access **With a Pass-Phrase** to **Regular** at the client level, at that time you are required to enter the current pass-phrase. By entering the correct pass-phrase, all keys are unlocked. This means for any past or subsequent data protection operations you will 1) no longer be required to enter the pass-phrase during a data recovery operation, and 2) scheduled data recovery operations will run successfully without having to export a pass-phrase.
 - Do not delete the exported pass-phrase file when a Migration Archiver Agent is present on the client computer. If a migration archiving operation was done using encryption and the key is deleted, stub recoveries will not be possible. At that point, your remaining option would be to perform a browse/recovery and provide the correct Decryption key.
 - Exchange data that has been archived with pass-phrase encryption cannot be recovered from Outlook or OWA, but can be recovered by performing a Browse and Recovery operation from the CommCell Console.
- When you **Reset** a client's pass-phrase, if you are in the practice of exporting pass-phrases, a recommended Best Practice is to **Export** immediately to keep the current and exported pass-phrases synchronized. Although it is possible when performing an immediate data recovery operation to override an out-of-date exported pass-phrase by entering the new pass-phrase, scheduled data recovery operations only utilize the exported pass-phrase. If the exported pass-phrase is not current, scheduled data recoveries will not complete successfully.
- At the time you change client properties from Restore Access **With a Pass-Phrase** directly to **Disabled** at the client level, the last pass-phrase is retained. Therefore, if you run an **Auxiliary Copy** operation at this point, for all backups that get copied in the Auxiliary Copy operation.
- When you change client properties from Restore Access **With a Pass-Phrase** to **Regular** and then to **Disabled** at the client level, and then run an **Auxiliary Copy** operation, for all backups that get copied in the Auxiliary Copy operation.

IMPORTANT CONSIDERATIONS

Keep the following in mind when encrypting data:

- Since encrypting data converts it into a random form, it becomes less compressible than non-encrypted data. It is therefore recommended that you do not enable hardware compression on encrypted data, as doing so may actually make the data grow in size.
- The backup throughput for encrypted data will be lower when compared to non-encrypted data. Enabling Client Compression may provide a higher throughput for encrypted data which is not already compressed. Note that alternatively, the Auxiliary Copy Encryption feature, which encrypts the data during auxiliary copy operations, allows backups to run at full speed.
- Exchange data that has been archived with pass-phrase encryption cannot be recovered from Outlook or OWA, but can be recovered by performing a Browse and Recovery operation from the CommCell Console.
- If an archive operation is performed without encryption for File Archiver Agents, and then encryption is enabled, in order to recover the data, enter the current pass-phrase in the CommCell Console (for browse recoveries), or export the pass-phrase to the client computer (for stub recoveries).
- While configuring the Windows File System backup sets, if you are using **Data Classification** as the scan method, you may face the following data encryption issue: When the data is restored, a non-encrypted file, in an encrypted folder, becomes encrypted. This issue does not occur if you use the **Change Journal** or **Classic Scan** as the scan method during the backup.
- Auxiliary Copy Encryption**
 - When configuring a Primary Copy and Secondary Copy with deduplication, the pass phrase option is not supported. For more information, see Deduplication.

- Auxiliary copy encryption is not supported for NetWare MediaAgents. If you wish to encrypt NetWare data with auxiliary copy encryption, you must use a Windows or Unix-based MediaAgent.
- Auxiliary copy encryption is supported for NDMP Remote Server data; however, it is not supported for NAS File Server data.
- If the CommServe and MediaAgent have been upgraded to the current release level but the client has not, any restored secondary copy data that was encrypted during an auxiliary copy operation will not be supported until the client is upgraded to the current release level.
- If you are creating a secondary copy from an encrypted, deduplicated source copy, the software automatically decrypts the deduplicated data during the creation of the secondary copy. Thus, if you wish to create a fully encrypted secondary copy of data from an encrypted, deduplicated source copy, ensure that the secondary copy is configured for re-encryption. Otherwise, the deduplicated portion of the data will remain decrypted. See Deduplication for more information.
- An inline copy enables users to create additional copies of data at the time of data protection operations, therefore, it will assume the encryption settings of the subclient for which the copy is being made. Note that if a data protection operation of a subclient whose storage policy has an inline copy enabled does not successfully create the Inline Copy, that data will be copied to a secondary copy the next time an auxiliary copy is run, and will be encrypted at that time. For more information see Inline Copies.
- If the CommServe and MediaAgent are upgraded to the current release, but the Client is not upgraded, the restored data from a secondary copy containing encrypted backups enabled using the auxiliary copy operation will not be supported until the Client is upgraded to the current release.

VERIFY ENCRYPTION

To verify the software and hardware encryption, create the following reports: Job Summary Report and Jobs in Storage Policy Copies Report. The reports will display the data that has been encrypted.

LICENSE REQUIREMENT

This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

[Back to Top](#)

Data Encryption - How To

[Topics](#) | [How To](#) | [Support](#) | [FAQ](#) | [Related Topics](#)

[Configure the Client for Data Encryption](#)

[Configure the Instance for Third-party Command Line Encrypted Operations](#)

[Configure the Replication Set for Data Encryption](#)

[Configure the Subclient for Data Encryption](#)

[Export an Encryption Pass-Phrase](#)

[Recover Encrypted Data \(Regular\)](#)

[Recover Encrypted Data \(With a Pass-Phrase\)](#)

[Configure a Storage Policy Copy for Data Encryption](#)

[Verify Data Encryption Method](#)

CONFIGURE THE CLIENT FOR DATA ENCRYPTION

To encrypt data during data protection and recovery operations using the CommCell Console, you must configure encryption at the client level first and then at the subclient level.

To encrypt data during third-party Command Line operations, you must configure encryption at the client level first and then at the instance level.

See [Data Encryption - Support](#) for a list of supported products.

Before You Begin

This procedure configures data encryption for all supported agents that reside on this client, however, no content at any level (instance or subclient) will be

encrypted until the respective level's encryption property is enabled.

Required Capability: Capabilities and Permitted Actions

▶ To configure the client for data encryption:

1. From the CommCell Console, right-click the Client and click **Properties**.
2. From the client's Client Properties (Encryption) tab, select the **Encrypt Data** check box to enable options.
3. Select options based on the criteria described in the Encryption tab help.
4. Configure data encryption for Restore Access and Direct Media Access.

If you configure data encryption with **With a Pass-Phrase** and do not elect to export the pass-phrase to destination clients:

- You will be required to enter the pass-phrase during immediate data recovery operations.
- You will not be able to run scheduled data recovery operations.

If you do not require this level of security, consider using **Regular** encryption instead or Export an Encryption Pass-Phrase. The following requires you to export the pass-phrase:

- Scheduled data recovery operations
- Stub data recovery operations (initiated from Migration Archiver Agents)
- Third-party Command Line data recovery operations

Note, if you selected pass-phrase security you must enter a pass-phrase in the dialog box that appears.

5. Click **OK** to save your settings and close client properties.

CONFIGURE THIRD-PARTY COMMAND LINE OPERATIONS FOR ENCRYPTION

Encryption settings made at the instance level for third-party Command Line operations are not related in any way to settings made at the subclient level. Subclient encryption settings are only for data protection and recovery operations run from the CommCell Console.

See Data Encryption - Support for a list of supported products.

Before You Begin

Encryption must be enabled at the client level prior to configuring any instances residing on that client. See Configure the Client for Data Encryption.

Required Capability: Capabilities and Permitted Actions

▶ To configure the instance for encryption of third-party command line operations:

1. From the CommCell Console, right-click the instance and click **Properties**.
2. From the respective Encryption tab, select an option based on the criteria described in the Encryption tab help.
3. Click **OK** to save your settings and close the properties dialog box.

For third-party Command Line data recovery operations to succeed when using pass-phrase security, you must export the pass-phrase to the destination client.

CONFIGURE THE REPLICATION SET FOR DATA ENCRYPTION

Before You Begin

- Encryption settings made at the Replication Set level are for encryption of data between the source machine and the destination machine.
- Encryption must be enabled at the client level prior to configuring data encryption for a Replication Set residing on that client. See Configure the Client for Data Encryption.

Required Capability: Capabilities and Permitted Actions

▶ To configure data encryption for a Replication Set:

1. From the CommCell Browser, right-click the Replication Set and select **Properties**.
2. From the Replication Set Properties (Replication Options) tab, either select or clear **Encrypt During Data Transfer**.
3. Click **OK** to save your settings and close the Replication Set Properties.

CONFIGURE THE SUBCLIENT FOR DATA ENCRYPTION

Encryption settings made at the subclient level are for data protection and recovery operations run from the CommCell Console and are not related in any way to settings made at the instance level which is for third-party Command Line operations only.

See Data Encryption - Support for a list of supported products.

Before You Begin

- Encryption must be enabled at the client level prior to configuring any subclients residing on that client. See Configure the Client for Data Encryption.
- If you are attempting to configure for third-party Command Line operations, do not use this procedure. See Configure Third-party Command Line Operations for Encryption.

Required Capability: Capabilities and Permitted Actions

▶ To configure the subclient for data encryption:

1. From the CommCell Console, right-click the subclient and click **Properties**.
2. From the Subclient Properties (Encryption) tab, select an option based on the criteria described in the Encryption tab help.
3. Click **OK** to save your settings and close subclient properties.

EXPORT AN ENCRYPTION PASS-PHRASE

For a scheduled data recovery operation of encrypted data to run successfully when the client encryption Restore Access property is set to **With a Pass-Phrase**, prior to the start of the scheduled recovery you must have exported the file that contains the scrambled pass-phrase to the destination client(s). This <hostname>.pf file is copied to the <software installation path>\PF folders and is named for the source client. Should you disable encryption at some point, either from the client or subclient level, know that these exported files are not deleted. Refer to Disable Encryption.

Although not mandatory, exporting the pass-phrase will also facilitate immediate data recoveries, bypassing the need to enter the pass-phrase for each recovery operation.

When using pass-phrase security for:

- **Migration Archiver Agents** - you must export the pass-phrase to the destination client before you can run a Stub data recovery. However, Exchange data that has been archived with pass-phrase encryption cannot be recovered from Outlook or OWA, but can be recovered by performing a Browse and Recovery operation from the CommCell Console.
- **Image Level and Image Level ProxyHost iDataAgents** - you must export the pass-phrase to the MediaAgent as well as the destination client, since a portion of the volume information is restored to the MediaAgent Index Cache. When using Alternate Data Paths (GridStor), this would apply to any MediaAgent involved in the restore.
- **Third-party Command Line operations** - you must export the pass-phrase to the destination client.

Before You Begin

- Normal configurations for this procedure are:
 - Client encryption properties - restore access is set to **With a Pass-Phrase**.
 - Client encryption properties - a pass-phrase has already been set.
 - Instance properties (for third-party Command Line operations) - any setting.
 - Subclient encryption properties - any setting.
- If you have changed encryption settings, refer to Change Encryption Settings for alternate configurations.

Required Capability: Capabilities and Permitted Actions

▶ To export an encryption pass-phrase to a client:

1. From the CommCell Console, right-click the Client and click **Properties**.
2. From the Client Computer Properties (Encryption) tab, click the **Export** button.
3. In the Export Pass-Phrase dialog box, select a **Destination Computer**.
4. Enter the pass-phrase as directed.
5. Click **Export** to copy the file with the pass-phrase to the selected client, and then close the dialog box.

Once you have configured the client and desired agent(s) and exported the pass-phrase, you are ready to run immediate and scheduled data recovery operations from the CommCell Console or immediate third-party Command Line operations.

RECOVER ENCRYPTED DATA (REGULAR)

Data Recovery Operations from the CommCell Console

When the client encryption properties Restore Access is set to **Regular**, recovery of encrypted data run from the CommCell Console is transparent, meaning, the Advanced Restore Options **Encryption** tab is not utilized.

Before you Begin

- Normal source client configurations for this procedure are:
 - Client encryption properties - Restore Access is set to **Regular** at the time of the data recovery operation.
 - Subclient encryption properties - Any setting.
- If you have changed encryption settings, refer to Change Encryption Settings for alternate configurations.
- This procedure also pertains to recovering data on media encrypted during auxiliary copy operations.

Required Capability: Capabilities and Permitted Actions

▶ To recover encrypted data when the source client's Restore Access is set to **Regular**:

1. From the CommCell Console, begin any immediate or scheduled data recovery procedure.
2. When you reach the **Restore Options** dialog box, do not use the **Encryption** tab (by clicking **Advanced** and then **Encryption**).
3. Continue your data recovery procedure as usual.

Third-party Command Line Recovery Operations

When the client encryption properties Restore Access is set to **Regular**, third-party Command Line recovery of encrypted data is transparent.

Before you Begin

- Normal source client configurations for this procedure are:
 - Client encryption properties - Restore Access is set to **Regular** at the time of the data recovery operation.
 - Instance encryption properties - Any setting.
- If you have changed encryption settings, refer to Change Encryption Settings for alternate configurations.

RECOVER ENCRYPTED DATA (WITH A PASS-PHRASE)

Data Recovery Operations from the CommCell Console

Before You Begin

- Normal source client configurations for this procedure are:
 - Client encryption properties - Restore Access of the source client must be set to **With a Pass-Phrase** at the time of the recovery operation.
 - Subclient encryption properties - **MediaAgent Only** or **Network and MediaAgent** at the time of the recovery operation.
- If you have changed encryption settings, refer to Change Encryption Settings for alternate configurations.
- For a scheduled recovery operation in these configurations to run successfully, prior to the start of the operation you must have exported the current pass-phrase to the destination client using the Client Properties Encryption tab. See Export an Encryption Pass-Phrase.

Required Capability: Capabilities and Permitted Actions

- If data is being recovered to the same destination as the original data protection operation:

Browse and In Place Recovery with at least subclient level association at the source client.

- If data is being recovered to a different destination than the original data protection operation:

- Browse and Out of Place Recovery with at least backup set/instance association at the source client, and
- Browse and In Place Recovery with at least agent level association at the destination client.

If the destination client is on a different platform than the source client (for example, a Unix File System client and a Windows File System client), then Browse and In Place Recovery with at least client level association at the destination client is needed.

- If recovering encrypted data that was encrypted during auxiliary copy operations, a pass-phrase will not be required regardless of the client's Restore Access settings.

▶ To recover encrypted data when the source client's Restore Access is set to **With a Pass-Phrase**:

1. From the CommCell Console, begin any immediate or scheduled data recovery procedure.
2. When you reach the **Restore Options** dialog box:
 - If the source client's current pass-phrase has been exported to the destination client, do not use the **Encryption** tab (by clicking **Advanced** and then the **Encryption** tab).

- If the data you are recovering belongs to a client for which you have not exported its pass-phrase to the destination client, or the exported pass-phrase is not synchronized with the current pass-phrase, click **Advanced** and then the Encryption tab from the Advanced Restore Options dialog box. In the spaces provided in this tab, enter the pass-phrase that is currently assigned to the client and click **OK**.
3. Continue your data recovery procedure as usual.

Third-party Command Line Recovery Operations

When the source client encryption properties option **Restore Access** is set to **With a Pass-Phrase**, you are required to Export the Encryption Pass-Phrase in order to perform immediate data recovery operations via a third-party Command Line.

Before You Begin

- Normal source client configurations for this procedure are:
 - Client encryption properties - Restore Access is set to **Regular** at the time of the data recovery operation.
 - Instance encryption properties - Any setting.
 - If you have changed encryption settings, refer to Change Encryption Settings for alternate configurations.
-

CONFIGURE A STORAGE POLICY COPY FOR DATA ENCRYPTION

Required Capability: See Capabilities and Permitted Actions

▶ To configure a storage policy copy for data encryption:

1. From the right pane of the CommCell Browser, right-click a secondary storage policy copy, and then click **Properties**. Note that you cannot configure a primary storage policy copy for data encryption.
 2. From the Advanced tab of the **Copy Properties** dialog box, click the **Encrypt Data** check box to enable options.
 3. Select options based on the criteria described in the **Advanced** tab help.
 4. Click **OK** to save your settings
-

VERIFY DATA ENCRYPTION METHOD

Required Capability: Capabilities and Permitted Actions

▶ To verify the encryption method:

1. From the CommCell Browser, right-click on the CommCell, and select **Properties** from the popup menu.
 2. Select the Version tab, and check that the **Crypto Library Version** is 1.0.
 3. Click **OK** to close this window.
 4. From the CommCell Browser, right click on a client, and select **Properties** from the popup menu.
 5. Select the Encryption tab.
 6. Verify that the **Encrypt Data** option is enabled, and that the **Data Encryption Algorithm Cipher** is set to an algorithm that suits your environment:
 - **AES** or **3-DES** (approved by FIPS).
 - **Blowfish**, **Serpent** or **Twofish** (not approved by FIPS).
 7. Click **OK** to close this window.
-

[Back to Top](#)

Operation Window

Topics | How To | Support | Related Topics

Overview

Operation Rules

- Defining Operation Rules
- Bypassing Other Operation Rules at Higher Levels
- Bypassing Time Windows

Things to Consider

Audit Trail

OVERVIEW

By default, all operations in the CommCell will run for 24 hours without restriction. However, it may be necessary to prevent operations from running during certain time periods of the day. To accomplish this, you can define operation rules which will disable certain operations from running during a time period you specify, thereby ensuring unexpected, time consuming operations do not disrupt the availability of network bandwidth, data, or storage resources when they are most needed.

When operation rules are configured, operations that are started within the time window specified will go to a queued (as opposed to pending) state.



However, for the SAP for Oracle and SAP for MAXDB *iDataAgents*, operations that are started within the time window specified will go to a running state.

Once the time window specified in the operation rule has elapsed, these queued or running operations will resume automatically.

OPERATION RULES

Operation rules can be defined using the **Operation Window** at the following levels in the CommCell Browser:

- CommServe
- Client Computer Group
- Client
- Agent
- Backup Set
- Subclient

The Operation Window is accessible from the CommCell Console Control Panel. For information on the operation rules available at each level, see Operation Window - Support.

Operation rules established at the CommServe level apply across the entire CommServe. Operation rules established at the Agent level apply only to the specified Agent. When an operation rule is defined at both the CommServe and Agent levels, the operation will run outside of the total time frame established by the operation rules configured at both levels.

DEFINING OPERATION RULES

When adding a new operation rule, you are given the opportunity to select the particular operation(s) you wish to include in the **Operation Rule Details** dialog box, which is launched when clicking the **Add**, **Modify**, or **Delete** buttons. You can also select the specific days and times the operation rule is to take effect. Once created, the operation rule will be displayed in the **Operation Window**, as well as the total number of operation rules that are currently configured.

For example, if users in your environment tend to use their Lotus Notes applications between the hours of 8:00AM and 6:00PM Monday through Friday, you can configure an operation rule at the Lotus Notes Document *iDataAgent* level that will not allow any Full or Non Full Data Protection operations to run during that time. This operation rule will ensure that their Lotus Notes data is freely accessible without any delays or interruptions.

See the following procedures for step-by-step instructions:

- Add an Operation Rule
- Modify an Operation Rule
- Delete an Operation Rule

BYPASSING OTHER OPERATION RULES AT HIGHER LEVELS

If you are creating an operation rule at a level other than the CommServe or Client Computer Group levels, you can choose to bypass any operation rules configured at a higher level than that of the given operation rule by selecting the **Ignore Operation Window Rules at Higher Levels** option in the **Operation Window**.

For example, if you are configuring an operation rule for a particular backup set, but do not want any operation rules configured at levels higher than the backup set to run concurrently, then selecting this option will ensure only the operation rule associated with the backup set and its accompanying subclient will run.

See [Bypass Other Operation Rules at Higher Levels](#) for step-by-step instructions.

BYPASSING TIME WINDOWS

In some cases, an operation launched prior to the time window of an operation rule may require the ability to run uninterrupted until completion. In such cases, you can enable the **Allow running jobs to complete past the operation window** option in the General tab of the Job Management dialog box. When selected, the running operation will ignore the operation rule and continue until completion.

See [Bypass Time Windows](#) for step-by-step instructions.

THINGS TO CONSIDER

Consider the following when configuring operation rules:

- Certain operations (such as database jobs, administrative tasks, and synthetic full backups) cannot be assigned to operation rules. For many of these operations, the **Job Preemption Control** feature can be used instead. See [Job Preemption Control](#) for more information.
- If a restartable operation has not finished when the window of time specified in the operation rule has started, the operation will be queued and restarted at the point from which it was suspended.
- If a non-restartable operation does not finish before an operation rule starts, the operation will continue and run uninterrupted to completion. Jobs from the following SRM Agents and SRM Report Jobs are not restartable:
 - Unix
 - Oracle
 - SQL
 - NetWare
- If the time zone of a Client is different than that of CommServe, then the time zone of the client is honored. However, if the operation rule is set at the CommServe level, the time zone of the client is not honored.
- If a preemptible operation begins within the time window specified in the operation window but does not complete before the time window expires, the Job Manager will put this operation into a queued state. The operation will then be restarted at the next occurrence of the time window.

If a non-preemptible operation begins within its window of operation but does not complete before the time window expires, the Job Manager will let the job run uninterrupted to completion.

- For the following agents, the backup phase of a data protection operation cannot be interrupted by an operation rule:
 - DataArchiver Agents
 - DB2 *iDataAgent*
 - DB2 DPF *iDataAgent*
 - Exchange Database *iDataAgent*
 - Image Level *iDataAgent*
 - Informix *iDataAgent*
 - Lotus Notes Database *iDataAgent*
 - Oracle *iDataAgent*
 - Quick Recovery Agent
 - SAP for MAXDB *iDataAgent*
 - SAP for Oracle *iDataAgent*
 - SharePoint Server *iDataAgent*

Any data protection operations for these agents that do not complete before the operation rule starts will run uninterrupted to completion regardless of any operation rules configured.

AUDIT TRAIL

Operations performed with this feature are recorded in the Audit Trail. See Audit Trail for more information.

[Back to Top](#)

Operation Window - How To

[Topics](#) | [How To](#) | [Support](#) | [Related Topics](#)

[Add an Operation Rule](#)

[Modify an Operation Rule](#)

[Delete an Operation Rule](#)

[Bypass Other Operation Rules at Higher Levels](#)

[Bypass Time Windows](#)

ADD AN OPERATION RULE

Required Capability: See Capabilities and Permitted Actions

▶ To add an operation rule at the CommServe, Agent, or Subclient level:

1. In the CommCell Browser:
 - For the CommServe level, right-click the CommServe, click **Control Panel**, and then click **Operation Window**.
 - For all other levels, right-click the appropriate entity, click **All Tasks**, and then click **Operation Window**.
 2. From the Operation Window dialog box, click **Add**.
 3. From the Operation Rule Details dialog box:
 - Enter the name of the rule in the **Name** field.
 - Select either an administration, data protection (either full or non-full), and/or a data recovery operation from the **Operations** pane.
 - Select the day(s) of the week to exclude the operation from the **Days of week** pane.
 - From the **Do not run intervals** pane, click **Add** to add a date interval that will prevent the selected operation(s) from running.
 4. From the Time Intervals dialog box, select a start and end time to exclude the operation(s) from running, then click **Add**. Click **OK** if this is the last time interval to be added.
 5. Click **OK** to save the changes.
-

MODIFY AN OPERATION RULE

Required Capability: See Capabilities and Permitted Actions

▶ To modify an operation rule:

1. In the CommCell Browser:
 - For the CommServe level, right-click the CommServe, click **Control Panel**, and then click **Operation Window**.
 - For all other levels, right-click the appropriate entity, click **All Tasks**, and then click **Operation Window**.
 2. From the Operation Window dialog box, select the appropriate operation rule, then click **Modify**.
 3. From the Operation Rule Details dialog box, modify the options, as necessary.
 4. To modify a time interval, from the Do not run intervals pane, click **Modify** to add a time interval, or click **Add** to add a new one.
 5. From the Time Intervals dialog box, select a start and end time to exclude the operation(s) from running, then click **Add**. Click **OK** if this is the last time interval to be added.
 6. Click **OK** in the **Operation Window** dialog box to save the changes.
-

DELETE AN OPERATION RULE

Required Capability: See Capabilities and Permitted Actions

▶ To delete an operation rule:

1. In the CommCell Browser:
 - For the CommServe level, right-click the CommServe, click **Control Panel**, and then click **Operation Window**.
 - For all other levels, right-click the appropriate entity, click **All Tasks**, and then click **Operation Window**.
 2. From the Operation Window dialog box, select the appropriate operation rule, then click **Delete**.
 3. Click **OK** to confirm.
 4. Click **OK** in the **Operation Window** dialog box to save the changes.
-

BYPASS OTHER OPERATION RULES AT HIGHER LEVELS

Required Capability: See Capabilities and Permitted Actions

Before you Begin:

- Note that the option to ignore operation window rules at higher levels is not supported at the CommServe or Client Computer Group levels.

▶ To bypass operation rules at higher levels:

1. In the CommCell Browser:
 - From any level other than the CommServe or Client Computer Group levels, right-click the appropriate entity, click **All Tasks**, and then click **Operation Window**.
2. From the Operation Window dialog box, click the **Ignore Operation Window Rules at Higher Levels** check box.
3. Click **OK** to save your changes.

All operation window rules configured at levels above the entity you've selected will be ignored.

BYPASS TIME WINDOWS

Required Capability: See Capabilities and Permitted Actions

▶ To bypass time windows configured in an operation rule:

1. From the CommCell Browser, right-click the **CommCell** icon, click **Control Panel**, and then click **Job Management**.
 2. From the General tab of the Job Management dialog box, click the **Allow running jobs to complete past the operation window** check box.
 3. Click **OK** to save your changes.
-

[Back to Top](#)

Activity Control

Topics | How To | Support | Related Topics

Overview

CommCell Browser Icons and Activity Control

Activity Control for Workstation Backup Agents

Audit Trail

OVERVIEW

The Activity Control feature allows you to enable or disable operations including scheduled operations at the following levels in the CommCell hierarchy:

CommCell	Allows you to enable/disable all activity, data management, data recovery, auxiliary copy, data aging, deduplication database, and/or content indexing operations for all client computers within the CommCell.
Client Computer Groups	Allows you to enable/disable all data management and data recovery operations on all client computers that are members of a client computer group.
Client	Allows you to enable/disable all data management, and data recovery operations on a specific client computer.
Agent	Allows you to enable/disable the data protection and/or data recovery operations of a specific agent on a specific client computer. SRM Data Collection operations can be enabled/disabled for SRM Agents.
Subclient	Allows you to enable/disable the data protection of a specific subclient.

When disabling operations, the CommCell level has the highest precedence while a subclient has the lowest precedence. For example, if you disable data management operations at the CommCell level, then all data management operations throughout the CommCell are disabled regardless of the corresponding settings of the individual client computer groups, client computers, agents, and subclients. If, however, a data management operation is enabled at the CommCell level, you can still disable data management operations at the client computer groups, client computer, agent, subclient levels, if the option is available at that level. By default, all operations are enabled at all levels of the CommCell hierarchy.

If an operation is disabled at any level of the CommCell hierarchy, it can be re-enabled by specifying the date and time at which the operation activity will start on the specified level.

COMMCELL BROWSER ICONS AND ACTIVITY CONTROL

The icons associated with the CommServe and Clients in the CommCell Browser include information on the activity control options for data management and/or data recovery operation in that specific entity, i.e., CommServe or the Client. The icons have two arrows - out-bound to denote activity control for data protection operations and in-coming to denote activity control for data recovery operations. These arrows appear in green when the activity control is enabled, and in red when disabled.

The following table further illustrates how to interpret the arrows in these icons. Note that the icons may vary depending on the entity. For a comprehensive list of all icons in the CommCell Console, see CommCell Console Icons.

If the incoming arrow is:	And the outgoing arrow is:	Then the icon denotes:
green	green	a Client with both Data Protection and Data Recovery jobs enabled.
green	red	a Client with only Data Protection jobs disabled.
red	green	a Client with only Data Recovery jobs disabled.
red	red	a Client with both Data Protection and Data Recovery jobs disabled.

Note that the icons do not reflect the status of other activity control options that may be available in these entities.

ACTIVITY CONTROL FOR WORKSTATION BACKUP AGENTS

Activity Control for Workstation Backup Agents includes controlling the backup, recovery, scheduling, and content management capabilities of the Workstation Backup clients. In addition, the following operational controls are also available from the CommCell Console:

- Set the maximum number of successive backup failures after which the client is alerted.
- Set the minimum bandwidth required to execute a backup job.
- Control the size of the journal that tracks the changes to the source.

By default the changes made to the activity control settings from the CommCell Console will be reflected on the clients after 24 hours.

Activity Control can be set at the following levels:

1. **CommCell Console** - Allows you to enable/disable backup activity, content management, data recovery, and scheduling operations for all the Workstation Backup Agents in the CommCell. See [Enable \(or Disable\) Operations for Workstation Backup Agents \(CommCell Level\)](#) for instructions.
 2. **Client** (from CommCell Console) - Allows you to enable/disable backup activity, content management, data recovery, and scheduling operations for the individual client (when operations are enabled at the CommCell level.) See [Enable \(or Disable\) Operations for Workstation Backup Agents \(Client Level\)](#) for instructions.
 3. **Client** (from Client Console) - Allows you to enable/disable backup operations from the Client Console (when operations are enabled for this client, from the CommCell Console.) See [Enable \(or Disable\) Backup Operations from the Client Console](#) for instructions.
-

AUDIT TRAIL

Operations performed with this feature are recorded in the Audit Trail. See [Audit Trail](#) for more information.

[Back to Top](#)

Job Management

[Topics](#) | [How To](#) | [Support](#) | [Related Topics](#)

Overview

Viewing Job Information

- [Job Errors](#)
- [Flags](#)
- [Viewing Additional Job Details](#)

Controlling Jobs

- [Controlling the Number of Simultaneously Running Streams](#)

Viewing Job Status

- [Job Status for SAP for Oracle iDataAgent](#)
- [Job Status Changes](#)

Customizing Completed with Errors Condition

- [Supported Agents](#)
- [Creating Decision Rules](#)
- [Common Error Codes](#)

Job Filters

Important Considerations for Running Jobs

Preempting Jobs

- [Preemptible and Non-Preemptible Jobs](#)
- [Controlling Job Preemption for the CommCell](#)
- [Configuring Preemptibility for Select Job Types](#)
- [What happens when a job is Preempted](#)

Restarting Jobs

- [Restartable and Non-Restartable Jobs](#)
- [Configuring Job Restarts for the CommCell](#)
- [QR Volume Creation Restartability](#)

Retrying Jobs

Resuming Jobs

Resubmitting Jobs

Job Results Directory

- [Calculating the Space Required for the Job Results Directory](#)
- [Using UNC Paths for Job Results Directory](#)
- [User Impersonation for Accessing the Job Results Directory](#)
- [Changing the Job Results Path of a Client](#)
- [Changing the Retention of the Job Results of a Client](#)

Job Management for Smart Devices

Other Considerations

- [Hardware Considerations for Data Recovery Operations](#)
- [Job Alive Check Interval](#)
- [Job Update Interval](#)
- [Job Running Time](#)
- [Job Queuing](#)
- [When a Non-Full Backup is Automatically Converted to a Full Backup](#)
- [What happens When There are no Resources for a Job](#)

OVERVIEW

The Job Controller allows you to manage and monitor the following types of jobs:



- Data protection operations
- Data recovery operations
- Administration operations
- Data Collection & Report operations in SRM
- Content Indexing and Search Operations
- Media Refresh operations



The Job Controller window displays all the current jobs in the CommCell. A status bar at the bottom of the job controller shows the total amount of jobs; the amount of jobs that are running, pending, waiting, queued and suspended; and the high and low watermarks. The watermarks indicate the minimum and maximum number of streams that the Job Manager can use simultaneously.



VIEWING JOB INFORMATION

Information about a job is continually updated and available in the Job Controller or Job History window. When a job is finished, the job stays in the Job Controller for five minutes. Once a job is finished, more information about that job is obtainable using the Job History.

The following job information is displayed, depending on the selected Job History:

Job ID	A unique number allocated by the Job Manager that identifies the data protection, data recovery, or administration operation.
Operation	The type of data protection, data recovery, or administration operation being conducted.
Client/Client Computer	For data protection operations, the client computer to which the backup set and subclient belong. For data recovery operations, the computer from which the data originated.
Destination Client	The destination client to which the recovered data will be stored.
Agent Type	The agent that is performing the operation. (e.g., Windows 2000 File System).
Instance/Partition	The instance/partition in the client computer that represents the database that was included in this operation.
Subclient	The subclient that was protected during the operation. Note that a deleted subclient will have a Unix time stamp appended to its name in cases where another subclient is currently using the same name as the deleted subclient.
Job Type	The type of operation that is being conducted on data.
Backup Type	The type of backup that was conducted: Differential , Full , Incremental or Synthetic .
Failed Folders	The number of folders that were not included in the operation.
Failed Files	The number of files that were not included in the operation.
Storage Policy	The storage policy to which the operation is being directed.
MediaAgent	The MediaAgent to which the operation is being directed.
Status	The status of the operation. For job status descriptions, see Job Status Levels
Progress	A status bar indicating its progress. The progress bar is not visible for certain operations (e.g., data aging) or for the initial phases of some data protection operations.  The Job Controller progress bar will not display the progress of SAP for MAXDB backup and restore jobs accurately. This is true because Calypso cannot detect data or objects transferred by SAP for MAXDB due to the way SAP for MAXDB transfers these items.
Errors	Displays any errors that have occurred during the operation, such as a hardware problem or the job has run outside of an operation window. (See Job Errors for more information.)
Backup Set	The backup set that was protected/recovered during the operation and to which the subclient belongs.
Index	Displays New Index to indicate a new index was created during the operation. If blank, a new index was not created.
Instance/Partition	The instance/partition in the client computer that represents the database that was included in this operation.
Phase	The current phase of the operation. The number of phases varies depending on the operation.
User Name	The name of the user who initiated the operation.
Priority	The priority that is assigned to the operation. (For more information, see Job Priorities and Priority Precedence).
Start/Start Time	The date and time on the CommServe when the operation started.
End Time	The date and time on the CommServe when the operation was completed.
Elapsed	The duration of time consumed by the operation.
Libraries	The libraries that is being used by the operation.
Drives/Mount Paths	The drives/mount paths that are being used by the operation. For more information about media, see Media Operations.
Last Update Time	The last time the Job Manager received job updates for the operation.
Transferred	The amount of data that has been transferred for the operation at the present time.
Estimated Completion Time	The time that the Job Manager estimates for this job to be completed. The estimated time will be based on time zone of the CommServe computer.
Size on Media	The total size of data that was transferred to the media (excluding duplicated data).  <ul style="list-style-type: none"> • The amount displayed is the compressed amount (if compression is enabled) and includes valid and invalid attempts of the backup jobs. • Application data that is backed up may include sparse files, metadata, inode security data, etc. As a result, the displayed size of the data may be greater than expected.

	<ul style="list-style-type: none"> If viewing from the storage policy copy level, amount displayed may be less if job is partially copied.
Size of Application	<p>The amount of the application data that has been protected.</p>  <ul style="list-style-type: none"> Application data that is backed up may include sparse files, metadata, inode security data, etc. As a result, the displayed size of the data may be greater than expected. If job has completed with multiple attempts, the amount displayed may be larger.
Size of Backup	The amount of compressed data that has been protected, which includes all application data and metadata.
Content Indexed	<p>Displays Full, Partial, or No to indicate whether content indexing was used for the operation. Operations performed with older releases of the software may display Yes or No.</p> <p>Note that if a job is displayed as partially content indexed, not all of the data protected in the job was content indexed successfully. Rerun content indexing on this job so that the protected data is fully content indexed.</p>
Delay Reason	The description of the reason why the operation may be pending, waiting, or failing.
Alert	The name of the job-based alert, if configured for the job.
Job Initiation	The origin of the operation: the CommCell Console (Interactive), a schedule (Scheduled), or a third party interface (Third Party).
Maximum Number of Readers	The maximum number of readers that can be used for the operation.
Automated Content Classification Policy	Name of the Automated Content Classification Policy.
Legal Hold Name	The Name specified for the Legal Hold data.
Legal Hold Retention Time	The time frame for which the Legal Hold Data will be retained.
Number of Readers in Use	The number of readers currently in use for the operation.
Number of Objects	<p>The total number of objects including successful, failed and skipped.</p>  <p>For a Unix File System iDataAgent backup job that includes hard links and for which the <code>HLINK</code> registry key is set to <code>Y</code> and the appropriate hard link updates are applied, the value in this field will also account for the number of hard links and hard link groups that were backed up.</p> <p>See the Service Pack documentation for more information on hard link updates.</p>
Restart Interval	The amount of time the Job Manager will wait before restarting a job that has gone into a pending state. This is set in the Job Management (Job Restarts) tab.
Max Restarts	The maximum number of times the job will be restarted after a phase of the job has failed. This is set in the Job Management (Job Restarts) tab.
Error Code	Error Code for job pending or job failure reason. (See Job Errors for more information.)
Retained By	The type of retention rules defined for the job, basic or extended. For more information, see Data Aging.
Description	A brief description of the running job.

The Pause  and Play  buttons allow you to control how the Job Controller displays real time information from active jobs. The Pause button stops the Job Controller from displaying real time information collected from jobs. The play button allows the Job Controller to display real time job updates.

To see all the columns in the Job Controller window, use the scroll bar at the bottom of the window.

JOB ERRORS

If a job has not completed successfully, the **Error Code** column will display a unique code linking to available troubleshooting and knowledgebase article(s) relevant to that error from the customer support website. These articles may include special considerations for the type(s) of job(s) you are running, suggested workarounds for issues, and common causes for that particular error.

If an error code pertains to more than one issue, the customer support website will display links to all articles for which the code is relevant. Conversely, if an error code does not have any articles associated with it, the customer support website will display a message indicating that no articles exist for that code.

Error codes may also be obtained from several other windows and dialog boxes, including:

- The Job History windows
- The Job Summary Report
- Events
- Alerts

Note the following when obtaining troubleshooting articles using error codes:

- The Error Code field will only contain a code if a job has not completed successfully.
- In the Job History windows and Job Summary Report, you can access troubleshooting articles by simply click on the linked error code.
- In the Events and Alerts windows, error codes do not provide direct links to troubleshooting articles. However, you can search the customer support website for related articles by typing the appropriate error code in the search field.

Note that jobs which fail Data Integrity Validation will be moved to pending status. Review the error code and description of the pending job from the job controller to identify the reason for failure. See Data Integrity Validation - Troubleshoot for troubleshooting Data Integrity validation errors.

For step-by-step instructions on viewing information about job errors, see View Troubleshooting Article(s) Available from the Customer Support Website.

FLAGS

The Job Controller window also provides a **Flags** column, which is located on the left-hand side of the Job Controller window. The **Flags** column displays an icon for any running jobs that encounter one of the following scenarios:

- A required media cannot be found in the library. This scenario requires user intervention for the job to complete successfully.
- The job has not sent an update (such as bytes or files received) in over 60 minutes. This scenario may or may not require user intervention; for example, if the delay in receipt of updates is caused by insufficient network bandwidth, the job may complete successfully once additional network bandwidth is available. Conversely, if the delay in receipt of updates is caused by a hardware issue, the job will not complete successfully until the user has resolved the hardware issue.
- The job is a high-priority job with a priority level of less than 100.



In order to activate this flag, the `JobHighPriorityMarkEnable` entry must be configured in the `GXGlobalParam` table with a value of 1. When this entry is present, all jobs with a priority of less than 100 will be given a flag in the Job Controller.

To change the default priority for which flags will be shown, the `JobHighPriorityMark` entry can be added and configured with the desired priority level. Note that the `JobHighPriorityMarkEnable` entry must still be present and configured.

If neither of the above scenarios are present, the **Flags** column will remain empty.

VIEWING ADDITIONAL JOB DETAILS

To view additional details about a particular job, right click the job in the Job Controller window and select **Detail**.

- The **General** tab of a Job Details dialog box provides general information about the selected job, such as the subclient, storage policy, etc.
- The **Progress** tab of a Job Details dialog box of the selected job provides more specific statistical information about the selected job's current phase.
- The **Streams** tab of a Job Details dialog box of the selected job provides data transferred by stream on the MediaAgent the job is using.
- The **Attempts** tab of a Job Details dialog box includes information on each attempt of each phase of the selected job, such as the status of each phase of the job. Each phase has a corresponding client log that can aid in troubleshooting data protection problems. Note that the **Data Size/Transferred** field amount includes metadata, and therefore, will be larger than the actual size of the backed up data.
- The **Phase Details** tab of a Job Details dialog box provides information on each phase of the Information Management operations, such as Search, Legal Hold, ERM Connector, Restore to Review Set, and Tagging.
- The **Retention** tab of a Job Details dialog box provides the retention information for the data protection job's storage policy. The associated storage policy copies will be listed with their defined retention rules. From here, you can quickly identify whether the storage policy copies are defined with basic or extended retention rules, and the date(s) until which the data will be retained for each storage policy copy.
- For Oracle specific backup and restore jobs, you can also view the RMAN log for the selected job in the Job Details dialog box.

The Job Controller also provides the facility to view job information using other CommCell Console features, including:

- **Job Events**, which can be viewed using the All Found Events window. For more information about events, see the Event Viewer.
- **Log Files**, which can be viewed for any active job. For more information about viewing log files, see Log Files.

VIEWING LIST OF BACKED UP FILES IN A JOB

Use the `ListFilesForJob` utility to generate a list of files which are backed up during a specific job. Follow the steps give below to create a file which contains the list of files:

1. Open the Command Prompt and navigate to following location:

```
<Software_Installation_Directory>\calypso\Base\
```

2. Enter the following command:

```
ListFilesForJob.exe -job <JOBID> -ma <MAName> [-vm <Instance>] [-flag <ArchiveBitFlag>] [-tmpdir <TMPDIRPATH>] [-o <OUTFILENAME>]
```

Where:

JobID	the job id of the job for which you are generating the list.
MAName	Name of the MediaAgent which is used to perform the backup job.
Instance	Name of the instance which you have used to instal the Windows File System ;DataAgent This is an optional argument. If you do not specify any value, the job in Instance001 will be used by default to generate the list of files.
ArchiveBitFlag	1 to set the Archive Bit 0 to reset the Archive Bit This is an optional argument. If you do not specify any value, the archive bit will not change and the file that contains the list of files can be deleted.
TMPDIRPATH	The directory in which you want to create the file. This argument is optional. If you do not specify any directory, the file will be created in the default temporary directory.

	The default temporary directory for the software is set using the dGALAXYTEMPDIR registry key. When you install Windows File System iDataAgent, the dGALAXYTEMPDIR registry key gets created at the following location: HKEY_LOCAL_MACHINE\SOFTWARE\CommVault Systems\Galaxy\Instance<xxx>\Base
OUTFILENAME	The name of the file in which you want to store the list

3. Navigate to the directory specified in `TMPDIRPATH` and open the `<OUTFILENAME>` file to view the list of files.

CONTROLLING JOBS

You can select a job in the Job Controller and perform a control action on that job individually. You can also control multiple jobs simultaneously in two ways:

- Select each of the desired jobs in the Job Controller window simultaneously, and then right-click any one of the selected jobs. You can then select the appropriate action from the menu displayed, which will be executed for each of the selected jobs.
- Use the Multi-Job Control dialog box.

Either method allows you to perform actions on:

- All jobs in the Job Controller.
- All selected jobs in the Job Controller providing you have the correct security associations at the proper level for each job selected.
- All data protection operations/data recovery operations/data collection operations running for a particular client or client/agent.
- All data protection operations running for a particular MediaAgent.

You can perform the following actions on jobs:

Suspend	Temporarily stops a job. A suspended job is not terminated; it can be restarted at a later time. Only preemptible jobs can be suspended.
Commit	Gracefully completes the current backup job, as of that point-in-time. Applicable only for Silo backup jobs. See Commit a Job for details.
Resume	Resumes a job and returns the status to Waiting, Pending, Queued, or Running depending on the availability of resources or the state of the operation windows and activity control settings.
Kill	Terminates a job.
Change Priority	Change the priority of a job or a group of jobs that are currently active. Note that the lower the priority number, the higher priority the Job Manager gives to the job when allocating resources.

When you suspend or resume a job, a dialog box appears offering you the ability to provide a reason for suspending or resuming a job. This reason, if entered, will be included in the **Description** field of the **Job Details** dialog box.

CONTROLLING THE NUMBER OF SIMULTANEOUSLY RUNNING STREAMS


The Job Controller window displays all the current jobs in the CommCell. A status bar at the bottom of the job controller shows the total amount of jobs; the amount of jobs that are running, pending, waiting, queued and suspended; and the high and low watermarks. The watermarks indicate the minimum and maximum number of streams that the Job Manager can use simultaneously.



- The high watermark has a default value of 10 for SRM Reports.
- The high watermark has a default value of 100 for WorkStation backup jobs running to one destination. You can use the `SetKeyIntoGlobalParamTbl.sql` qscript with the `JMReplicationJobActivityLevelHighWaterMark` global parameter to change the default value. For more information, see Command Line Interface - QScripts.

VIEWING JOB STATUS

The following table describes the status levels that may appear in the Job Controller window for a particular job:

Completed	The job has completed successfully. Note that pop-up messages for reporting job completion can be enabled or disabled using the F12 key.  For a 1-Touch Recovery for Unix job, two jobs are listed as completed if the job is successful. The first job is the operating system recovery, and the second job is the data recovery. The 1-Touch Recovery job is completed once the data recovery is completed.
Completed With Warning	The job has completed successfully but with a notification to the user.
Completed With One or More Errors	The job has completed with errors. The following administration conditions will result in the Completed With One or More Errors status level. <ul style="list-style-type: none"> • Disaster Recovery Backup <ul style="list-style-type: none"> ○ During the operation, Phase 1 failed and Phase 2 completed, or Phase 1 completed and Phase 2 failed. • Data Aging <ul style="list-style-type: none"> ○ During the operation, one or more components failed, e.g., subclients failed to be aged or job history failed to be removed. • Install Updates

	<ul style="list-style-type: none"> ○ During the operation, one or more clients failed to be updated. ● Offline Content Indexing <ul style="list-style-type: none"> ○ During the offline content indexing operation, one or more backup data failed to be content indexed. ● Information Management <ul style="list-style-type: none"> ○ During an information management operation, if the operation defined in the Automated Content Classification Policy is partially successful. <p>The following iDataAgent-specific conditions will result in the Completed With One or More Errors status level.</p> <ul style="list-style-type: none"> ● Exchange Compliance Archiver <ul style="list-style-type: none"> ○ During a retrieve operation, one or more files failed to be retrieved. ● Exchange Mailbox Archiver and Exchange Public Folder Archiver <ul style="list-style-type: none"> ○ During a recovery operation, one or more files failed to be recovered. ● Microsoft Windows File System <ul style="list-style-type: none"> ○ During a system state backup operation, one or more non-critical components failed to be backed up. ○ During a file system restore operation, one or more files failed to restore or were locked. ○ During a system state restore operation, one or more non-critical components failed to be restored. ● Microsoft Exchange Server <ul style="list-style-type: none"> ○ During a backup operation of a storage group assigned to a subclient, one or more databases failed to be backed up. ○ During a restore operation, one or more databases failed to be restored. ● Informix <ul style="list-style-type: none"> ○ During a backup operation, one or more files failed to be backed up. ● Oracle, Oracle RAC <ul style="list-style-type: none"> ○ During a backup operation, one or more files failed to be backed up. ● SAP for Oracle, SAP for MAXDB <ul style="list-style-type: none"> ○ During a backup operation, one or more files failed to be backed up. ● SharePoint Server iDataAgent <ul style="list-style-type: none"> ○ During a backup operation, one or more elements in the subclient content failed to be backed up. ○ During a restore operation, one or more elements in the subclient content failed to be restored. ● SharePoint Archiver <ul style="list-style-type: none"> ○ During a migration archiving operation, one or more elements in the subclient content failed to be archived. ○ During a recovery operation, one or more elements in the subclient content failed to be recovered. ● Sybase <ul style="list-style-type: none"> ○ During a backup operation, one or more files failed to be backed up. ● UNIX File System <ul style="list-style-type: none"> ○ During a backup operation, one or more files failed to be backed up.
Dangling Cleanup	A job phase has been terminated by the job manager, and the job manager is waiting for the completion of associated processes before killing the job phase.
Failed	The job has failed due to errors or the job has been terminated by the job manager.
Interrupt Pending	The job manager is waiting for the completion of associated processes before interrupting the job due to resource contention with jobs that have a higher priority, etc.
Kill Pending	The job has been terminated by the user using the Kill option, and the job manager is waiting for the completion of associated processes before killing the job.
Killed	The job is terminated by the user using the Kill option or by the Job Manager.*
Pending	The Job Manager has suspended the job due to phase failure and will restart it without user intervention.
Queued	<ul style="list-style-type: none"> ● The job conflicted with other currently running jobs (such as multiple data protection operations for the same subclient), and the Queue jobs if other conflicting jobs are active option was enabled from the General tab of the Job Management dialog box. The Job Manager will automatically resume the job only if the condition that caused the job to queue has cleared. ● The activity control for the job type is disabled, and the Queue jobs if activity is disabled option was enabled from the General tab of the Job Management dialog box. The Job Manager will automatically resume the job only if the condition that caused the job to queue has cleared. ● The Queue Scheduled Jobs option was enabled from the General tab of the Job Management dialog box. Scheduled Jobs can be resumed manually using the Resume option or resumed automatically by disabling the Queue Scheduled Jobs option. ● The job started within the operation window's start and end time. ● The running job conflicted with the operation window and the Allow running jobs to complete pass the operation window option was not enabled from the General tab of the Job Management dialog box. (This is only applicable for jobs that can be restarted. See Restarting Jobs for more information.)
Running	The job is active and has access to the resources it needs.
Running (Cannot be verified)	During a running operation, the Job Alive Check failed. See Job Alive Check Interval for more information.
Suspend Pending	A job is suspended by a user using the Suspend option, and the Job Manager is waiting for the completion of associated processes before stopping the job.
Suspended	<ul style="list-style-type: none"> ● A running, waiting or pending job has been manually stopped by a user using the Suspend option. The job will not complete until it is restarted using the Resume option. ● A job has been started in a suspended state using the Start Suspended or Startup in Suspended State options available from the dialog box of the job that was initiated. Restore jobs from Search Console can be started in the suspended state

	using the Start End User restores in suspended state and Start Compliance restores in suspended state options in the Browse/Recover Option Dialog box in the Control Panel.
System Kill Pending	The job has been terminated by the Job Manager*, and the Job Manager is waiting for the completion of associated processes before killing the job.
Waiting	The job is active, waiting for resources (e.g., media or drive) to become available or for internal processes to start.
Destination Client	The restore client machine name. This allows users to verify if the restore data is being written to the correct machine/target.

*The Job Manager will terminate a job when:

- The number of job retries has exceeded the value set in the Job Retry dialog box.
- The total running time has exceeded the amount of time set in the **Job Retry** dialog box.
- Conflicting jobs overlap, i.e., a new backup job is initiated for the same subclient as a job that is currently running.



The Job Manager will only terminate a conflicting job if the new backup job encompasses the earlier job and if the earlier started job has yet to transfer any data to media. If these conditions exist, then the earlier job will be killed by the system and replaced by the newer job. To be more encompassing indicates that a FULL backup can kill jobs such as incrementals, differentials and other fulls; however, incrementals will not be able to kill fulls. If the current job has already started transferring data, then the normal queue rules for the new job will apply.

This feature must be enabled on the CommServe with the `JMKillPreviousBackupJobForSameSubclient` registry key.

- The free space is less than 25MB in the CommServe installation directory.

JOB STATUS FOR SAP FOR ORACLE /DATAAGENT

In the case of SAP for Oracle iDataAgent, the job status is displayed depending on the BRTOOLS error codes.

BRTools Error Code	Message	Job Status
--------------------	---------	------------

In the case of SAP for Oracle iDataAgent, the job status is displayed depending on the BRTOOLS error codes.

JOB STATUS CHANGES

The status of a job and the preemptibility of the phase of the job in the Job Controller determines the actions (Kill, Suspend, or Resume) that you can perform. The following table describes the status of a job after an action has been performed on it:

Original Status	Actions Available	New Status
Running	Suspend	Suspended
	Kill	Killed
Waiting	Suspend	Suspended
	Kill	Killed
Interrupt Pending	N/A	N/A
Pending	Suspend	Suspended
	Resume	Returns to original state, resources and other conditions permitting
	Kill	Killed
Suspend Pending	N/A	N/A
Queued	Suspend	Suspended
	Resume (scheduled jobs only)	Changes into a state of an active job, resources and other conditions permitting
	Kill	Killed
Suspended	Resume	<ul style="list-style-type: none"> • Returns to original state, resources and other conditions permitting • Changes into a state of an active job, resources and other conditions permitting
	Kill	Killed
Kill Pending	N/A	N/A
Dangling Cleanup	N/A	N/A



Jobs that are pending or have failed, will be killed after being in that state for more than 24 hours.

CUSTOMIZING COMPLETED WITH ERRORS CONDITION

You can control the overall status of a backup job by defining error decision rules. You can define multiple decision rules for an agent based on the following criteria:

- File path pattern
- Error codes
- Decision to mark the job with a specific status

The available job status you can select from the decision rule allows you to:
(the list below also reflects the job status priority used by the decision rules)

- Mark the Job as Failed
- Mark the Job as Completed with Errors
- Mark the Job as Complete

Once created, the agent applies the error decision rules at the end of the backup operation. During this process, the agent traverses the `failures.csv` file to match the decision rules based on the priority of the rules. The `failures.csv` file includes information of all the backup files that failed along with their associated error code. When a file and its error codes match a rule, the file is marked with the defined status, and the agent continues to traverse the `failures.csv` file. However, if a file matches a rule that will mark the job as failed, the backup job ends immediately with the failed status. See the graph on the right to understand the process.

Here are some examples that show when it is useful to define error decision rules:

Example 1

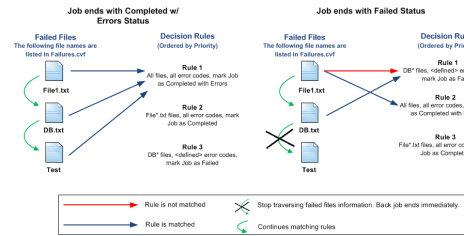
You create a decision rule to ignore any error found in temporary files.

File Pattern: `C:\temp*`
System Error Code: All Error Codes
On error mark Job as: `Complete`

Example 2

You create a decision rule to mark the backup job as failed when an error is found in system data files.

File Pattern: `/**/*.dat`
System Error Code: `1 - 10`
On error mark Job as: `Failed`



SUPPORTED AGENTS

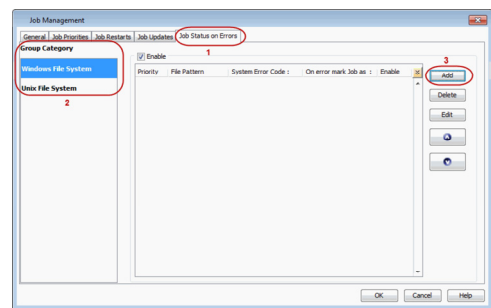
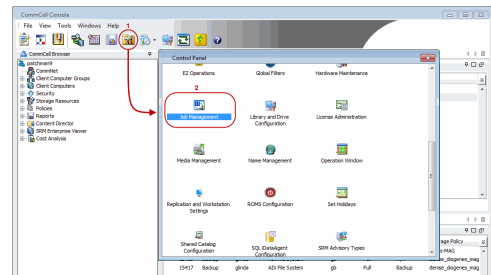
This feature is supported by the following agents:

- Windows File System
- Unix File System

CREATING DECISION RULES

Follow the steps below to add a decision rule for any errors that may occur during a backup operation:

- From the toolbar in the CommCell Console, click **Control Panel**.
 - Double-click **Job Management**.
- Click the Job Status on Errors tab.
 - From the **Group Category** pane, select the agent to add the decision rules for.
 - Click **Add**.
- By default, in the Add Job Error Decision Rule dialog box, all file patterns are considered for the new decision rule.



You can define a file pattern by clearing the **All File Pattern** checkbox and entering a specific file pattern in the **User Defined Pattern** field.

- From the **System Error Code** area:
 - If you want to include all errors, click **All Error Codes**.
 - If you want to define a specific set of error codes, enter the error code range.
- Select the job status from the **On Error mark Job as** drop-down list to update the job if the rule is matched.

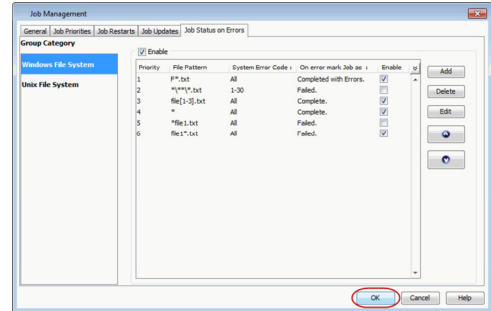
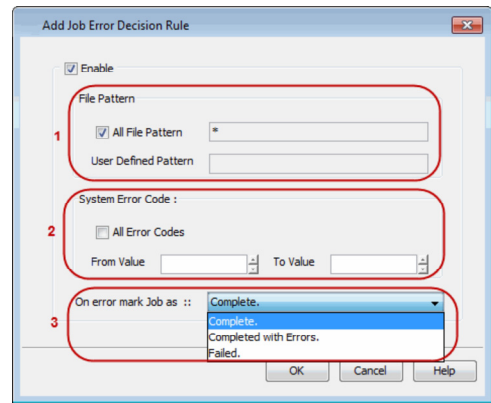
For a SnapProtect backup job, if a decision rule with the "Completed with Errors" status is matched, the job status will be marked as "Complete".

- Click **OK**.

4. Click **OK**.

You can add more error decision rules for the selected agent, or choose a different agent to add new decision rules.

You can also set the priority for the decision rules you created by moving a rule up (higher priority) or down (lower priority) using the arrow buttons.



COMMON ERROR CODES

The following table displays common error codes examples for Windows and Solaris computers:

ERROR CODE VALUE	SYSTEM ERROR MESSAGE
1	Operation not permitted
2	No such file or directory
3	No such process
5	I/O Error
6	No such device or address
13	Permission denied
16	Mount device busy
32	Broken pipe

Please refer to the operating system vendor documentation for a comprehensive list of error codes.

JOB FILTERS

You can filter the jobs that are displayed in the Job Controller by creating a job filter from the Filter Definition dialog box. You can filter by Data Protection, Data Recovery, Data Collection (for SRM jobs), and Administration operations. The filter can also be based on an active job for a particular CommCell entity.

CommCell Administrators can utilize filters created by all users. All other users can only utilize the filters that they create. If a user account is deleted, their filters will automatically be deleted as well.

IMPORTANT CONSIDERATIONS FOR RUNNING JOBS

- If a user is not part of the `View All` user group, then that user will not see CommCell objects for which the user's member user group(s) does not have associations. Furthermore, users will not be able to view the Job Controller or Event Viewer details associated with the CommCell objects for which they do not have permissions. Note that a user will not be able to view these CommCell objects upon logging onto the CommCell Console after the restrictions have been set.
- For the File Archiver Agents, multiple stub recoveries from disk media or tape are submitted to the Job Controller as one job. For such stub recoveries, only one job will display in the Job Controller.

JOB PREEMPTION CONTROL

Jobs or operations fall into two main phases:

Preemptible Phase	In a preemptible phase, the job can be interrupted by the Job Manager or suspended by the user and then restarted without having to start the phase over again from the beginning. Preemption is defined by the Job Manager at each phase of a job. A File System backup phase is one example of a preemptible phase; the Job Manager can interrupt this phase when resource contention occurs with a higher priority job. You can also suspend this phase in progress and resume it later.
Non-preemptible Phase	A non-preemptible phase is one that cannot be interrupted by the Job Manager or suspended by the user. It can only run to completion, be killed by administrative action, or be failed by the system. For example, the data recovery operations of database agents are non-preemptible.

Both preemptible and non-preemptible jobs can also be defined in terms of their restartability; preemptible jobs are always restartable. In addition, even jobs that are not preemptible might fail to start and be in a "waiting" state; these are restartable as well. For more specific information on this topic, see Job Restart.

PREEMPTIBLE AND NON-PREEMPTIBLE JOBS

The following table lists the types of preemptible and non-preemptible jobs:

Preemptible and Restartable	Non-preemptible and Non-Restartable	Non-preemptible but Restartable
<ul style="list-style-type: none"> • Data protection operations for most non-database agents. • DataArchiver archive jobs during the Archive Index and Archive Content Index phases of the job. • Data recovery operations for most File System-like (indexing-based) agents during the restore phase. • Data recovery operations from the Search Console. • Most administration jobs including Install Automatic Updates and Download Automatic Updates. • Silo backup and restore operations. • Media refresh operations. • Deduplication database reconstruction job. 	<ul style="list-style-type: none"> • Data recovery operations for database-like agents. • Media export, erase media, and inventory jobs. • SAN volume data protection jobs (non-preemptible in its scan phase). • All QR jobs on Unix platforms. • Disk volume reconciliation jobs. 	<ul style="list-style-type: none"> • Data protection operations for database agents. • The system state phase of Windows File System data protection operations. • Offline Content Indexing jobs. • Data Collection operations for SRM Agents.

For information on Agents that support Job Restarts, see the following:

- Job Restart - Data Protection - Support
- Job Restart - Data Recovery - Support
- Job Restart - Data Collection - Support

CONTROLLING JOB PREEMPTION FOR THE COMMCELL

You can specify that certain operations will preempt other operations based on their job priority, in cases where multiple jobs are competing for media and drives.

If a running job is preemptible, the Job Manager can interrupt the running job and allocate the resources to a higher-priority job. (The interrupted job enters a waiting state and resumes when the resources it needs becomes available.)

You can:

- Allow restores and browse backup data index restores to preempt other jobs of lower priority such as backups, synthetic fulls, and auxiliary copy operations.
- Allow backups (including Disaster Recovery backups) to preempt other backups of lower priority.
- Allow backups (including Disaster Recovery backups) to preempt auxiliary copy jobs of lower priority.

See Set Job Preemption Control for the CommCell.

CONFIGURING PREEMPTIBILITY FOR SELECT JOB TYPES

You can specify which of the following types of jobs are preemptible:

- Data Protection and Data Recovery operations of indexing-based file system-like agents.
- Disaster Recovery backup
- Auxiliary Copy

To configure preemptibility in the CommCell for specific job types, see Specify Preemptibility of Job Types.

WHAT HAPPENS WHEN A JOB IS PREEMPTED

The following table provides information on the Status of the job in the Job Controller window and the Reason for job delay displayed in the Job Details dialog box when a job is preempted. In addition, a brief explanation on what happens when a job is preempted is also provided.

Job	Status in the Job Controller	Reason for Job Delay	Additional Information
Data Protection Operation	Interrupt Pending	No Job Delay	Once interrupted, job does not hold on to resources and returns to Waiting status. The job retries for resources. (The Status of the job in the Job Controller window and messages in the Reason for job delay are discussed in What Happens When There are no Resources for a Job.)
	Waiting	No resources available	
Data Recovery Operations (for File System-like agents)	Interrupt Pending	No Job Delay	Once interrupted, job does not hold on to resources and returns to Waiting status. The job retries for resources. (The Status of the job in the Job Controller window and messages in the Reason for job delay are discussed in What Happens When There are no Resources for a Job.)
	Waiting	No resources available	
Data Recovery Operation (for Database-like agents)	Not Preemptible		
Index Restore (Browse Backup Data)	Not Preemptible		
Auxiliary Copy	Interrupt Pending	No Job Delay	Once interrupted, job does not hold on to resources and returns to Waiting status. The job retries for resources. (The Status of the job in the Job Controller window and messages in the Reason for job delay are discussed in What Happens When There are no Resources for a Job.)
	Waiting	No resources available	
Synthetic Full	Interrupt Pending	No Job Delay	Once interrupted, job does not hold on to resources and returns to Waiting status. The job retries for resources. (The Status of the job in the Job Controller window and messages in the Reason for job delay are discussed in What Happens When There are no Resources for a Job.)
	Waiting	No resources available	
Media Refresh	Waiting	No resources available	Once interrupted, job does not hold on to resources and returns to Waiting status. The job retries for resources.



The higher priority job that is doing the preemption for resources will display the Reason for Job delay as follows:
Waiting for job[] to release the resources.

IMPORTANT CONSIDERATIONS

- For the Image Level and Image Level ProxyHost /DataAgents, if a backup job is suspended either by the user or the Job Controller during metadata collection, the job will automatically resume from the scan phase.
- For Oracle and Oracle RAC /DataAgents, selective online full backup jobs are not preemptible nor restartable. Similarly, oracle log backup jobs that are submitted during selective online full backups (data phase) also cannot be preempted nor restarted.

RESTARTING JOBS

Restartable jobs can be restarted either by a user or automatically by the Job Manager. Job Restartability can be configured in the Job Management Control Panel; restartability can be turned on or off, the maximum number of restart attempts can be specified, and the time interval between each restart attempt can be configured. These settings are for the entire CommCell, so that all jobs in the CommCell of a selected type will behave according to the Job Restart settings you have specified.

RESTARTABLE AND NON-RESTARTABLE JOBS

Both preemptible and non-preemptible jobs can be restartable; preemptible jobs are always restartable after they are suspended; jobs that are not preemptible might fail to start and be in a "waiting" state and can be restartable as well. Additional insight about jobs that fail to start can be gained from reviewing What Happens When There are no Resources for a Job.

The following types of operations can be restarted, if so configured:

- Auxiliary Copy
- Data Aging
- Data Protection operations of indexing-based, file system-like agents, and certain database-like agents**
- Data Recovery operations of indexing-based, file system-like agents**

- Disaster Recovery backup
- Erase Stubs (a job-based setting is available)
- Online and Offline Content Indexing jobs
- Data Collection (for SRM Agents only)
- Media Refresh

The Job Restarts tab in Job Management Control Panel lists all agents that can be configured for restartability for data protection, data collection and data recovery operations. For more information see, Specify Job Restartability for the CommCell.

For a specific job, you can override one of these settings, the maximum number of restart attempts, by specifying the Number of Retries in the Job Retry tab of the job initiation dialog box for that particular job. See How to Configure Job Restarts for more specific direction on this.

In all cases, whether the Max Restarts setting is used in the Job Management Control Panel, or the Number of Retries setting in the Job Retry tab, once the maximum number of retries has been reached, if the job has still not restarted successfully, the Job Manager will kill the job.



1. The job-based setting will have no affect unless restartability has been turned on in the Job Management Control Panel.
2. You can not configure the interval between restart attempts for an individual job, only the number of attempted restarts.
3. Data Aging restartability can only be set in the Job Management Control Panel; you cannot set it in the Job Retry tab of the job initiation dialog box for that particular job.
4. The restartability of Unix raw partition backup jobs either manually or by the system is not supported. Therefore, you should run such jobs under high priority.
5. Data Protection/Data Collection Jobs that enter a **Running (Cannot be verified)** job state during a temporary network or CommServe service outage will not be restarted. These jobs do not enter a pending state; they will continue, without interruption, when the network or CommServe services become available. For more information, see Fault Tolerance.
6. Restarting an Oracle On Demand backup job for multiple scripts for the same instance will cause the instance, whose backup was interrupted, to be backed up again from the beginning of the script which was running. Because of this restart behavior, if the archive files for that instance were successfully backed up before the restart, they will be backed up again after the restart. As a result, Job Manager may count the data size of archive files twice for the instance that the Oracle On Demand backup job was restarted from. Therefore, the size of data reported as backed up for this job (in the Job Details and Backup Job History) will reflect the duplicate size of the archive files that were backed up twice for that instance. The scripts should be updated to prevent this behavior before resuming the job.
7. If a data management job for the DB2 DPF iDataAgent goes to a pending state, and if the job has completed on some of the nodes, the restart option will start the job on all the nodes unless the `SBKPRESTARTFAILEDNODESTimeOut` registry key is set appropriately.

CONFIGURING JOB RESTARTS FOR THE COMMCELL

1. Using the Job Management control panel, Job Restarts are configured for the entire CommCell. For each job, Specify Job Restartability for the CommCell.
2. For Agents that support the capability, to override the CommCell's **Max Restart** setting for a particular job, you can specify the **Number of Retries** in the **Job Retry** tab of the job configuration dialog box for the following types of jobs:

JOB NAME	HOW TO CONFIGURE JOB RESTARTS	NOTES
Auxiliary Copy	In the Auxiliary Copy dialog, click Advanced , then select the Job Retry tab and specify Number of Retries .	See Start an Auxiliary Copy or Schedule an Auxil Copy for step-by-step instructions.
Data Protection	In the Backup Options or Archive Options dialog, click Advanced , then select the Job Retry tab and specify Number of Retries .	Refer to information specific to your Agent, beginning with the Compliance Archiving, Backup Data, or Migration Archiving page.
Data Recovery	In the Restore Options or Recover Options dialog, click Advanced , then select the Job Retry tab and specify Number of Retries .	Refer to information specific to your Agent, beginning with the Retrieve Data - Exchange Compliance Archiver Agent, Restore Backup Data: Recover Archived Data page.
Data Collection	In the Schedule Data Collection Job dialog, click Advanced , then select Job Retry tab and specify Number of Retries .	See, Data Collection and Run/Schedule a Data Collection Job for an SRM Instance, Agent or Subclient for detailed information.
Disaster Recovery Backup	In the Disaster Recovery Backup Options dialog, select the Job Retry tab and specify Number of Retries .	See Starting a Disaster Recovery Backup or Scheduling a Disaster Recovery Backup for step-step instructions.
Erase Stub/Erase Data jobs	In the Erase Stubs selected for deletion dialog, select the Job Retry tab and specify Number of Retries .	See Erase Data from Outlook Add-In and Erase I by Stubs for step-by-step instructions.
Offline Content Indexing	In the Content Indexing dialog box, click Advanced , then select the Job Retry tab and specify Number of Retries .	See Start or Schedule Offline Content Indexing Operations for step-by-step instructions.
Media Refresh	In the Media Refresh Options dialog box, click	See Media Refresh for step-by-step instructions.

Advanced, then select **Job Retry** tab and specify the **Number of Retries**.

QR VOLUME CREATION RESTARTABILITY

QR Volume Creation restartability is only supported on Windows platforms. See [Create a QR Volume](#) for more information.

SINGLE VOLUME SUBCLIENT

The Quick Recovery Agent maintains a restart string during the Volume Creation (copying) phase of full and incremental copy jobs to keep track of the progress made on each volume being copied. This restart string is updated on the CommServe database every time 1 GB of data is copied per volume. If a job is resumed from a suspended or pending state, this restart string will be retrieved and used to identify the location in the volume from where to resume the copying. For example, a job was suspended with 2.8 GB of the data copied for a particular volume; since the restart string on the volume was last updated when 2 GB completed copying, the job resumed from that point.

MULTI-VOLUME SUBCLIENT

In the QR Volume Creation phase, volumes are copied sequentially (i.e., not in parallel). This affects job restartability behavior for a multi-volume subclient. When a QR Volume Creation job is interrupted (suspended or pending), some of the volumes in the subclient may be completely copied while others may not be copied yet at all. If the job is restarted (either manually or automatically), the behavior toward each volume in the subclient will depend on the condition of the volume at the time of job interruption. Refer to the following table for the expected behavior (for each volume) when resuming an interrupted QR Volume Creation job for a multi-volume subclient.

Volume Condition at the Time of Job Interruption	Behavior when Job Restarts
volume was successfully copied	The Quick Recovery Agent copies any changes to the volume that occurred after the starting point of the original job up to the time of the restart. <i>For example: A job was initiated at 2:00 P.M. At 2:30 P.M., you suspended the job. This job was suspended in the QR Volume Creation (copying) phase, after the volume was successfully copied. At 3:00 P.M. you restarted the job. Upon the resume, the Quick Recovery Agent copied the changes made to the volume from 2:00 to 3:00 P.M.</i>
volume was partially copied	The Quick Recovery Agent runs the full or incremental copy, and then copies any changes to the volume that occurred after the starting point of the original job up to the time of the restart. <i>For example: A job was initiated at 2:00 P.M. At 2:30 P.M., you suspended the job. This job was suspended in the QR Volume Creation (copying) phase, during the copying of the volume. At 3:00 P.M. you restarted the job. Upon the resume, the Quick Recovery Agent ran the initial copy job and then copied the changes made to the volume from 2:00 to 3:00 P.M.</i>
volume was not yet copied	If it's a full copy , the Quick Recovery Agent runs a normal full copy. <i>For example: A job was initiated at 2:00 P.M. At 2:02 P.M., you suspended the job. This job was suspended in the QR Volume Creation (copying) phase, before it copied any parts of the volume. At 3:00 P.M. you restarted the job. Upon the resume, the Quick Recovery Agent ran a full copy job, copying all the data in the volume up to 3:00 P.M.</i> If it's an incremental copy , the Quick Recovery Agent copies any changes that the original incremental would have copied as well any changes to the volume that occurred after the starting point of the original incremental copy job up to the time of the restart. <i>For example: A job was initiated at 2:00 P.M. At 2:02 P.M., you suspended the job. This job was suspended in the QR Volume Creation (copying) phase, before it copied any parts of the volume. At 3:00 P.M. you restarted the job. Upon the resume, the Quick Recovery Agent copied the data that the original incremental copy would have copied, as well as the changes made to the volume from 2:00 to 3:00 P.M.</i>

RETRYING JOBS

The Job Initiation dialog box provides several configuration options for retrying jobs, including:

- **Total Running Time** - The maximum elapsed time, in hours and minutes, from the time that the job is created. When the specified maximum elapsed time is reached, as long as the job is in the "Running" state, it will continue; if the job is not in the "Running" state when the specified time is reached, Job Manager will kill the job.
- **Number of Retries** - The number of times that Job Manager will attempt to restart the job. Once the maximum number of retry attempts has been reached, if the job has still not restarted successfully, Job Manager will kill the job. Note that this job-based setting will not be valid if restartability has been turned off in the Job Management Control Panel.
- **Kill Running Jobs When Total Running Time Expires** - Option to kill the job when the specified Total Running Time has elapsed, even if its state is "Running". This option is available only if you have specified a Total Running Time.

RESUMING JOBS

Jobs that have been in a waiting or pending state can be resumed by right-clicking on the job itself in the Job Controller and selecting **Resume Job**.

RESUBMITTING JOBS

If necessary, you can resubmit a job from the job history windows. This is useful if a job has failed, and you want to run it again. This removes the need to reconfigure a job with the same options. You can resubmit the same job directly from the job history windows. Once you resubmit the job, you will also have the ability to edit the schedule pattern (e.g., daily, weekly, monthly, etc.) and the job options, (e.g., if it is a schedule for a backup job, then the job options would be the type of backup, full, differential, etc.).

For step-by-step instructions, see:

- Resubmit an Admin Job
- Resubmit a Backup Job
- Resubmit a Data Protection Job for a Client
- Resubmit a Data Recovery Job for a Client



Resubmitting jobs can only be executed for jobs that have run utilizing the current release of this software.

JOB RESULTS DIRECTORY

The Job Results directory stores the job results files from backup and restore operations of a client. The following sections describe the steps to configure this directory.

CALCULATING THE SPACE REQUIRED FOR THE JOB RESULTS DIRECTORY

Use the steps below to calculate the required space for the Job Results directory:

SIZE VALUES	HOW TO CALCULATE	EXAMPLE
Step 1: For backup jobs, identify the value for the directory size of the subclients.	$6 * (\text{number of files}) * (\text{subclient average filename size})$	Assume you have the following for all your subclients: <ul style="list-style-type: none"> • 2000 files like /dir1/dir2/filename1. The filename size of these files is 20. • 1000 files like /dir1/dir2/dir3/filename2. The filename size of these files is 25. Using the values above, you can find that: <ul style="list-style-type: none"> • the number of files is 3000 • the subclient average filename size is $(20*2000 + 1000*25)/3000 = 21.67$ So, you can conclude that the directory size of the subclients is: $6*3000*21.67 = 390060 \text{ bytes} = 0.372 \text{ MB}$
Step 2: For restore jobs, identify the value for the average size of a restore job.	$1.5 * (\text{number of restore files}) * (\text{average filename size})$	Assume you have the following; <ul style="list-style-type: none"> • 1500 restore files like /dir1/dir2/filename1. The filename size of these files is 20. • 1000 restore files like /dir1/dir2/dir3/filename2. The filename size of these files is 25. Using the values above, you can find that: <ul style="list-style-type: none"> • the number of restore files is 2500 • the average filename size is $(20*1500 + 1000*25)/2500 = 22$ So, you can conclude that the average size of a restore job is: $1.5*2500*22 = 82500 \text{ bytes} = 0.079 \text{ MB}$
Step 3: For each subclient configured for SnapProtect operations, identify the value for the size of the snapshot copy job.	$7 * (\text{number of files}) * (\text{subclient average filename size})$	Assume you have the following for all your SnapProtect subclients: <ul style="list-style-type: none"> • 1000 files like /dir1/filename1. The filename size of these files is 15. • 500 files like /dir1/dir2/filename2. The filename size of these files is 20. Using the values above, you can find that: <ul style="list-style-type: none"> • the number of files is 1500 • the subclient average filename size is $(15*1000 + 500*20)/1500 = 16.67$ So, you can conclude that the directory size of the subclients is:

		$7*1500*16.67 = 175035 \text{ bytes} = 0.167 \text{ MB}$
Step 4: If using deduplication, identify the value for the size of the Source Side Database.	This value is controlled from the Client Side Deduplication tab of the client properties in the CommCell Console. The default size is 4 GB.	Assuming the default size is being used, then 4 GB are 4096 MB.
Step 5: Using the size values identified in the previous steps, obtain the required space for the Job Results Directory.	<p>directory size of the subclients + (average size of a restore job * A) + (size of the snapshot copy job * B) + size of the Source Side Database</p> <p>where A is the number of restore results to be stored for longer time and B is the number of snapshot copy jobs to be run.</p>	<p>Assume you plan to have:</p> <ul style="list-style-type: none"> • 20 restore results to be stored for longer time. • 10 snapshot copy jobs to be run. <p>Using the size values from the examples above, the required space is:</p> $0.372 + 0.079*20 + 0.167*10 + 4096 = 4099.62 \text{ MB}$

The minimum space required for the Job Results directory is the size value obtained from **Step 1**. If using SnapProtect backups, the minimum space required is the addition of **Step 1** and **Step 3**.

USING UNC PATHS FOR JOB RESULTS DIRECTORY

UNC paths are supported for job results directory by the Exchange Database *iDataAgent* 2007 and above when configured in Cluster Continuous Replicator environment. The Windows File System *iDataAgent* is also supported when configured in this environment.

When assigning UNC paths, the designated directory must be ONE level below the directory which is shared for this purpose. Examples:

\\machine1\<share_name>\job_results\ is shared. Then specify \\machine1\<share_name>\job_results\job_results_1 as the job results directory.

\\machine1\<share_name>\job_results\ is shared. Then specifying \\machine1\<share_name>\job_results as the job results directory is not supported.

USER IMPERSONATION FOR ACCESSING THE JOB RESULTS DIRECTORY

On a Windows client, you need to specify a Windows User Account with the appropriate privileges to access the job results directory.

User impersonation requires that the specified user have write permissions to the product installation folders; otherwise, the user impersonation account may not take effect. This is especially true if the associated computer is not part of a domain and if the user is not a domain user. Additionally, users will need full permissions (registry rights) to the following registry key: \\HKEY_LOCAL_MACHINE\SOFTWARE\CommVault Systems.

In addition, if UNC paths are used for job results and subclient contents are specified as UNC paths, the user impersonation account used for the job results directory must have access to both paths.

For the File System *iDataAgent*, the user impersonation occurs only once; therefore, the user impersonation account specified for the job results directory will take precedence and will be used to back up the contents of the UNC path included in the subclient content.

For the Virtual Server *iDataAgent*, the user impersonation account specified for the job results directory will take precedence and will be used to backup and restore data from a virtual machine. This may result into file access related issues during the backup. Therefore, it is recommended to use a local folder on the client computer as the job results directory.

For the Exchange *iDataAgent*, the account must have the following:

- The account must have the Remote Access rights to the UNC path.

Remote Access can be granted by right-clicking **My Computer** | **Properties** | **Remote** | **Select Remote Users** | **Add** and then specifying the domain\user in the **Select User** dialog box in the computer hosting the UNC path.

- In addition, the Exchange Administrator account specified in the Agent Properties dialog box must have write access permissions to the share used for job results.

Follow the steps below to change the user account for accessing the Job Results directory for the client:

1. From the CommCell Browser, right-click the icon of the client computer whose job results path user account you want to change, and then click **Properties**.
2. From the Job Configuration tab of the **Client Computer Properties** dialog box, click **User Name/Password**.
3. In the Change User Account dialog box, enter the appropriate User Impersonation account information.
4. Click **OK** to save your changes.

CHANGING THE JOB RESULTS PATH OF A CLIENT

1. From the CommCell Browser, right-click the icon of the client computer whose job results path you want to change, and then click **Properties**.
2. From the Job Configuration tab of the **Client Computer Properties** dialog box, if necessary or desired, click **User Name/Password** to establish or change the Impersonate User account to access the Job Results Directory. If you do this, click **OK** once you have administered the account.
3. From the Job Configuration tab, type a new job results path in the **Job results path** field.

You can also click **Browse** to browse to a new job results path from the **Browse for Job Result Path** dialog box. Click **OK**.

4. Click **OK** to save your changes.

CHANGING THE RETENTION OF THE JOB RESULTS OF A CLIENT

1. From the CommCell Browser, right-click the icon of the client computer whose job results retention criteria you want to change, and then click **Properties**.
 2. From the Job Configuration tab of the **Client Computer Properties** dialog box, select the number of days job results should be pruned from the **Prune job results after** field.
 3. Select a disk capacity after which job results should be pruned from the **Prune job results when disk capacity reaches** field.
 4. Click **OK** to save your changes.
-

JOB MANAGEMENT FOR SMART DEVICES

The mobile application allows you to manage and monitor jobs remotely from any mobile device with internet connection. This application is available on Apple and Android devices. For more information, see the Overview page for this application.

OTHER CONSIDERATIONS

Several additional job management capabilities are available. These capabilities are described in the following sections.

HARDWARE CONSIDERATIONS FOR DATA RECOVERY OPERATIONS

The occurrence of a hardware failure during a restore operation puts the job in a device wait state for indefinite time. If a hardware failure occurs, you need to kill the job and start it at a later time when the hardware is available.

When a hardware failure occurs during a restore, the restore job will go into a device wait state indefinitely and will need to be killed.

JOB ALIVE CHECK INTERVAL

The Job Alive Check Interval option within the General tab of the Job Management dialog box allows you to specify the time interval by which the Job Manager will check active jobs to determine if they are still running.

JOB UPDATE INTERVAL

The Job Update Interval allows you to view or modify how often information must be updated for data protection and data recovery operations in the Job Details.

The Job Updates tab of the **Job Management** dialog box displays the:

- Available Agent Types
- Protection Time (in Minutes)
- Recovery Time (in Minutes)

It also includes:

- Update interval time for the ContinuousDataReplicator.

JOB RUNNING TIME

At the time of job initiation, you can determine the total amount of time a job can run before it is killed by the Job Manager. The configurable parameters for Job running time allow you to control the following:

- **Enable Total Running Time**

The maximum elapsed time, in hours and minutes, from the time that the job is created. When the specified maximum elapsed time is reached, as long as the job is in the "Running" state, it will continue; if the job is not in the "Running" state when the specified time is reached, Job Manager will kill the job.

Example: Total Running Time for a job is specified as 1 hour.

- If the job is still running at the 1 hour point, it will continue to run.
- If the job is still running at the 1 hour point, but 30 minutes later you suspend the job, Job Manager will kill the job.
- If the job begins running, and 15 minutes later is suspended and left in that state, 45 minutes later (when the specified Total Running Time of 1 hour has elapsed) Job Manager will kill the job.
- If the job is started in the suspended state and left in that state, 1 hour later (when the specified Total Running Time of 1 hour has elapsed) Job Manager

will kill the job.

- **Kill Running Jobs When Total Running Time Expires**

Option to kill the job when the specified Total Running Time has elapsed, even if its state is "Running". This option is available only if you have specified a Total Running Time.

You can configure the **Total Running Time** and whether to **Kill running jobs when total running time expires** in the **Job Retry** tab of the job initiation dialog box for the following types of jobs:

- For an Auxiliary Copy job, see Start an Auxiliary Copy or Schedule an Auxiliary Copy. In the Auxiliary Copy dialog, click **Advanced**, then select the **Job Retry** tab.
- For a Data Aging job, see Data Aging. In the Data Aging dialog, select the **Job Retry** tab.
- For a Data Protection operation, in the Backup Options or Archive Options dialog, click **Advanced**, then select the **Job Retry** tab. Refer to information specific to your Agent, beginning with the Archive, Backup Data, or Migration Archiving page.
- For a Data Recovery Operation, in the Restore Options or Recover Options dialog, click **Advanced**, then select the **Job Retry** tab. Refer to information specific to your Agent, beginning with the Retrieve Data - Exchange Compliance Archiver Agent, Restore Backup Data, or Recover Archived Data page.
- For a Data Collection Operation, in the Schedule Data Collection Job dialog, click **Advanced**, then select **Job Retry** tab and specify **Number of Retries**. See, Data Collection and Run/Schedule a Data Collection Job for an SRM Instance, Agent or Subclient for detailed information.
- For a Disaster Recovery Backup operation, see Starting a Disaster Recovery Backup or Scheduling a Disaster Recovery Backup. In the Disaster Recovery Backup Options dialog, select the **Job Retry** tab.
- For an Erase Stubs job for Exchange Mailbox Archiver, see Erase Stubs. In the **Erase Stubs selected for deletion in Outlook** dialog, select the **Job Retry** tab.

JOB QUEUING

Setting jobs to be queued allows a job that would otherwise fail to remain in the Job Controller in a **Queued** state, i.e., waiting. Once the condition that caused the job to be queued clears, the Job Manager will automatically resume the job. Jobs can be queued if:

- they conflict with other currently running jobs (such as multiple data protection operations for the same subclient).
- the activity control for the job type is disabled.

You can also set scheduled jobs to be queued. If jobs are scheduled and the **Queue Scheduled Jobs** option is enabled, these jobs will start in the Job Controller in a **Queued** state at their scheduled time. These jobs can be manually resumed or, if the **Queue Scheduled Jobs** option is disabled, these jobs will resume automatically. Selecting this option is especially useful during times of maintenance. Rather than suspend each job manually after it has started, you can enable the **Queue Scheduled Jobs** option, which will start all the scheduled jobs in the Job Controller in a **Queued** state. Once you have completed the maintenance, you can manually resume specific scheduled jobs, or simply deselect the **Queue Scheduled Jobs** option to automatically resume all the scheduled jobs.

The following types of jobs can be queued:

- Data Protection
- Data Recovery
- Data Collection
- Administration Operations

You can set the jobs to be queued from the **General** tab of the **Job Management** dialog box. The following types of jobs can be queued:

- Jobs that are conflicting with other active jobs.
- Jobs that cannot run because activity control for the job type(s) is disabled.
- Scheduled jobs.

WHEN A NON-FULL BACKUP IS AUTOMATICALLY CONVERTED TO A FULL BACKUP

Under the following conditions, a non-full backup is automatically converted to a full backup:

- If it is the first backup of the subclient.
- If you re-associate a subclient to another storage policy.
- If you promote a secondary storage policy copy that is not synchronized with a primary copy (for all the subclients of a storage policy).
- If a backup job within the most recent backup cycle is pruned or disabled from a primary copy.
- If a new content path is added to the subclient.
- If you switch from a SnapProtect backup to a traditional backup or vice versa.
- After CommCell Migration (for some agents).

Some agents have additional scenarios in which a non-full backup is also automatically converted to a full backup:

- **Exchange Database /DataAgents**
 - If an Exchange Database has been restored

- If an Exchange Database has been auto-discovered
- If the Pre-Selected backup type has been changed
- **Image Level and Image Level ProxyHost iDataAgents**
 - After a failover occurs in a clustered environment, without having CXBF bitmap persistence enabled. For more information, see Configure Persistence.
 - After an in-place Volume Level restore
- **Oracle iDataAgent**
 - If an incremental backup is selected for an Oracle subclient that includes Archive Logs and/or control files only
- **SQL Server iDataAgent**
 - See Default Subclient Backup Conversion Rules and File/File Group Subclient Backup Conversion Rules for complete listings.
- **NetWare File System iDataAgent**
 - The first NetWare File System backup run after having selected the backup set option **Decompress Data Before Backup** is converted to a full backup for all subclients that belong to that backup set.
- **Workstation Backup Agent**
 - After an ungraceful shutdown of the source client computer.

WHAT HAPPENS WHEN THERE ARE NO RESOURCES FOR A JOB

Each job requires certain resources for its successful completion. Absence of these resources has different impact on different type of jobs. The following table discusses the resources required by each job, the status of the job in the Job Controller window when there are no resources and the corresponding examples of the Reason for job delay displayed in the **Job Details** dialog box. In addition, a brief explanation on what happens when a job does not have the required resources is also provided.

By default the Bull Calypso Media & Library Manager service on the CommServe cleans up any media and drive reservation that is held by a job which failed to release the resource when it was abruptly terminated, every 1440 minutes. You can modify the frequency using the `nRESOURCERELEASEINTERVALMIN` registry key.

Job	Resources	Status in the Job Controller	Reason for Job Delay	Additional Information
Data Protection Operation	Streams, Active Media, Drive	Waiting	See Example 1.	Job checks for necessary resources.
		Waiting	See Example 2.	If the resources are not available the job retries to reserve the resources when ever they are freed.
				Does not hold on to any resource until all the necessary resources are available.
Data Recovery Operations (for File System-like agents)	Drive	Pending	The media is already reserved by some other job(s).	If the resources are not available the job retries to reserve the resources when ever they are freed.
Data Recovery Operation (for Database-like agents)	Drive	Failed	See Example 1.	Job checks for necessary resources.
		Running	See Example 2.	If the resources are not available it retries every 2 minutes to reserve the resources.
				Does not hold on to any resource until all the necessary resources are available.
Index Restore Operation (Browse Backup Data)	Drive	Failed	See Example 1.	Job checks for necessary resources.
		Running	See Example 2.	If the resources are not available it retries every 2 minutes to reserve the resources.
				Does not hold on to any resource until all the necessary resources are available.
Auxiliary Copy	Destination Drives	Pending	See Example 1.	Job checks for necessary resources.
		Waiting		Job reserves 2 drives for source and destination media.
		Waiting	See Example 2.	If the above resources are not available, it retries every 2 minutes to reserve these resources.
				Does not hold on to any resource until all the necessary resources are available.
		Running		

	Source Media			Once the 2 drives and destination media is obtained job reserves the source media.
		Pending	See Example 2.	If the job encounters resource contention while reserving the source media, (Example 2) it retries every 20 minutes and a maximum of 144 times to obtain the source media.
				Holds on to the 2 drives and destination media as long as it is not interrupted and as long as the source media is available.
Synthetic Full	Streams, Destination Drives, Destination Media	Waiting	See Example 1.	Job checks for necessary resources.
		Waiting		Job reserves streams, marks active media full, reserves 2 drives and destination media.
		Waiting	See Example 2.	If the resources are not available the job retries to reserve the resources whenever they are freed.
				Does not hold on to any resource until all the necessary resources are available.
	Source Media	Running		Once the 2 drives and destination media is obtained job reserves the source media.
		Pending	See Example 2.	If the job encounters resource contention while reserving the source media, (Example 2) it retries every 20 minutes and a maximum of 144 times to obtain the source media.
			Holds on to the 2 drives and destination media as long as it is not interrupted.	

[Back to Top](#)

Job Management - How To

[Topics](#) | [How To](#) | [Support](#) | [Related Topics](#)

Viewing Job Information

[View the Details of a Job](#)

[View the Events of a Job](#)

[View the Media of a Job](#)

[View the Log Files of an Active Job](#)

[View the RMAN Log of an Active Job](#)

[View Troubleshooting Article\(s\) Available from the Customer Support Website](#)

[Change Table Views](#)

[Open a Console Window](#)

Controlling Jobs

[Kill a Job](#)

[Resume a Job](#)

[Suspend a Job](#)

[Commit a Job](#)

[Start a Job in a Suspended State](#)

[Suspend, Resume, and Kill Groups of Jobs](#)

[Suspend, Resume, and Kill Selected Jobs](#)

[Pause and Play Active Jobs in the Job Controller](#)

Disabling Backups for Disabled Clients

Job Filters

Create a Job Filter

Apply a Job Filter

Delete a Job Filter

Job Preemption

Set Job Preemption Control for the CommCell

Specify Preemptibility of Job Types

Restarting Jobs

Specify Job Restartability for the CommCell

Job Alive Check Interval

Set the Job Alive Check Interval

Job Update Interval

Set the Job Update Interval

Job Running Time

Set the Total Running Time for a Job

Job Queuing

Queue Jobs if Other Conflicting Jobs are Active

Queue Jobs if Activity Control is Disabled

Queue Scheduled Jobs

Job Phases

File System *iDataAgent*

Oracle *iDataAgent*

Sybase *iDataAgent*

NAS *iDataAgent*

SQL Server *iDataAgent*

Exchange Database *iDataAgent*

Job States

VIEW THE DETAILS OF A JOB

▶ To view the details of a job:

1. From the CommCell Console, click the Job Controller icon (or select **Job Controller** from the Tools menu). The Job Controller window appears.
2. Right-click the job and then click **Detail** from the shortcut menu. The details of the job you selected are displayed.
3. Click **OK**.



If viewing the details of a job with a pending or failed status, the **Reason for Job Delay** field will contain an Error Code, which, if clicked, will launch the customer support website displaying troubleshooting article(s) related to the specific issue. Additionally, if cache corruption has been found, the field will also contain the information pertaining to the missing updates or service packs.

VIEW THE EVENTS OF A JOB

▶ To view events of a particular job:

1. From the CommCell Console, click the Job Controller icon (or select **Job Controller** from the Tools menu). The Job Controller window is displayed.
2. Right-click the job you want to view the events of and select **View Events**. The All Found Events window is displayed. Use this window to view all of the events associated with this particular job.

VIEW THE MEDIA OF A JOB

Before You Begin

You can only view the media of a data protection operation.

▶ To view the media of a data protection operation:

1. From the CommCell Console, click the Job Controller icon (or select **Job Controller** from the Tools menu). The Job Controller window appears.
 2. Right-click the job and then select **Detail** from the shortcut menu.
 3. Click **View Media** the job details dialog box that is displayed.
 - If the storage policy used by the subclient that you are performing a data protection operation uses disk media, then the List of Mount Paths dialog box is displayed.
 - If the storage policy used by the subclient you are performing the data protection operation uses a tape or optical library, then the Media List is displayed.
 4. Click **OK**.
-

VIEW THE LOG FILES OF AN ACTIVE JOB

Required Capability: See Capabilities and Permitted Actions

▶ To view the log files of an active job:

1. From the Job Controller of the CommCell Console, right-click a job, then click **View Logs** from the short-cut menu.
 2. The contents of the log file related to the selected job are displayed in the **Log File for Job n** window.
-

VIEW THE RMAN LOG OF AN ACTIVE JOB

Required Capability: See Capabilities and Permitted Actions

▶ To view the RMan log of an active job: (applies to Oracle backup and restore jobs only)

1. From the Job Controller of the CommCell Console, right-click a job, then click **Detail** from the short-cut menu.
 2. From the **Job Details** dialog box, click **View Rman Log**.
-

VIEW TROUBLESHOOTING ARTICLE(S) AVAILABLE FROM THE CUSTOMER SUPPORT WEBSITE

Before You Begin

- Verify that the proper user name and password credentials have been entered into the System (Advanced) dialog box.

▶ To view the troubleshooting article(s) available from the customer support website:

1. From the CommCell Console, click the Job Controller icon (or select **Job Controller** from the Tools menu). The Job Controller window appears.
2. From the **Job Controller** window, click on any of the column headings, and enable the **Error Code** column from the popup menu.
3. Click on the code displayed in the **Error Code** column for a failed job. This will launch the customer support website and display the related troubleshooting article(s).



- Error codes may also be obtained from several other windows and dialog boxes, including:
 - The Job History windows
 - The Job Summary Report
 - Events
 - Alerts
 - The Error Code field will only contain a code if a job has not completed successfully.
 - In the Job History windows and Job Summary Report, you can access troubleshooting articles by simply click on the linked error code.
 - In the Events and Alerts windows, error codes do not provide direct links to troubleshooting articles. However, you can search the customer support website for related articles by typing the appropriate error code in the search field.
-

CHANGE TABLE VIEWS

▶ To change the table views for the Job Controller and Event Viewer:

1. From the Job Controller or Event Viewer windows in the CommCell Console, perform either of the following:
 - Right-click any field within the associated window.
 - OR
 - Click the Table Menu icon at the upper right hand corner of the associated window.

The available options for that window are displayed.

2. Select or deselect the parameters you want presented in the respective window.
-

OPEN A CONSOLE WINDOW

▶ To open the CommCell Browser, Job Controller or Event Viewer window:

1. From the CommCell Console, select **Tools** and the desired window.
 2. Alternatively, click the desired icon from the toolbar.
-

KILL A JOB

Required Capability: See Capabilities and Permitted Actions

▶ To kill a job:

1. From the Job Controller of the CommCell Console, right-click the job to be killed and select **Kill** from the shortcut menu.
 2. If you are sure you want to kill the job, click **Yes** when the confirmation prompt appears. The job status may change to **Kill Pending** for a few moments while the operation completes. Once completed, the job status will change to **Killed** and it will be removed from the Job Controller window after five minutes.
-

RESUME A JOB

Required Capability: See Capabilities and Permitted Actions

1. If needed, from the CommCell Console select **Job Controller** from the Tools menu to open the Job Controller window.
2. Right-click the job to be resumed and select **Resume** from the shortcut menu.

As the Job Manager attempts to restart the job, the job status changes to **Waiting**, **Pending**, or **Running**.

SUSPEND A JOB

If you suspend a preemptible job, allow adequate time for the associated processes to stabilize before resuming the job. Resuming the job too early can start additional processes that may interfere with the job.

Required Capability: See Capabilities and Permitted Actions

1. If needed, from the CommCell Console select **Job Controller** from the Tools menu to open the Job Controller window.
2. Right-click the job you want to suspend and select **Suspend** from the shortcut menu.

The job status changes to **Suspended**; however the status may change to **Suspend Pending** for a few moments while the operation completes.

COMMIT A JOB

Before You Begin

This option is available only for Silo Storage. Review Getting Started - Deduplication to Tape (Silo Storage) before you proceed.

Required Capability: See Capabilities and Permitted Actions

▶ To commit a job:

1. From the Job Controller of the CommCell Console, right-click the job and select **Commit** from the shortcut menu.

- The job status may change to **Interrupt Pending** for a few moments while the operation completes. Once completed, the job status will change to **Complete**.
-

START A JOB IN A SUSPENDED STATE

Required Capability: See Capabilities and Permitted Actions

▶ To start a job in a suspended state:

- From the dialog box of the job for which you wish to start in a suspended state:
 - Click **Start Suspended**. From the Enter Option dialog box, click the **Start job in suspended state** check box. Click **OK**. Click **OK** or **Run** to start the job.
 - Click the **Startup in suspended state** check box from the **Startup** tab of the **Advanced Backup/Migration/Archive Options** dialog box if you are initiating a data protection operation. Click **OK**. Click **OK** from the **Backup/Migration/Archive Options** dialog box.
 - Click the **Start job in suspended state** check box from the **Startup** tab of the **Advanced Restore Options** dialog box if you are initiating a data recovery operation. Click **OK** from the **Restore Options** dialog box.
 - The status of the job is displayed as **Suspended** in the Job Controller. To resume the job, right-click the job and click **Resume**.
-

SUSPEND, RESUME, AND KILL GROUPS OF JOBS

Required Capability: When performing an action on multiple jobs in the Job Controller, you must have the correct capability and association for all of the jobs you have selected. If you do not, then you cannot perform a group action on any of these jobs. Make sure you have the correct capability and association before attempting to control groups of jobs in the Job Controller. For more information on capabilities and associations, see Capabilities and Permitted Actions.

▶ To suspend, resume, or kill groups of jobs in the Job Controller:

- From the Job Controller of the CommCell Console, right-click a job in the Job Controller, then select **Multi-Job Control** from the short-cut menu.
 - From the Multi-Job Control Dialog dialog box, select either **Suspend, Resume**, or **Kill**.
 - If you want to suspend, resume, or kill the jobs of clients/agents, then select **All Jobs For This Client**. If you want to control only the data protection/data recovery operations of a particular agent of the client, then select **Only Jobs for this Agent Type**.
 - If you want to suspend, resume, or kill the data protection operations of a MediaAgent, then select **All Jobs On This MediaAgent**.
 - Click **OK**.
-

SUSPEND, RESUME, AND KILL SELECTED JOBS



Required Capability: When performing an action on multiple jobs in the Job Controller, you must have the correct capability and association for all of the jobs you have selected. If you do not, then you cannot perform a group action on any of these jobs. Make sure you have the correct capability and association before attempting to control groups of jobs in the Job Controller. For more information, see Capabilities and Permitted Actions.

▶ To suspend, resume, or kill selected jobs in the Job Controller:

- From the Job Controller of the CommCell Console, highlight and right-click the appropriate jobs, then select **Multi-Job Control** from the short-cut menu.
 - From the Multi-Job Control Dialog dialog box, select either Suspend, Resume, or Kill, then select **All Jobs**.
 - Click **OK**.
-

PAUSE AND PLAY ACTIVE JOBS IN THE JOB CONTROLLER

▶ To pause and play active jobs in the Job Controller:

From the Job Controller of the CommCell Console, click the  pause or  play button in the Job Controller. The pause icon will pause the Job Controller from receiving new job updates. The play icon enables the Job Controller to receive real-time job updates.

DISABLING BACKUPS FOR DISABLED CLIENTS

Required Capability: See Capabilities and Permitted Actions

▶ To disable jobs associated with disabled clients:


- In the CommCell Console, click the **Control Panel** icon, then double-click **Job Management**.


- In the **Job Pre-Emption Control** pane of the General tab of the Job Management dialog box, select the **Do not start backups on disabled client** option.
- Click **OK** to save your changes.

CREATE A JOB FILTER

▶ To create a job filter for the Job Controller or Scheduled Jobs window:

- From the **Job Controller** window, right-click any of the jobs listed, and select the **Filters** option.

Note: To create a filter from the **Schedule Jobs** window of a CommCell Console, select the  button, and skip to Step 3.

- From the Filter Operation dialog box, select the  button.
- From the Filter Definition dialog box:
 - Type a name for the filter in the **Name** box.
 - Click the checkbox next to the operation(s) to be included in this filter.
 - Select the appropriate CommCell entities whose operations are to be included in this filter.
 - Click **OK**.

The filter is created.

APPLY A JOB FILTER

▶ To apply a job filter for the Job Controller or Scheduled Jobs window:

From the Job Controller or from the **Scheduled Jobs** window of a CommCell Console, select a filter from the **Filters** drop-down box, and then click **Apply**. Note that only those operations that were selected as part of the filter will be displayed in the Job Controller or Scheduled Jobs window.

DELETE A JOB FILTER

▶ To delete a job filter:

From the Job Controller or from the **Scheduled Jobs** window of a CommCell Console, select a filter from the **Filters** drop-down box, and then click the  button. The filter is now deleted.

SET JOB PREEMPTION CONTROL FOR THE COMMCELL

Required Capability: See Capabilities and Permitted Actions

▶ To set job preemption control for the CommCell:

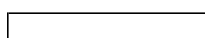
- In the CommCell Console, click the **Control Panel** icon, then double-click **Job Management**.
- In the **Job Pre-Emption Control** pane of the General tab of the Job Management dialog box, select any of the following:
 - Restore Preempts Other Jobs**
 - Backups Preempts Other Backups**
 - Backups Preempts Auxiliary Copy**
- Click **OK** to save your changes.

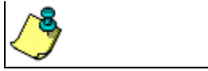
SPECIFY PREEMPTIBILITY OF JOB TYPES

Required Capability: See Capabilities and Permitted Actions

▶ To determine if a job should be Preemptible:

- In the CommCell Console, click the **Control Panel** icon, then double-click **Job Management**.
- In the Job Restarts tab of the Job Management dialog box, select from the **Job Type** list, then click the **Preemptible** check box.
- Click **OK** to save your changes.

 Not all job types are Preemptible.



SPECIFY JOB RESTARTABILITY FOR THE COMMCELL

Required Capability: See Capabilities and Permitted Actions

▶ To specify job restartability for the CommCell:

1. In the CommCell Console, click the **Control Panel** icon, then double-click **Job Management**.
2. In the Job Restarts tab of the Job Management dialog box, select a job type from the **Job Type** list, and then select the **Restartable** check box.
3. To change the maximum number of times the Job Manager will try to restart a job, select a number in the **Max Restarts** box.
4. To change the time interval between attempts by the Job Manager to restart the job, select a number of minutes in the **Restart Interval (Mins)** box.
5. Click **OK** to save your changes.



Not all job types are restartable.

SET THE JOB ALIVE CHECK INTERVAL

Before You Begin

The Job Alive Check Interval cannot be set to less than 120 seconds.

Required Capability: See Capabilities and Permitted Actions

▶ To change the Job Alive Check Interval:

1. From the CommCell Browser, right-click the **CommCell** icon, click **Control Panel**, and then click **Job Management**.
2. Select the General tab of the Job Management dialog box.
3. To set the Job Alive Check Interval, click the up and down arrows, as appropriate, for the **Job Alive Check Interval (Mins)** box.
4. Click **OK** to save your changes.

SET THE JOB UPDATE INTERVAL

Required Capability: See Capabilities and Permitted Actions

▶ To set the Job Update Interval:

1. From the CommCell Browser, right-click the CommServe icon, click **Control Panel**, and then click **Job Management**.
2. From the Job Updates tab of the Job Management dialog box,
 - In the **Protection (Mins)** and/or the **Recovery (Mins)** column, click the integer in the column to change the time.
 - In the **State update interval for ContinuousDataReplicator** and/or the **State update interval for Data Classification** fields, click the integer in the box to change the time.
3. Click **OK** to save your changes.

SET THE TOTAL RUNNING TIME FOR A JOB

Required Capability: See Capabilities and Permitted Actions

▶ To set the total time a job can run before it is killed:

1. From the CommCell Browser, initiate a Data Aging, Data Protection, Data Recovery, Auxiliary Copy, or Disaster Recovery Backup operation.
2. From the Job Retry tab of the appropriate dialog box, select one or both of the following options:
 - Select **Total Running Time** and specify the number of hours and minutes.
 - Optionally select **Kill running jobs when total running time expires**.
3. Click **OK** to save your changes.

QUEUE JOBS IF OTHER CONFLICTING JOBS ARE ACTIVE

Required Capability: See Capabilities and Permitted Actions

▶ To queue jobs when other conflicting jobs are active in the Job Controller:

1. From the CommCell Browser, right-click the **CommCell** icon, click **Control Panel**, and then click **Job Management**.
2. From the General tab of the Job Management dialog box, select the **Queue jobs if other conflicting jobs are active** check box.
3. Click **OK** to save your changes.



- Jobs that are in conflict with other active jobs will remain in the Job Controller in a **Queued** state until the conflict is resolved.
- On Demand Data Protection jobs will always queue because the directive and content files can change with every run.

QUEUE JOBS IF ACTIVITY CONTROL IS DISABLED

Required Capability: See Capabilities and Permitted Actions

▶ To queue jobs if activity control for the job type(s) is disabled:

1. From the CommCell Browser, right-click the **CommCell** icon, click **Control Panel**, and then click **Job Management**.
2. From the General tab of the Job Management dialog box, select the **Queue jobs if activity is disabled** check box.
3. Click **OK** to save your changes.



Jobs will remain in the Job Controller in a **Queued** state until activity control for the job type(s) is enabled.

QUEUE SCHEDULED JOBS

Required Capability: See Capabilities and Permitted Actions

▶ To queue scheduled jobs in the Job Controller until their scheduled time:

1. From the CommCell Browser, right-click the **CommCell** icon, click **Control Panel**, and then click **Job Management**.
2. From the General tab of the Job Management dialog box, select the **Queue Scheduled Jobs** check box.
3. Click **OK** to save your changes.



Jobs scheduled after the **Queue Scheduled Jobs** option is enabled will be started in the Job Controller with a **Queued** status at their scheduled time. Such jobs will resume if the **Queued Scheduled Jobs** option is disabled, or a user manually resumes the job using the **Resume** option.

JOB PHASES

All possible job phases for different *iDataAgents* are described below.

FILE SYSTEM /DATAAGENT

All possible phases for File System *iDataAgent* backup and their descriptions are as follows:

PHASE	DESCRIPTION	BACKUP TYPE
FINISH SYNTHETIC FULL	This phase is run for the first backup job after synthetic full.	Full, Incremental
INDEX RESTORE	If the index from full backup is not in index cache directory, this optional phase is run to restore the index.	Incremental
PRE SCAN	This phase is run to execute Pre Scan operation based on subclient option Pre Scan.	Full, Incremental
SCAN*	During this phase the backup file list is generated and stored in collect files.	Full, Incremental
POST SCAN	This phase is run to execute post scan operation based on subclient option Post Scan.	Full, Incremental
	This phase is run to execute Pre Backup operation based on subclient option Pre	Full, Incremental

PRE BACKUP	Backup.	
BACKUP*	The content is actually backed up to media.	Full, Incremental
POST BACKUP	This phase is run to execute Post Backup operation based on subclient option Post Backup.	Full, Incremental
ARCHIVE INDEX*	Index Cache for the backup job is backedup to media.	Full, Incremental
IMPORT ANALYTICS	SRM analytics are collected if SRM option is selected in subclient options.	Full, Incremental
STUBBING	Generates stubs during turbo archiving backup job.	Full, Incremental

All possible phases for File System iDataAgent restore and their descriptions are as follows:

PHASE	DESCRIPTION	COMMENTS
PRE RESTORE	This phase is run to execute pre restore operations based upon restore options.	Not Applicable
RESTORE*	The selected content will be restored to the destination client and path.	Not Applicable
CLEANUP	This phase is run to cleanup restore task entries if the original restore job fails.	Not Applicable
POST RESTORE	This phase is run to execute post restore operations based upon restore options.	Not Applicable

* are mandatory phases

ORACLE /DATAAGENT

All possible phases for Oracle iDataAgent backup and their descriptions are as follows:

PHASE	DESCRIPTION	BACKUP TYPE
DISCOVER	Discover phase is run for Oracle RAC backup to calculate the number of streams available for backup.	Oracle RAC agent FULL and Incremental.
INDEX RESTORE	Index restore phase is run during incremental job, which is collecting table meta data and the index from previous full is not in index cache directory.	Incremental
PRE BACKUP	This phase is run to execute pre backup command based on subclient option.	Full, Incremental
DATABASE BACKUP*	Rman is executed to backup the database.	Full, Incremental
LOGS BACKUP*	Rman is executed to backup the archive logs.	Full, Incremental
POST BACKUP	This phase is run to execute post backup command based on subclient option.	Full, Incremental
ARCHIVE INDEX	Archives index.	Full, Incremental

All possible phases for Oracle iDataAgent restore and their descriptions are as follows:

PHASE	DESCRIPTION	COMMENTS
PRE RESTORE	This phase is run to execute pre restore operations based upon restore options.	
CONTROL RESTORE*	Rman is executed to restore the control file.	If "Control File" is not chosen in restore options, this phase is skipped.
DATA RESTORE*	Rman is executed to restore and recover the data.	If "Database" content is not selected or "recovery" options are not selected, this phase is skipped.
POST RESTORE	This phase is run to execute post restore operations based upon restore options.	

* are mandatory phases

SYBASE /DATAAGENT

All possible phases for Sybase iDataAgent backup and their descriptions are as follows:

PHASE	DESCRIPTION	BACKUP TYPE
PRE BACKUP	This phase is run to execute pre backup command based on subclient option.	Full, Incremental
TRANSACTION LOG BACKUP*	Rman is executed to backup the archive logs.	Incremental/Transaction Logs Backup
DATABASE BACKUP*	Rman is executed to backup the database.	Full
	This phase is run to execute post backup command based on subclient option.	Full, Incremental

POST BACKUP		
--------------------	--	--

All possible phases for Sybase iDataAgent restore and their descriptions are as follows:

PHASE	DESCRIPTION	COMMENTS
PRE RESTORE	This phase is run to execute pre restore operations based upon restore options.	
DATA RESTORE*	Selected databases will be restored and brought online.	
POST RESTORE	This phase is run to execute post restore operations based upon restore options.	

* are mandatory phases

NAS /DATAAGENT

All possible phases for NAS iDataAgent backup and their descriptions are as follows:

PHASE	DESCRIPTION	BACKUP TYPE
INDEX RESTORE	Restores index from previous full for incremental backups if not available in cache directory.	Incremental
CREATE INDEX*	Initializes Index for the backup job.	Full, Incremental
PRE BACKUP	Runs any defined pre backup script as defined in subclient properties.	Full, Incremental
BACKUP*	Runs the backup. The file server will determine what it needs to backup and will send the NAS Backup process a list of the files it backs up.	Full, Incremental
POST BACKUP	Runs any defined post backup script as defined in subclient properties.	Full, Incremental
ARCHIVE INDEX*	Index Cache for the backup job is backed-up to media.	Full, Incremental
IMPORT ANALYTICS	SRM analytics are collected if SRM option is selected in subclient options.	Full, Incremental

All possible phases for NAS iDataAgent restore and their descriptions are as follows:

PHASE	DESCRIPTION	COMMENTS
PRE RESTORE	Runs and pre-restore script from restore options.	
RESTORE*	Runs the restore. Restore list is sent to the file server – the file servers requests reads of the data.	
CLEANUP	Cleanup is run to free task entries when the restore job fails.	
POST RESTORE	Runs and post-restore script from restore options.	

* are mandatory phases

SQL SERVER /DATAAGENT

All possible phases for SQL Server iDataAgent backup and their descriptions are as follows:

PHASE	DESCRIPTION	BACKUP TYPE
PRE BACKUP	Runs any defined pre backup script as defined in subclient properties.	Full, Transaction Logs Backup
TRANSACTION LOGS*	Backs up transaction logs.	Transaction Logs Backup
DIFFERENTIAL BACKUP*	Backs-up all the changes from previous full backup job.	Differential Backup
DATABASE BACKUP*	Runs the database backup.	Full
POST BACKUP	Runs any defined post backup script as defined in subclient properties.	Full, Incremental

All possible phases for SQL Server iDataAgent restore and their descriptions are as follows:

PHASE	DESCRIPTION	COMMENTS
PRE RESTORE	Runs and pre-restore script from restore options.	
RESTORE	Runs the restore. Restore list is sent to the file server – the file servers requests reads of the data.	
POST RESTORE	Runs and post-restore script from restore options.	

* are mandatory phases

EXCHANGE DATABASE IDATAAGENT

All possible phases for Exchange Database iDataAgent backup and their descriptions are as follows:

PHASE	DESCRIPTION	BACKUP TYPE
DISCOVER	Discovers the databases and nodes available for DAG backups.	Full, Incremental
PRE BACKUP	Runs any defined pre backup script as defined in subclient properties.	Full, Incremental
DATABASE BACKUP*	Runs the backup of database.	Full, Incremental
POST BACKUP	Runs any defined post backup script as defined in subclient properties.	Full, Incremental

All possible phases for Exchange Database iDataAgent restore and their descriptions are as follows:

PHASE	DESCRIPTION	COMMENTS
PRE RESTORE	Runs and pre-restore script from restore options.	
RESTORE*	Runs the restore. Restore list is sent to the file server – the file servers requests reads of the data.	
POST RESTORE	Runs and post-restore script from restore options.	

* are mandatory phases

JOB STATES

All possible states for a Backup/Restore Job and their descriptions are listed as follows:

PHASE	DESCRIPTION
WAITING	A job can be in waiting state for the following reasons: <ol style="list-style-type: none"> 1. Waiting for Storage Resources. 2. Number of jobs have exceeded high water mark limit configuration.
RUNNING*	Job is currently in Progress.
COMPLETED*	Job has successfully run.
COMPLETED WITH ERRORS*	Job has completed with PARTIAL SUCCESS. It has encountered one or more errors. PARTIAL SUCCESS job does not guarantee full recovery of the application.
RUNNING (CANNOT BE VERIFIED)	Job is has been started on the client but Job Manager can not verify the job status. The reason could be network connectivity between client and CS or client process is not responding to Job manager requests.
QUEUED	Job is Queued because of dependent operation/Job is in progress.
PENDING	Job has encountered a recoverable error and can be resumed. Check Job Pending reason and associated event messages. User needs to take care of appropriate action based upon Job Pending Reason.
FAILED	Job is Failed <ol style="list-style-type: none"> 1. It has encountered unrecoverable error. 2. Exceeded Maximum allowed number of restart attempts.

* are mandatory phases

[Back to Top](#)

Job History

Topics | How Do I | Related Topics

Overview

Related Reports

OVERVIEW

Job History allows you to view more detailed information about a job once it has completed. Job history is aged during the Data Aging operation based on the job type, job status and storage policy copy retention criteria. The data is permanently removed only after the job history criteria is met. See Data Aging of Job History Data for more information.

From the following levels of the CommCell, you can view more detailed information about a job, such as how many files were backed up during a data protection operation; the reason an auxiliary copy job failed to start; the throughput of a backup, the job status of the job, etc. Additional job details can be viewed, such as (as applicable per agent) the items that failed or were successfully protected during a data protection operation, items that were restored during a data recovery operation, associated media (of a data protection operation), job events, and the log files of the job.

Level	Types of history
CommServe	Use this level to view the history of administration jobs such as Data Aging, Export Media Auxiliary Copy, Inventory, Disaster Recovery Backup, Data Verification, Erase Media, Erase Backup/Archived Data, Drive Validation, Drive Cleaning, and Stamp Media. See Admin Job History for more information. You can also view the job history for all data management, data recovery, and content indexing jobs that have occurred throughout the CommCell. This history can include history information for any of the entities listed below.
Client Computer Group	Use this level to view the job history of data management and data recovery operations for the client computers that are associated with a client computer group. See Client Job History.
Client	Use this level to view the job history of data management and data recovery operations, for the selected client computer. See Client Job History.
iDataAgent/Backup Set/Instance/Subclient	Use these levels to view the backup and restore history of iDataAgents, backup sets/instances, and subclients. See Backup Job History and Restore Job History.
DataArchiver Agents	Use this level to view the archive and recovery/retrieve history of the DataArchiver agents. See Archive History and Recovery/Retrieve History.
Quick Recovery Agent	Use this level to view the quick recovery volume creation and quick recovery volume recovery of Quick Recovery Agents. See QR Volume Creation History and QR Volume Recovery History.
ContinuousDataReplicator	Use this level to view the Recovery Point creation and Recovery Point copyback history of ContinuousDataReplicator agents. See Recovery Point Creation History and Recovery Point Copyback History.
SRM	
Agents	Use this level to view the Data Collection History of SRM Agents and subclients. See Data Collection Job History for more information.
Reports	Use this level to view the Job History for SRM Report Jobs. See Admin Job History for more information.

JOB ERRORS

If a job has not completed successfully, you can view information about the error(s) encountered by that job by clicking on the job's error code. See Job Errors in Job Controller for more information.

RESUBMIT JOBS

If necessary, you can resubmit a job from the job history windows. This is useful if a job has failed, and you want to run it again. This removes the need to reconfigure a job with the same options. You can resubmit the same job directly from the job history windows.

For step-by-step instructions, see:

- Resubmit an Admin Job
- Resubmit a Backup Job
- Resubmit a Data Protection Job for a Client
- Resubmit a Data Recovery Job for a Client



Resubmitting jobs can only be executed for jobs that have run utilizing the current release of this software.

RELATED REPORTS

JOB SUMMARY REPORT

The Job Summary Report provides a list of various Data Management, Data Recovery, and Administrative jobs.

[Back to Top](#)

Admin Job History

[Topics](#) | [How To](#) | [Related Topics](#)

The **Admin Job History Filter** dialog box allows you to view detailed, historical information about the following administration job types:

- All
- Data Aging
- Export Media
- Auxiliary Copy
- Inventory
- Disaster Recovery Backup
- Data Verification
- Offline Content Indexing
- Erase Media
- Erase Backup/Archived Data
- Drive Validation
- Drive Cleaning
- Stamp Media
- Install Updates
- Download Updates
- Disk Library Maintenance
- SRM Reports
- Information Management

Once chosen, your filter options are then displayed in the Admin Job History window. From this window you can view more detailed information such as the:

- Details of the administration job.
- Events of the administration job.
- Log files of the administration job.

For information on Job Details displayed in the Job History, see [Viewing Job Information](#).

[Back to Top](#)

Admin Job History - How To

[Topics](#) | [How To](#) | [Related Topics](#)

[View Admin Job History](#)

[View Job History Details](#)

[View the Events of a Job History](#)

[Viewing the Log Files of a Job History](#)

[Resubmit an Admin Job](#)

VIEW ADMIN JOB HISTORY

Required Capability: See [Capabilities and Permitted Actions](#)

▶ To view admin job history:

1. From the CommCell Browser, right-click the CommServe, click **View**, and then click **Admin Job History**.
2. From the Admin Job History Filter dialog box, select the filter options that you want to apply and click **OK**.
3. The Admin Job History dialog box displays with the specified filter options.
4. Click **Close**.

VIEW JOB HISTORY DETAILS

Required Capability: See Capabilities and Permitted Actions

▶ To view the details of a job history:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then click job history.
2. From the Job History Filter dialog box, select the filter options that you want to apply and click **OK**.
3. From the Data Management Job History window, right-click the job whose job details you want to view, and then click **View Job Details**.
4. The Job Details dialog box appears, displaying detailed job history in General, Details, Phase Details and Attempts tabs for the selected job.
5. Click **OK**.



If viewing the details of a job with a pending or failed status, the **Reason for Job Delay** field will contain an Error Code, which, if clicked, will launch the customer support website displaying troubleshooting article(s) related to the specific issue.

VIEW THE EVENTS OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

▶ To view the events associated with a job:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then click **Job History**.
2. From the Job History Filter dialog box, select the filter options that you want to apply and click **OK**.
3. From the Data Management Job History window, right-click the job whose job details you want to view, and then click **View Events**.
4. The All Found Events window gets displayed. If no events were found for the back up, a message is displayed to that effect.
5. Click **Close**.

VIEW THE LOG FILES OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

▶ To view the log files of a Job History:

1. From the CommCell Browser, right-click the entity whose job history you want to view, and then click to view a job history.
2. From the job history filter window select the filter options, if any, that you want to apply, and then click **OK**.
3. From the job history window, right-click the job whose log files you want to view, and then click **View Logs**.
4. The contents of the log file related to the selected job history are displayed in the **Log File for Job n** window.

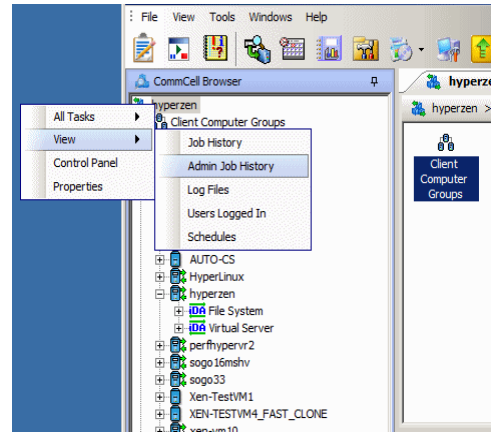
RESUBMIT AN ADMIN JOB

Required Capability: See Capabilities and Permitted Actions

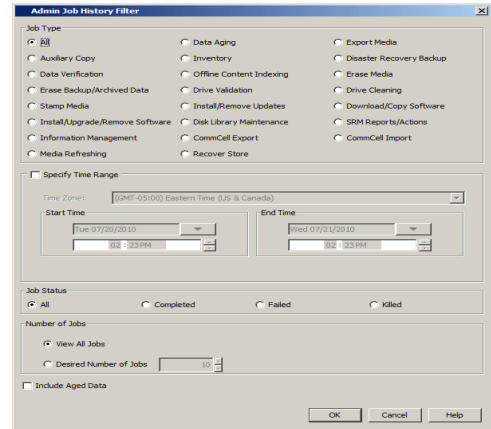
▶ To resubmit an admin job:

1. From the CommCell Browser, right-click the CommServe, click **View**, and then click **Admin Job History**.

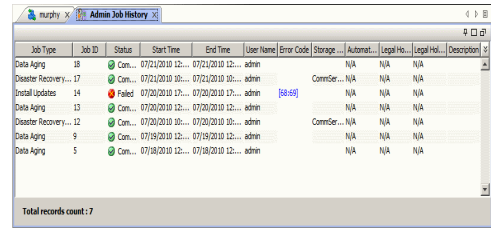
- From the Admin Job History Filter dialog box, select the filter options that you want to apply and click **OK**.



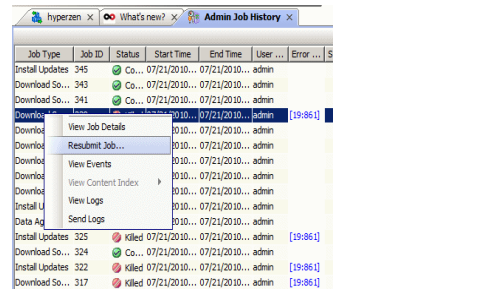
- The Admin Job History window displays with the specified filter options.



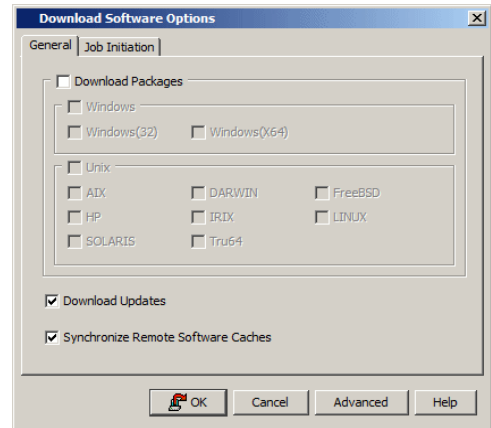
- Right-click on any job (e.g., Download Software), and select **Resubmit**.



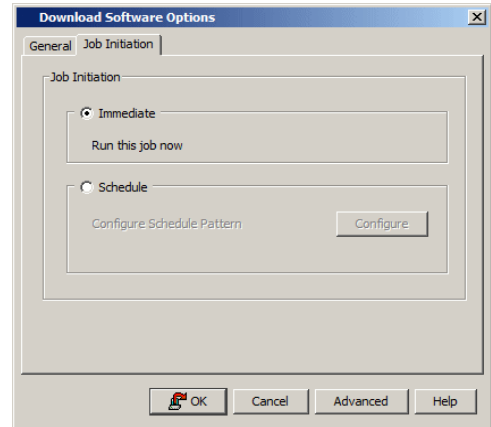
- Select the job options appropriate for the job you want to restart.



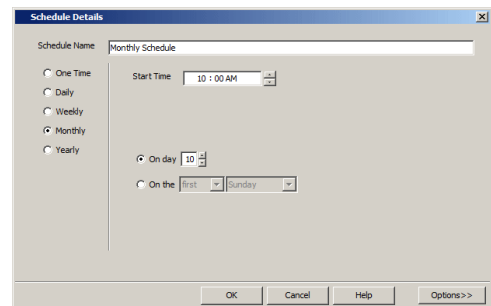
- If you need to run the backup operation immediately, select **Immediate** from the **Job Initiation** tab. Go to step 11.



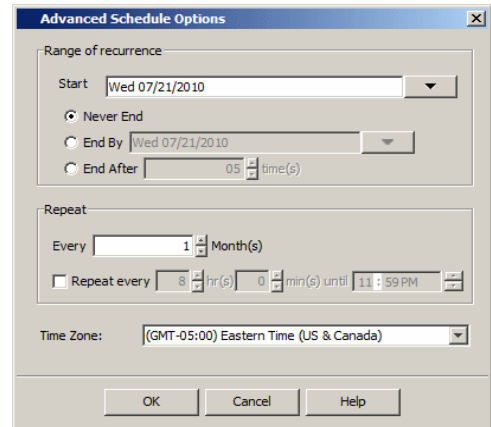
- If you need to schedule the restore operation, select **Schedule** from the Job Initiation tab and click **Configure**.
- From the **Schedule Details** dialog box that appears, select the appropriate scheduling options.
Click **Options** to view the Advanced Schedule Options dialog box.



- From the **Advanced Schedule Options** dialog box:
 - Range of recurrence:** Specify the date on which you want this schedule to take effect.
 - Repeat:** Select the value for which you want to run the job repeatedly on the day in which the job is scheduled to run.
 - Time Zone:** Select a specific time zone from which the job schedule time will be based.
- Click **OK** to close the **Advanced Schedule Options** dialog box.



- Click **OK** to close the **Schedule Details** window.
- Click **OK** to close the job restart window.



[Back to Top](#)

Backup Job History

Topics | How To | Related Topics

Overview

Items That Were Backed Up

Items That Failed

Pruning Backup History Information

Supported Features

Content Indexing History Information

OVERVIEW

You can view the backup and restore history of *iDataAgents*, *BackupSets/Instances*, and subclients.

The **Backup Job History Filter** dialog box allows you view detailed, historical information about backup jobs. Once you have chosen your filter options, they are displayed in the **Backup Job History** window.

For information on Job Details displayed in the Job History, see [Viewing Job Information](#).

From this window, you can right-click a backup job to:

- Browse the data backed up by the backup set or instance from the **Backup Job History** window. This is provided as right-click option for each job. (This menu option, when selected, initiates the **Browse Options** dialog box preset with the values needed to browse the data.)
 - Browse the snapshots created during SnapProtect backup
 - View items that failed during the backup job
 - View details of the backup job
 - View files that were not indexed during a backup job that performed content indexing
 - View associated media
 - View events of the backup job
 - View a list of items that were backed up
 - View a list of items that were moved to media for a SnapProtect backup job
 - View the log files of the backup job.
 - View the RMAN log of an Oracle backup job.
 - View the BRTools log of a SAP for Oracle job. You can view the BRTools log for only those jobs that were initiated from the CommCell Console.
-

ITEMS THAT WERE BACKED UP

The **View backup file list** option allows you to view a list of the files that were backed up during a backup job, along with the data sizes of each backed up file. The **View backed up messages** option allows you to view a list of messages that were backed up by using, along with the alias name, display name, email address, sender name, and recipient of each message.

From these windows you can conduct searches based on a particular string, allowing to find particular files quickly and easily.



It is not recommended that this option is used to view a very large list of items that were backed up (such as lists that total over 100,000 items). It is suggested that the Browse option is used to find a list of backed up items in such cases.

See [View the Items That Were Protected During a Data Protection Operation](#) for step-by-step instructions.

ITEMS THAT FAILED

The items that failed for a data protection operation include individual files that may fail the job even though a particular job completed successfully. You can determine the degree of success for these jobs using this window.

Filters can be used in conjunction with the "Items That Failed" list on the data protection Job History Report to eliminate backup or archive failures by excluding items which consistently fail that are not integral to the operation of the system or applications. Some items fail because they are locked by the operating system or application and cannot be opened at the time of the data protection operation. This often occurs with certain system-related files and database

application files.

Also, keep in mind that you will need to run a full backup after adding failed files to the filter in order to remove them.



A listing of files and folders that failed is not available for the Quick Recovery Agent, or the Image Level and Image Level ProxyHost *iDataAgents*. These agents do not perform a file level backup/copy.

Certain application related files can never be backed up by the File System *iDataAgent* due to the nature of the data. For example, Microsoft SQL Server database files cannot be backed up by the File System *iDataAgent*. In this and other similar circumstances, consider entering files such as these as exclusions in the corresponding subclient filter.

See [View the Items That Failed For a Data Protection Operation](#) for step-by-step instructions.

PRUNING BACKUP HISTORY INFORMATION

You can prune backup history information based on the number of days established in the **Days to keep the backup job histories** option from the **Media Management Configuration (Service Configuration)** dialog box available in the **Control Panel**.



If you have installed the SQL Server *iDataAgent*, do not use the stored procedure **sp_delete_backuphistory**, **sp_delete_database_backuphistory** and **sp_delete_backup_and_restore_history** provided by Microsoft clean up backup history. By default backup history is automatically pruned from the CommServe database and the Microsoft SQL Server, as necessary.

SUPPORTED FEATURES

- NAS *iDataAgents* do not support the ability to view items that failed.
- The Image Level and Image Level ProxyHost *iDataAgents* do not support the ability to Browse the data of a selected backup job in Backup Job History.

CONTENT INDEXING HISTORY INFORMATION

Content Indexing history can also be viewed of *iDataAgents*, BackupSets/Instances, and subclients. The following information is displayed:

ITEMS THAT WERE SUCCESSFULLY CONTENT INDEXED

You can view the list of items that were successfully content indexed during a Content Indexing operation for a particular job. for step-by-step instructions, see [View the Items that Were Successfully Content Indexed](#).

CONTENT INDEXING FAILURES

Content Indexing failures allows you to look at the messages, files and documents that could not be indexed during a content indexing operation. Content Indexing looks at each file (of the supported data types) and indexes its contents allowing advanced searches of backed up/archived/migrated data.

Files that were not indexed, (perhaps because the file's content could not be read) are added to the Content Indexing Failures list, and are viewable from the View Content Index (Failed Items) option in the Job History window. For step-by-step instruction, see [View the Items that Failed to Content Index](#).

[Back to Top](#)

Backup Job History - How To

[Topics](#) | [How To](#) | [Related Topics](#)

[View Backup Job History](#)

[View the Items That Were Protected During a Data Protection Operation](#)

[View the Items That Failed For a Data Protection Operation](#)

[View Job History Details](#)

[View the Media or Mount Paths of a Job History](#)

[View the Events of a Job History](#)

[View the Items that were Moved to Media during SnapProtect Backup](#)

[View the Log Files of a Job History](#)

View the Items that Were Not Indexed During Content Indexing

View the Items that Were Successfully Content Indexed

Resubmit a Backup Job

VIEW BACKUP JOB HISTORY

▶ To view backup history:

1. From the CommCell Browser, right-click the entity (client computer, iDataAgent, backup set or subclient) whose backup history you want to view, click **View**, and then click **View Backup History**.
2. From the Backup History filter window select the filter options, if any, that you want to apply, and then click OK. The system displays the Backup Job History window.
3. Click **OK**.

VIEW THE ITEMS THAT WERE PROTECTED DURING A DATA PROTECTION OPERATION



This option is available for File System-like agents.

Required Capability: none required

▶ To view the list of items that were protected during a data protection operation.

1. From the CommCell Browser, right-click the entity whose history of data protection operations you want to view, click **View**, and then click the necessary options to view a job history.
2. From the Job History Filter dialog box, select the filter options, if any, that you want to apply, and then click **OK**.
3. From the Job History window, right-click the operation whose list of protected items you want to view, and then select **View backup file list/View Backed Up Messages**. The **Backup file List** window displays a list of the backed up files/messages that were included in the backup job. You can use the **Search** option to find items in the window.
4. Click **File -> Exit**.
5. Click **Close** from the **Job History** window.

VIEW THE ITEMS THAT FAILED FOR A DATA PROTECTION OPERATION



A listing of files and folders that failed is not available for the Quick Recovery Agent, nor the Image Level and Image Level ProxyHost iDataAgents. These agents do not perform a file level backup/copy.

▶ To view the list of items that failed for a data protection operation:

1. From the CommCell Browser, right-click the entity whose history of data protection operations you want to view, click **View**, and then click to view a job history.
2. From the Job History Filter dialog box, select the filter options, if any, that you want to apply, and then click **OK**.
3. From the Job History window, right-click the operation whose list of failed items you want to view, and then select **View Failed Items**. The **Unsuccessful Backup Files** window (for DataArchiver Agents, **Items On Which Archive Failed**) displays those items that failed. If no items failed, a message to that effect is displayed.
4. Click **Close**.

VIEW JOB HISTORY DETAILS

Required Capability: See Capabilities and Permitted Actions

▶ To view the details of a job history:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then click job history.
2. From the Job History Filter dialog box, select the filter options that you want to apply and click **OK**.

3. From the Data Management Job History window, right-click the job whose job details you want to view, and then click **View Job Details**.
4. The Job Details dialog box appears, displaying detailed job history in General, Details, Phase Details and Attempts tabs for the selected job.
5. Click **OK**.



If viewing the details of a job with a pending or failed status, the **Reason for Job Delay** field will contain an Error Code, which, if clicked, will launch the customer support website displaying troubleshooting article(s) related to the specific issue.

VIEW THE MEDIA OR MOUNT PATHS OF A JOB HISTORY

▶ To view media or mount paths associated with a job history:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then select the appropriate history.
2. From the Job History window select the filter options, if any, that you want to apply, and then click **OK**.
3. From the job history window, right-click the backup whose media or mount paths you want to view, and then click **View Media**.
4. The Media Used By Job ID window displays a list of media or mount paths used by the operation.
5. Click **OK**.

VIEW THE EVENTS OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

▶ To view the events associated with a job:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then click **Job History**.
2. From the Job History Filter dialog box, select the filter options that you want to apply and click **OK**.
3. From the Data Management Job History window, right-click the job whose job details you want to view, and then click **View Events**.
4. The All Found Events window gets displayed. If no events were found for the backup, a message is displayed to that effect.
5. Click **Close**.

VIEW THE ITEMS THAT WERE MOVED TO MEDIA DURING SNAPPROTECT BACKUP



This option is available for the SnapProtect Backup.

▶ To view the list of items that were moved to tape during SnapProtect Backup.

1. From the CommCell Browser, right-click the entity whose history of data protection operations you want to view, click **View**, and then click the necessary options to view a job history.
2. From the Job History Filter dialog box, select the filter options, if any, that you want to apply, and then click **OK**.
3. From the Job History window, right-click the operation whose list of items moved to media you want to view, and then select **View Backup Copy file listing**. The **Backup file List** window displays a list of the backed up files that were included in the backup copy job. You can use the **Search** option to find items in the window.



- To view the files moved to media for a backup copy job, right-click the SnapProtect backup job corresponding to the Backup Copy job and select **View Backup Copy file listing**.
- View backup items will not display anything for a Backup Copy job.

4. Click **File** -> **Exit**.
5. Click **Close** from the **Job History** window.

VIEW THE LOG FILES OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

► To view the log files of a Job History:

1. From the CommCell Browser, right-click the entity whose job history you want to view, and then click to view a job history.
2. From the job history filter window select the filter options, if any, that you want to apply, and then click **OK**.
3. From the job history window, right-click the job whose log files you want to view, and then click **View Logs**.
4. The contents of the log file related to the selected job history are displayed in the **Log File for Job n** window.

VIEW THE ITEMS THAT WERE SUCCESSFULLY CONTENT INDEXED



This option is available for operations that performed content indexing.

► To view the list items that were not indexed during content indexing:

1. From the CommCell Browser, right-click the entity whose operations you want to view, click **View**, and then click the necessary options to view a job history.
2. From the Job History Filter dialog box, select the filter options, if any, that you want to apply, and then click **OK**.
3. From the Job History window, right-click the job for which you want to view the successfully content indexed items, select **View Content Index**, and click **Successful Items**.
4. Click **Close**.
5. Click **Close** from the **Job History** window.

VIEW THE ITEMS THAT FAILED TO CONTENT INDEX



This option is available for operations that performed content indexing.

► To view the list of items that failed to content index:

1. From the CommCell Browser, right-click the entity whose operations you want to view, click **View**, and then click the necessary options to view a job history.
2. From the Job History Filter dialog box, select the filter options, if any, that you want to apply, and then click **OK**.
3. From the Job History window, right-click the job for which you want to view the list of items failed to content index, select **View Content Index**, and click **Failed Items**.
4. Click **Close**.
5. Click **Close** from the **Job History** window.

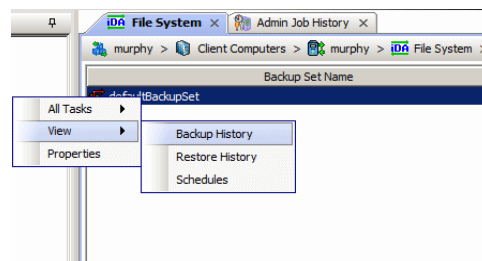
RESUBMIT A BACKUP JOB

► To resubmit a backup job:

1. From the CommCell Browser, right-click the subclient whose backup history you want to view, click **View**, and then click **View Backup History**.

Additionally, you can view the backup history for a client computer, iDataAgent, or backup set. However, the dialogs displayed may be different.

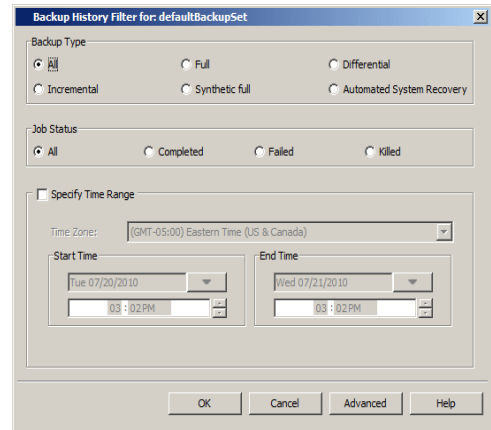
Note, if viewing the backup history for a client computer, right-click the computer name and select **Job History**.



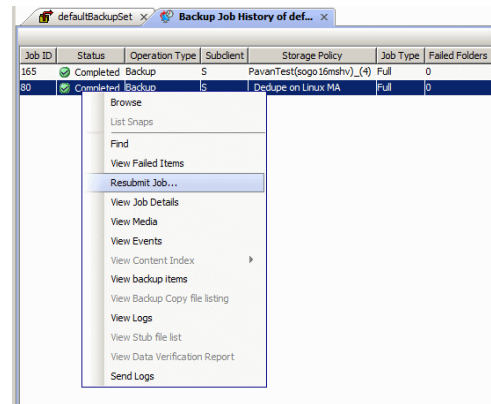
2. From the Backup History filter window select the filter options, if any, that you want to apply, and then click OK. The system displays the Backup Job History window.

Note: If viewing the job history for a client computer, ensure that the **Backup** radio button is selected.

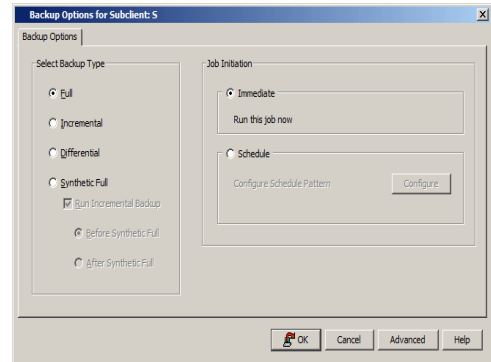
3. The Backup Job History window displays with the specified filter options.
4. Right-click on any job, and select **Resubmit Job**.



5. From the Backup Options dialog box, select the job options appropriate for the job you want to restart.

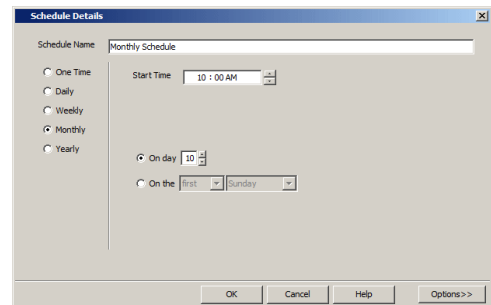


6. If you need to run the backup operation immediately, select **Immediate** from the **Job Initiation** tab. Go to step 11.
7. If you need to schedule the restore operation, select **Schedule** from the Job Initiation tab and click **Configure**.
8. From the **Schedule Details** dialog box that appears, select the appropriate scheduling options.



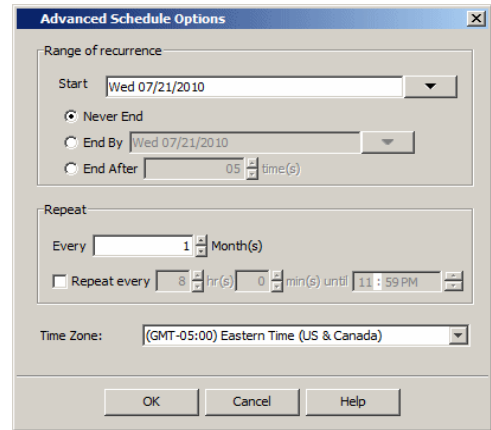
Click **Options** to view the Advanced Schedule Options dialog box.

9. From the **Advanced Schedule Options** dialog box:
 - **Range of recurrence:** Specify the date on which you want this schedule to take effect.



- **Repeat:** Select the value for which you want to run the job repeatedly on the day in which the job is scheduled to run.
- **Time Zone:** Select a specific time zone from which the job schedule time will be based.

Click **OK** to close the **Advanced Schedule Options** dialog box.



10. Click **OK** to close the **Schedule Details** window.
11. Click **OK** to close the job restart window.

[Back to Top](#)

Client Job History

[Topics](#) | [How To](#) | [Related Topics](#)

Overview

[Data Protection Job History](#)

[Data Recovery Job History](#)

OVERVIEW

The Job History filter allows you to view the following types of client and client computer group job history:

- Data protection job history
 - Backup
 - QR Volume Creation
 - Migration/Archive
- Data recovery job history
 - Restore
 - QR Volume Recovery
 - Recovery/Retrieve

For information on Job Details displayed in the Job History, see [Viewing Job Information](#).

DATA PROTECTION JOB HISTORY

If Data Protection Operations is chosen from the Job History Filter dialog box, your filter options are displayed in the Data Protection Job History window. Data protection operations include: **Backup**, **QR Volume Creation**, **Migration/Archive** and **Recovery Point Creation**.

From the Data Protection Job History window, you can view more detailed information such as the:

- Items that failed during the data protection job.
 - Files that were not indexed during a data protection job that performed content indexing.
 - Details of the data protection job.
 - Associated Media.
 - Events of the data protection job.
 - Items that were protected.
 - Log files of the data protection job.
 - Archived messages.
-

DATA RECOVERY JOB HISTORY

If Data Recovery Operations is chosen from the Job History Filter dialog box, your filter options are displayed in the Data Recovery Job History window. Data recovery operations include: **Restore**, **QR Volume Recovery**, **Recovery/Retrieve** and **Stub Recall**.

From the Data Recovery Job History window, you can view more detailed information such as the:

- Items that did/did not restore/recover during the data recovery job.
- Details of the data recovery job.
- Events of the data recovery job.
- Log files of the data recovery job.

If you selected **Stub Recall** as a data recovery job filter option, the results will be displayed in the **Data Recovery Job History** window's Stub Recall Jobs tab.

[Back to Top](#)

Client Job History - How To

Topics | How To | Related Topics

View the Data Protection Job History of a Client

View the Data Recovery Job History of a Client

View the Job History of a Client Computer Group

View the Media or Mount Paths of a Job History

View Job History Details

View the Events of a Job History

View the Items That Were Protected During a Data Protection Operation

View the Items that Were Not Indexed During Content Indexing

View the Items that Were Successfully Content Indexed

View the Log Files of a Job History

Resubmit a Data Protection Job for a Client

Resubmit a Data Recovery Job for a Client

VIEW THE DATA PROTECTION JOB HISTORY OF A CLIENT

▶ To view the data protection job history of a client:

1. From the CommCell Browser, right-click a client computer whose data protection history you want to view, click **View**, then click **View Job History**.
 2. From the Job History Filter, select **Backup, QR Volume Creation**, and/or **Archive/Compliance Archive** from the Data Protection Operations pane, then click **OK**.
 3. If you want to view more advanced options, from the Job History Filter window, select **Backup** and/or **QR Volume Creation**, then click **Advanced**.
 4. From the Data Protection History Advanced Filter, select the type of backup you would like to view, as well as the type of QR Volume Creation operation. Click **OK**.
 5. The system displays the options you selected in the Data Protection Job History window.
 6. Click **OK**.
-

VIEW THE DATA RECOVERY JOB HISTORY OF A CLIENT

▶ To view the history of data recovery operations:

1. From the CommCell Browser, right-click a client computer whose data recovery history you want to view, click **View**, then click to view a job history.
2. From the Job History Filter dialog box, select **Restore, QR Volume Recovery, Recovery/Retrieve** and/or **Stub Recall** from the Data Recovery Operations pane, then click **OK**.
 - If you want to view more advanced options for restores, from the Job History Filter, select **Restore**, then click **Advanced**.
 - From the Data Recovery History Advanced Filter select the destination client computer of the restores you would like to view, then click **OK**.
3. The system displays the results of the options you selected in the Data Recovery Job History window.

If you selected **Stub Recall** as a job history filter option, the system displays the results of the options you selected in the **Data Recovery Job History** window's Stub Recall Jobs tab.

4. Click **OK**.
-

VIEW THE JOB HISTORY OF A CLIENT COMPUTER GROUP

▶ To view the job history of a client computer group:

1. From the CommCell Browser, right-click a client computer whose job history you want to view, click **View**, and then click **Job History**.
2. From Job History Filter dialog box:
 - If you wish to view Data Protection Operations:
 - Click **Backup, QR Volume Creation**, and/or **Archive/Compliance Archive** from the Data Protection Operations pane, then click **OK**.

- If you want to view more advanced options, from the Job History Filter window, select **Backup** and/or **QR Volume Creation**, then click **Advanced**.
 - From the Data Protection History Advanced Filter, select the type of backup you would like to view, as well as the type of QR Volume Creation operation. Click **OK**.
 - The system displays the options you selected in the Data Protection Job History window.
- If you wish to view Data Recovery Operations:
- Click either **Restore**, **QR Volume Recovery**, and/or **Recovery/Retrieve** from the Data Recovery Operations pane, then click **OK**.
 - If you want to view more advanced options for restores, from the Job History Filter, select **Restore**, then click **Advanced**.
 - From the Data Recovery History Advanced Filter select the destination client computer of the restores you would like to view, then click **OK**.
 - The system displays the options you selected in the Data Recovery Job History window. Click **OK**.

VIEW THE MEDIA OR MOUNT PATHS OF A JOB HISTORY

▶ To view media or mount paths associated with a job history:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then select the appropriate history.
2. From the Job History window select the filter options, if any, that you want to apply, and then click **OK**.
3. From the job history window, right-click the backup whose media or mount paths you want to view, and then click **View Media**.
4. The Media Used By Job ID window displays a list of media or mount paths used by the operation.
5. Click **OK**.

VIEW JOB HISTORY DETAILS

Required Capability: See Capabilities and Permitted Actions

▶ To view the details of a job history:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then click job history.
2. From the Job History Filter dialog box, select the filter options that you want to apply and click **OK**.
3. From the Data Management Job History window, right-click the job whose job details you want to view, and then click **View Job Details**.
4. The Job Details dialog box appears, displaying detailed job history in General, Details, Phase Details and Attempts tabs for the selected job.
5. Click **OK**.



If viewing the details of a job with a pending or failed status, the **Reason for Job Delay** field will contain an Error Code, which, if clicked, will launch the customer support website displaying troubleshooting article(s) related to the specific issue.

VIEW THE EVENTS OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

▶ To view the events associated with a job:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then click **Job History**.
2. From the Job History Filter dialog box, select the filter options that you want to apply and click **OK**.
3. From the Data Management Job History window, right-click the job whose job details you want to view, and then click **View Events**.
4. The All Found Events window gets displayed. If no events were found for the back up, a message is displayed to that effect.
5. Click **Close**.

VIEW THE ITEMS THAT WERE PROTECTED DURING A DATA PROTECTION OPERATION



This option is available for File System-like agents.

Required Capability: none required

► To view the list of items that were protected during a data protection operation.

1. From the CommCell Browser, right-click the entity whose history of data protection operations you want to view, click **View**, and then click the necessary options to view a job history.
 2. From the Job History Filter dialog box, select the filter options, if any, that you want to apply, and then click **OK**.
 3. From the Job History window, right-click the operation whose list of protected items you want to view, and then select **View backup file list/View Backed Up Messages**. The **Backup file List** window displays a list of the backed up files/messages that were included in the backup job. You can use the **Search** option to find items in the window.
 4. Click **File -> Exit**.
 5. Click **Close** from the **Job History** window.
-

VIEW THE ITEMS THAT FAILED TO CONTENT INDEX



This option is available for operations that performed content indexing.

► To view the list of items that failed to content index:

1. From the CommCell Browser, right-click the entity whose operations you want to view, click **View**, and then click the necessary options to view a job history.
 2. From the Job History Filter dialog box, select the filter options, if any, that you want to apply, and then click **OK**.
 3. From the Job History window, right-click the job for which you want to view the list of items failed to content index, select **View Content Index**, and click **Failed Items**.
 4. Click **Close**.
 5. Click **Close** from the **Job History** window.
-

VIEW THE ITEMS THAT WERE SUCCESSFULLY CONTENT INDEXED



This option is available for operations that performed content indexing.

► To view the list items that were not indexed during content indexing:

1. From the CommCell Browser, right-click the entity whose operations you want to view, click **View**, and then click the necessary options to view a job history.
 2. From the Job History Filter dialog box, select the filter options, if any, that you want to apply, and then click **OK**.
 3. From the Job History window, right-click the job for which you want to view the successfully content indexed items, select **View Content Index**, and click **Successful Items**.
 4. Click **Close**.
 5. Click **Close** from the **Job History** window.
-

VIEW THE LOG FILES OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

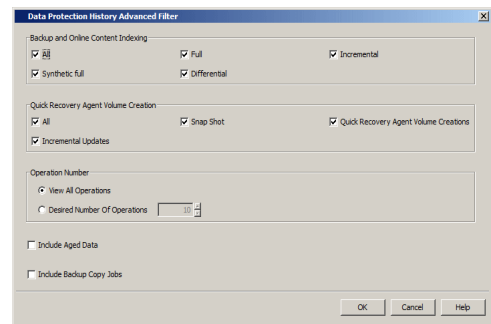
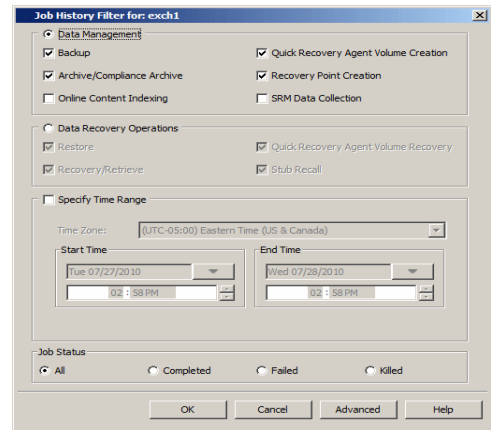
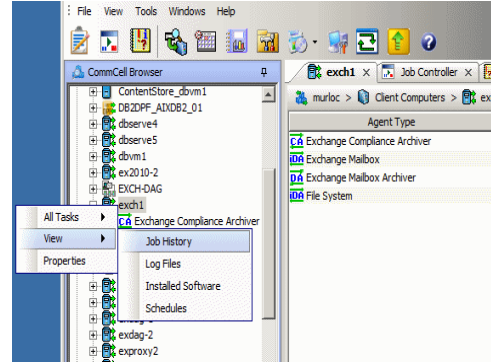
► To view the log files of a Job History:

1. From the CommCell Browser, right-click the entity whose job history you want to view, and then click to view a job history.
 2. From the job history filter window select the filter options, if any, that you want to apply, and then click **OK**.
 3. From the job history window, right-click the job whose log files you want to view, and then click **View Logs**.
 4. The contents of the log file related to the selected job history are displayed in the **Log File for Job n** window.
-

RESUBMIT A DATA PROTECTION JOB FOR A CLIENT

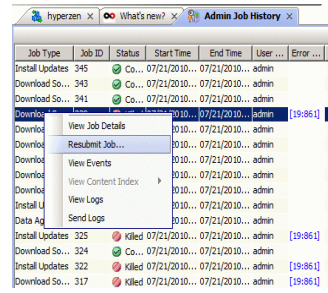
▶ To resubmit a data protection job:

- From the CommCell Browser, right-click a client computer whose data protection history you want to view, click **View**, then click **Job History**.
- From the Job History Filter, select **Backup, QR Recovery Agent Volume Creation, and/or Archive/Compliance Archive** from the Data Protection Operations pane.
- If you want to view more advanced options, from the Job History Filter window, click **Advanced**. Specify the desired options, and then click **OK**.
- From the Job History Filter window, click **OK**. The Admin Job History window displays with the specified filter options.
- Right-click on any job (e.g., a Download Software job), and select **Resubmit**.

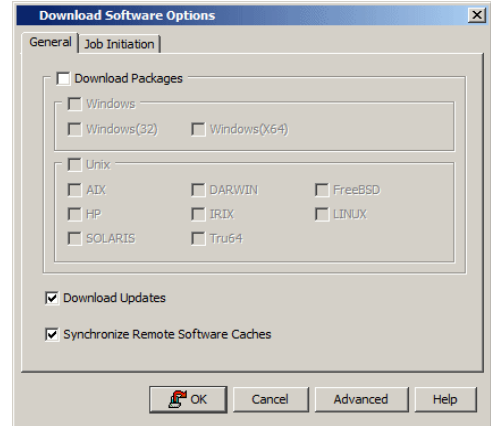


Job ID	Status	Operation Type	Agent Type	Instance	Backup Set	Subclient	Storage Policy
1617	Killed	Compliance Archive	Exchange Compliance Archiver		sub1	Pyre Magnetic	
1616	Killed	Compliance Archive	Exchange Compliance Archiver		sub1	Pyre Magnetic	
1607	Killed	Compliance Archive	Exchange Compliance Archiver		sub1	Pyre Magnetic	
1583	Killed	Compliance Archive	Exchange Compliance Archiver		sub1		
1133	Completed	Compliance Archive	Exchange Compliance Archiver		sub2	legal_SP	
1121	Completed	Compliance Archive	Exchange Compliance Archiver		sub2	legal_SP	
1047	Completed	Compliance Archive	Exchange Compliance Archiver		sub2	legal_SP	
873	Completed	Compliance Archive	Exchange Compliance Archiver		sub1	test	
824	Completed	Compliance Archive	Exchange Compliance Archiver		sub1	sp_1_test	
812	Completed	Compliance Archive	Exchange Compliance Archiver		sub1	sp_1_test	
693	Completed	Compliance Archive	Exchange Compliance Archiver		sub1	sp_1_test	
682	Completed	Compliance Archive	Exchange Compliance Archiver		sub1	sp_1_test	
590	Completed	Compliance Archive	Exchange Compliance Archiver		sub1	sp_1_test	
577	Completed	Compliance Archive	Exchange Compliance Archiver		sub1	sp_1_test	
545	Completed	Compliance Archive	Exchange Compliance Archiver		sub1	sp_1_test	
536	Completed	Compliance Archive	Exchange Compliance Archiver		sub1	sp_1_test	
533	Completed	Compliance Archive	Exchange Compliance Archiver		sub1	sp_1_test	
406	Completed	Compliance Archive	Exchange Compliance Archiver		sub1	sp_1_test	
403	Completed	Compliance Archive	Exchange Compliance Archiver		sub1	sp_1_test	

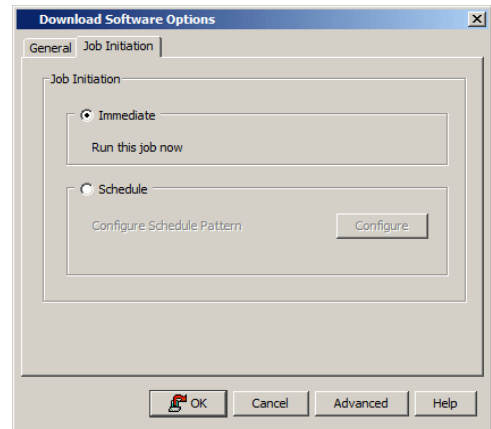
- From the options window (e.g., Download Software Options window), select the appropriate options for the job you want to restart. The available options vary depending on the type of job you want to restart.



- If you need to run the backup operation immediately, select **Immediate** from the **Job Initiation** tab, and then go to step 11.

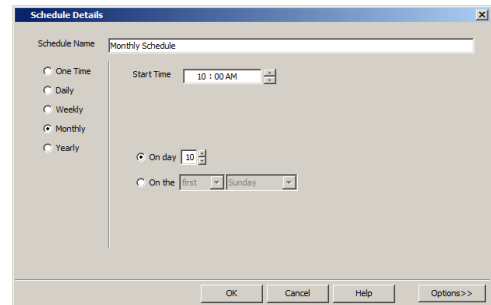


- If you need to schedule the restore operation, select **Schedule** from the Job Initiation pane and click **Configure**.



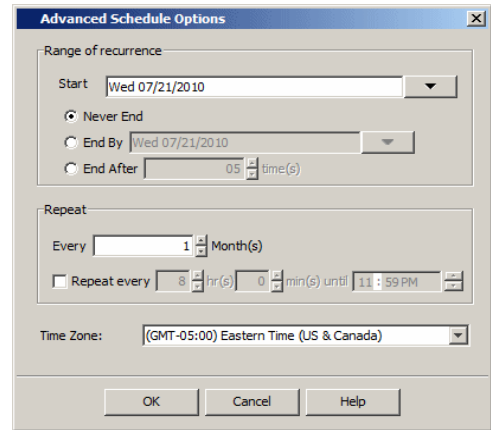
- From the **Schedule Details** dialog box that appears, select the appropriate scheduling options.

Click **Options** to view the Advanced Schedule Options dialog box.



- From the **Advanced Schedule Options** dialog box:
 - Range of recurrence:** Specify the date on which you want this schedule to take effect.
 - Repeat:** Select the value for which you want to run the job repeatedly on the day in which the job is scheduled to run.
 - Time Zone:** Select a specific time zone from which the job schedule time will be based.

Click **OK** to close the **Advanced Schedule Options** dialog box.

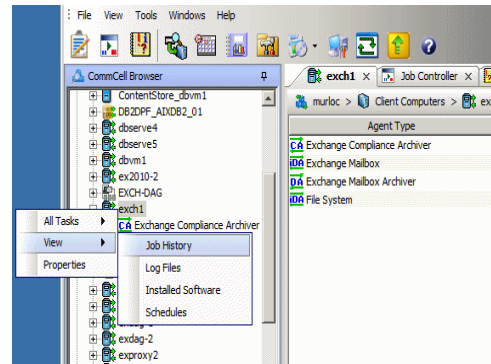


10. Click **OK** to close the **Schedule Details** window.
11. Click **OK** to close the job restart window.

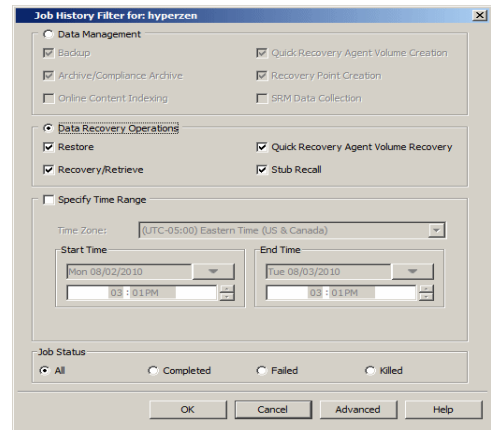
RESUBMIT A DATA RECOVERY JOB FOR A CLIENT

▶ To resubmit a data recovery job for a client:

1. From the CommCell Browser, right-click a client computer whose data recovery history you want to view, click **View**, then click **Job History**. Additionally you can view jobs, by right-clicking a CommNet or a Client Computer Group.

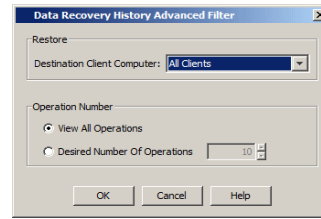


2. From the Job History Filter, select the **Data Recovery Operations** radio button.

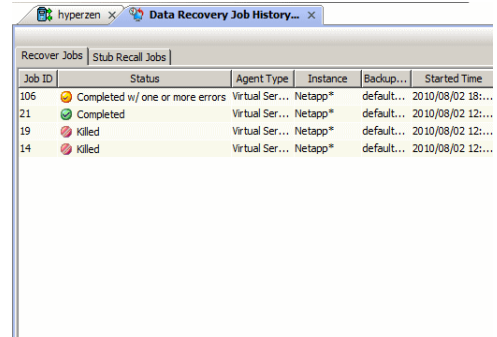


3. Select **Restore**, **QR Volume Recovery**, **Recovery/Retrieve** and/or **Stub Recall** from the Recovery Operations pane.
4. If you want to view more advanced options, from the Job History Filter window, click **Advanced**. Specify the desired options, and then click **OK**.

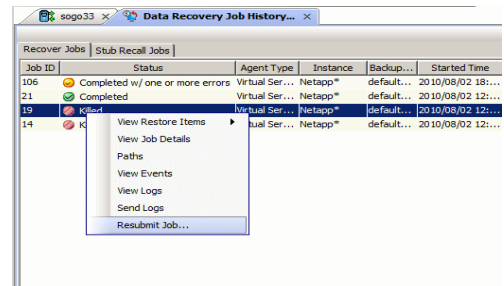
- From the Job History Filter window, click **OK**. The Admin Job History window displays with the specified filter options.
Select the desired Data Recovery Operation tab (e.g., Stub Recall Jobs) if needed.



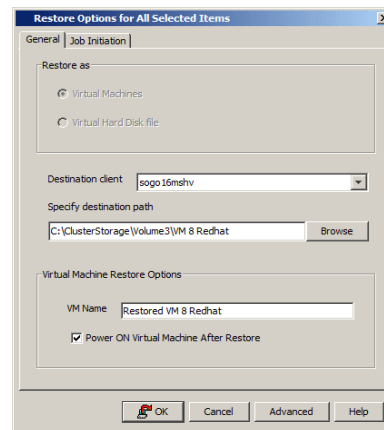
- Right-click on any job (e.g., a Download Software job), and select **Resubmit Job**.



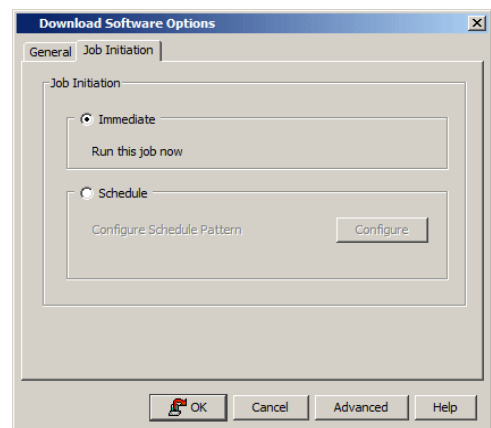
- From the options window (e.g., Download Software Options window), select the appropriate options for the job you want to restart. The available options vary depending on the type of job you want to restart.



- If you need to run the backup operation immediately, select **Immediate** from the **Job Initiation** tab, and then go to step 13.



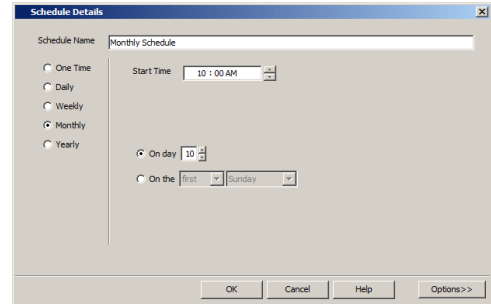
- If you need to schedule the restore operation, select **Schedule** from the Job Initiation



pane and click **Configure**.

10. From the **Schedule Details** dialog box that appears, select the appropriate scheduling options.

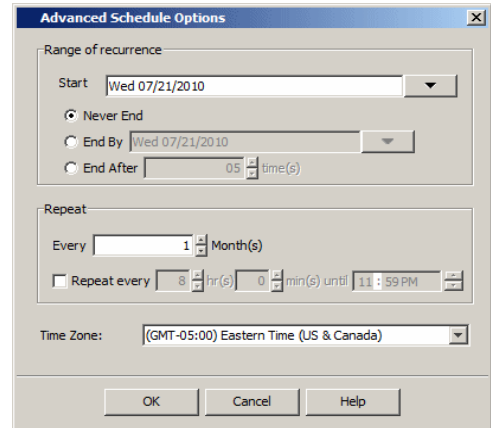
Click **Options** to view the Advanced Schedule Options dialog box.



11. From the **Advanced Schedule Options** dialog box:

- **Range of recurrence:** Specify the date on which you want this schedule to take effect.
- **Repeat:** Select the value for which you want to run the job repeatedly on the day in which the job is scheduled to run.
- **Time Zone:** Select a specific time zone from which the job schedule time will be based.

Click **OK** to close the **Advanced Schedule Options** dialog box.



12. Click **OK** to close the **Schedule Details** window.

13. Click **OK** to close the job restart window.

[Back to Top](#)

Recovery/Retrieve History

Topics | How To | Related Topics

Overview

Items That Recovered

- Showing Recovered Objects for DataArchiver Persistent Recovery Jobs

Pruning Recovery History Information

Recovery/Retrieve History Considerations

OVERVIEW

The **Recovery/Retrieve History Filter** dialog box allows you to view detailed, historical information about recovery or retrieve operations for the DataArchiver agents.

For information on Job Details displayed in the Job History, see [Viewing Job Information](#).

Once chosen, your filter options are then displayed in the Recovery/Retrieve Job History window. From this window you can view more detailed information such as the:

- Items that did/did not recover during the recovery or retrieve job.
- Details of the recovery or retrieve job.
- Events of the recovery or retrieve job.
- Log files of the recovery or retrieve job.

If you want to change the number of days that DataArchiver recovery job history is kept, go to the Control Panel's Media Management Configuration (Data Aging) dialog box and change the settings for the **Days to keep the archiver restore job histories** field.

ITEMS THAT RECOVERED

The list of files that were recovered or retrieved by a data recovery or retrieve operation include those files that were successfully written back to the client file system are appended with the word:

- `RESTORED` (with the File Archiver Agent)
- `RESTORED NEW` (with the Exchange Mailbox/Public Folder Archiver Agents and the Exchange Compliance Archiver Agent)

Occasionally, data may not have been recovered or retrieved due to errors. Such data is appended with the word `Not Restored`.

Under some circumstances, the system may not recover or retrieve certain files because they are older versions of the same files already present in the files system. Such files are appended with the word `OLDER`. However, this word differs if the following recovery options are selected for Exchange Mailbox/Public Folder Archiver Agents:

- If the option `Overwrite` is selected then the message will have be appended with `EXISTED, OVERWROTE`.
- If the option `Skip` is selected, then the message will be appended with `EXISTED, SKIPPED`.

SHOWING RECOVERED OBJECTS FOR DATAARCHIVER PERSISTENT RECOVERY JOBS

The Show Recovered Objects List option may be unavailable from the Recovery History window for DataArchiver stub recovery jobs associated with a common open pipeline (i.e., *persistent recovery* jobs). This includes stub recoveries from disk media for File Archiver for Windows/Unix/NetWare, and stub recoveries from both tape and disk media for File Archiver for Windows/Unix/NetWare instances (Local File System, Celerra, FPolicy, Network File Share). In order to view the list of recovered objects for these DataArchiver persistent recovery jobs, select the View Job Details option then access the Job Details (Details) tab.

You can use the `nDMRSendFileStatus` registry key to reduce the frequency at which the stub recovery job statistics are sent to Job Manager for updating the Recovery Job History views and reports. This is useful for increasing the efficiency of system resources in cases where there are frequent stub recalls and there is no need to update the Job History immediately after each stub recall.

PRUNING RECOVERY HISTORY INFORMATION

You can prune recovery history information based on the number of days established in the **Days to keep the archiver restore job histories** option from the Media Management Configuration (Data Aging) dialog box available in the **Control Panel**.

RECOVERY/RETRIEVE HISTORY CONSIDERATIONS

- Keep in mind that stub recall job history cannot be viewed for File Archiver for Windows recall jobs initiated from the physical node of a cluster in cases where only the driver is loaded on that node. However, browse recovery jobs which are initiated from the virtual server can still be viewed in job history. To obtain statistics on stub recall jobs in this scenario, we recommend running the Stub Recall Summary Report.
 - When viewing the Recovery History of Stub Recalls (via the **Stub Recall Jobs** tab), it will be displayed as originating from the **defaultArchiveSet** and the first **Partition** even if a user-defined Archive Set or other partition were used during the recall. Partitions are applicable to Domino Mailbox Archiver.
-

[Back to Top](#)

Recovery History - How To

[Topics](#) | [How To](#) | [Related Topics](#)

[View Recovery/Retrieve Job History](#)

[View Job History Details](#)

[View the Events of a Job History](#)

[View the Items Recovered for a Data Recovery Operation](#)

[View the Log Files of a Job History](#)

VIEWING RECOVERY/RETRIEVE JOB HISTORY

▶ To view the job history of recovery/retrieve operations:

1. From the CommCell Browser, right-click the agent whose recovery/retrieve history you want to view, click **View**, then click **Job History** -> **Recovery**, or click **View Retrieve History**.
 2. From the Recovery/Retrieve History Filter select the desired options, then click **OK**.
 3. The system displays the Recovery/Retrieve Job History window using the options you selected.
 4. Click **OK**.
-

VIEW JOB HISTORY DETAILS

Required Capability: See Capabilities and Permitted Actions

▶ To view the details of a job history:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then click job history.
2. From the Job History Filter dialog box, select the filter options that you want to apply and click **OK**.
3. From the Data Management Job History window, right-click the job whose job details you want to view, and then click **View Job Details**.
4. The Job Details dialog box appears, displaying detailed job history in General, Details, Phase Details and Attempts tabs for the selected job.
5. Click **OK**.



If viewing the details of a job with a pending or failed status, the **Reason for Job Delay** field will contain an Error Code, which, if clicked, will launch the customer support website displaying troubleshooting article(s) related to the specific issue.

VIEW THE EVENTS OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

▶ To view the events associated with a job:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then click **Job History**.

2. From the Job History Filter dialog box, select the filter options that you want to apply and click **OK**.
 3. From the Data Management Job History window, right-click the job whose job details you want to view, and then click **View Events**.
 4. The All Found Events window gets displayed. If no events were found for the backup, a message is displayed to that effect.
 5. Click **Close**.
-

VIEW THE ITEMS THAT RESTORED/RECOVERED FOR A DATA RECOVERY OPERATION

▶ To view the list of files that were restored/recovered for a data recovery operation:

1. From the CommCell Browser, right-click the entity whose data recovery operation history you want to view, click **View**, and then click to view a job history.
 2. From the Job History Filter window, select the filter options, if any, that you want to apply, and then click **OK**.
 3. From the Job History window, right-click the job whose list of restored files you want to view, and then select **View Restore Files List** (for DataArchiver Agents select **Show Recovered Objects List**). The **Restored Files** window (for DataArchiver Agents it is the **Recovered Objects** window) displays those items that were restored/recovered. If no items failed, a message is displayed to that effect.
 4. Click **Close**.
-

VIEW THE LOG FILES OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

▶ To view the log files of a Job History:

1. From the CommCell Browser, right-click the entity whose job history you want to view, and then click to view a job history.
 2. From the job history filter window select the filter options, if any, that you want to apply, and then click **OK**.
 3. From the job history window, right-click the job whose log files you want to view, and then click **View Logs**.
 4. The contents of the log file related to the selected job history are displayed in the **Log File for Job n** window.
-

[Back to Top](#)

Restore Job History

Topics | How To | Related Topics

Overview

Items That Restored

Supported Features

OVERVIEW

The **Restore History Filter** dialog box allows you to view detailed, historical information about restore jobs.

For information on Job Details displayed in the Job History, see [Viewing Job Information](#).

Once you have chosen your filter options, they are displayed in the **Restore Job History** window. From this window you can right-click a restore job to:

- View Restore Items; items in the job that were **Successful**, **Failed**, **Skipped** or **All**. These items, if any, will be listed in the **Restored Files** window.
 - View Job Details of the restore job. The job details will be listed in the **Job Details** window.
 - View Events of the restore job. The job events will be listed in the **All Found Events** window.
 - View Log files of the restore job. The job log files will be listed in the **Log File** window.
 - View the RMAN Log of an Oracle restore job. The RMAN Log will be listed in the **Oracle Restore Log** window.
 - View the BRTools log of a SAP for Oracle restore job. You can view the BRTools log for only those jobs that were initiated from the CommCell Console.
-

ITEMS THAT ARE RESTORED

When viewing files that are restored in the **Restored Files** window, each of the files is listed with the restore status level appended at the end of the file path. The possible status levels are: `RESTORED`, `FAILED` and `OLDER`.

Successfully restored files will be listed with `RESTORED` appended to the file path. If files are not restored/recovered due to errors, the file paths will be appended with `FAILED`. Under some circumstances, the system may not restore/recover certain files because they are older versions of the same files already present in the files system; these files are appended with the word `OLDER`.

SUPPORTED FEATURES

Consider the following.

- NAS *iDataAgents* do not support the ability to view failed/successful item lists.
 - Restore Job History will not display Oracle `rman_util` jobs at the instance level.
-

[Back to Top](#)

Restore History - How To

Topics | How To | Related Topics

[View Restore Job History](#)

[View the Events of a Job History](#)

[View the Media of a Job History](#)

[View the Log Files of a Job History](#)

VIEW RESTORE JOB HISTORY

▶ To view the restored items associated with a job:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job restore history you want to view, click **View**, and then click **Restore History**.

2. From the Job History filter window, select the filter options, if any, that you want to apply, and then click **OK**.
 3. From the Job History window, right-click the job whose restored items you want to view; click **View Restore Items**, and select from the type of items to view: **Successful**, **Failed**, **Skipped** or **All**.
 4. The **Restored Files** window will display the selected type of restored items for the job.
 5. Click **OK**.
-

VIEW THE EVENTS OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

▶ To view the events associated with a job:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then click **Job History**.
 2. From the Job History Filter dialog box, select the filter options that you want to apply and click **OK**.
 3. From the Data Management Job History window, right-click the job whose job details you want to view, and then click **View Events**.
 4. The All Found Events window gets displayed. If no events were found for the backup, a message is displayed to that effect.
 5. Click **Close**.
-

VIEW THE MEDIA OR MOUNT PATHS OF A JOB HISTORY

▶ To view media or mount paths associated with a job history:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then select the appropriate history.
 2. From the Job History window select the filter options, if any, that you want to apply, and then click **OK**.
 3. From the job history window, right-click the backup whose media or mount paths you want to view, and then click **View Media**.
 4. The Media Used By Job ID window displays a list of media or mount paths used by the operation.
 5. Click **OK**.
-

VIEW THE LOG FILES OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

▶ To view the log files of a Job History:

1. From the CommCell Browser, right-click the entity whose job history you want to view, and then click to view a job history.
 2. From the job history filter window select the filter options, if any, that you want to apply, and then click **OK**.
 3. From the job history window, right-click the job whose log files you want to view, and then click **View Logs**.
 4. The contents of the log file related to the selected job history are displayed in the **Log File for Job n** window.
-

[Back to Top](#)

Recovery Point Creation History

Topics | How To | Related Topics

You can view the Recovery Point creation history of ContinuousDataReplicator. The **Job History Filter** dialog box allows you to view detailed, historical information about jobs.

Once you have chosen your filter options, jobs that meet the criteria you selected are displayed in the **Job History** window. From this window you can right-click a job and view more detailed information such as the:

- Items that failed during the job.
 - Items that were killed.
 - Details and events of the job.
 - A list of the Recovery Points that were created.
-

[Back to Top](#)

Recovery Point Creation History - How To

Topics | How To | Related Topics

[View Job History Details](#)

[View the Items That Failed For a Data Protection Operation](#)

[View the Events of a Job History](#)

[View the Log Files of a Job History](#)

VIEW JOB HISTORY DETAILS

Required Capability: See Capabilities and Permitted Actions

▶ To view the details of a job history:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then click job history.
2. From the Job History Filter dialog box, select the filter options that you want to apply and click **OK**.
3. From the Data Management Job History window, right-click the job whose job details you want to view, and then click **View Job Details**.
4. The Job Details dialog box appears, displaying detailed job history in General, Details, Phase Details and Attempts tabs for the selected job.
5. Click **OK**.



If viewing the details of a job with a pending or failed status, the **Reason for Job Delay** field will contain an Error Code, which, if clicked, will launch the customer support website displaying troubleshooting article(s) related to the specific issue.

VIEW THE ITEMS THAT FAILED FOR A DATA PROTECTION OPERATION



A listing of files and folders that failed is not available for the Quick Recovery Agent, nor the Image Level and Image Level ProxyHost iDataAgents. These agents do not perform a file level backup/copy.

▶ To view the list of items that failed for a data protection operation:

1. From the CommCell Browser, right-click the entity whose history of data protection operations you want to view, click **View**, and then click to view a job history.
2. From the Job History Filter dialog box, select the filter options, if any, that you want to apply, and then click **OK**.
3. From the Job History window, right-click the operation whose list of failed items you want to view, and then select **View Failed Items**. The **Unsuccessful Backup Files** window (for DataArchiver Agents, **Items On Which Archive Failed**) displays those items that failed. If no items failed, a message to that effect is displayed.

4. Click **Close**.
-

VIEW THE EVENTS OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

▶ To view the events associated with a job:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then click **Job History**.
 2. From the Job History Filter dialog box, select the filter options that you want to apply and click **OK**.
 3. From the Data Management Job History window, right-click the job whose job details you want to view, and then click **View Events**.
 4. The All Found Events window gets displayed. If no events were found for the backup, a message is displayed to that effect.
 5. Click **Close**.
-

VIEW THE LOG FILES OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

▶ To view the log files of a Job History:

1. From the CommCell Browser, right-click the entity whose job history you want to view, and then click to view a job history.
 2. From the job history filter window select the filter options, if any, that you want to apply, and then click **OK**.
 3. From the job history window, right-click the job whose log files you want to view, and then click **View Logs**.
 4. The contents of the log file related to the selected job history are displayed in the **Log File for Job n** window.
-

[Back to Top](#)

Recovery Point Copyback History

Topics | How To | Related Topics

You can view the Recovery Point copyback history of ContinuousDataReplicator. The **Job History Filter** dialog box allows you view detailed, historical information about job.

Once you have chosen your filter options, jobs that meet the criteria you selected are displayed in the **Job History** window. From this window you can right-click a job and view more detailed information such as the:

- Details of the Copyback job
- Events of the Copyback job
- Log files of the Copyback job
- Source Volume
- Destination Volume



The source and destination fields are not supported for Copyback history.

[Back to Top](#)

Recovery Point Copyback History - How To

Topics | How To | Related Topics

[View Job History Details](#)

[View the Items That Failed For a Data Protection Operation](#)

[View the Events of a Job History](#)

[View the Log Files of a Job History](#)

VIEW JOB HISTORY DETAILS

Required Capability: See Capabilities and Permitted Actions

▶ To view the details of a job history:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then click job history.
2. From the Job History Filter dialog box, select the filter options that you want to apply and click **OK**.
3. From the Data Management Job History window, right-click the job whose job details you want to view, and then click **View Job Details**.
4. The Job Details dialog box appears, displaying detailed job history in General, Details, Phase Details and Attempts tabs for the selected job.
5. Click **OK**.



If viewing the details of a job with a pending or failed status, the **Reason for Job Delay** field will contain an Error Code, which, if clicked, will launch the customer support website displaying troubleshooting article(s) related to the specific issue.

VIEW THE ITEMS THAT FAILED FOR A DATA PROTECTION OPERATION



A listing of files and folders that failed is not available for the Quick Recovery Agent, nor the Image Level and Image Level ProxyHost iDataAgents. These agents do not perform a file level backup/copy.

▶ To view the list of items that failed for a data protection operation:

1. From the CommCell Browser, right-click the entity whose history of data protection operations you want to view, click **View**, and then click to view a job history.

2. From the Job History Filter dialog box, select the filter options, if any, that you want to apply, and then click **OK**.
 3. From the Job History window, right-click the operation whose list of failed items you want to view, and then select **View Failed Items**. The **Unsuccessful Backup Files** window (for DataArchiver Agents, **Items On Which Archive Failed**) displays those items that failed. If no items failed, a message to that effect is displayed.
 4. Click **Close**.
-

VIEW THE EVENTS OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

▶ To view the events associated with a job:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then click **Job History**.
 2. From the Job History Filter dialog box, select the filter options that you want to apply and click **OK**.
 3. From the Data Management Job History window, right-click the job whose job details you want to view, and then click **View Events**.
 4. The All Found Events window gets displayed. If no events were found for the back up, a message is displayed to that effect.
 5. Click **Close**.
-

VIEW THE LOG FILES OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

▶ To view the log files of a Job History:

1. From the CommCell Browser, right-click the entity whose job history you want to view, and then click to view a job history.
 2. From the job history filter window select the filter options, if any, that you want to apply, and then click **OK**.
 3. From the job history window, right-click the job whose log files you want to view, and then click **View Logs**.
 4. The contents of the log file related to the selected job history are displayed in the **Log File for Job n** window.
-

[Back to Top](#)

QR Volume Creation History

Topics | How To | Related Topics

The **QR Volume Creation Job History Filter** dialog box allows you view detailed, historical information about quick recovery volume creation operations for the Quick Recovery Agent.

For information on Job Details displayed in the Job History, see [Viewing Job Information](#).

Once chosen, your filter options are then displayed in the QR Volume Creation Job History of QR Agent window. From this window you can view more detailed information such as the:

- Details of the QR volume creation job.
- Events of the QR volume creation job.
- Log files of the QR volume creation job.



After releasing a QR Volume, only the failed jobs will be retained in the job history.

QR Volume Creation History - How To

Topics | How To | Related Topics

[View QR Volume Creation Job History for the Quick Recovery Agent](#)

[View Job History Details](#)

[View the Events of a Job History](#)

[Viewing the Log Files of a Job History](#)

VIEW QR VOLUME CREATION JOB HISTORY FOR THE QUICK RECOVERY AGENT

▶ To view the job history of QR Volume Creation operations:

1. From the CommCell Browser, right-click an agent whose QR Volume Creation history you want to view, click **View**, then select **View Job History -> QR Volume Creation**.
2. From the QR Volume Creation Job History Filter, select the desired options and then click **OK**.
3. The system displays the options you selected in the QR Volume Creation Job History window.
4. Click **OK**.

VIEW JOB HISTORY DETAILS

Required Capability: See [Capabilities and Permitted Actions](#)

▶ To view the details of a job history:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then click job history.
2. From the Job History Filter dialog box, select the filter options that you want to apply and click **OK**.
3. From the Data Management Job History window, right-click the job whose job details you want to view, and then click **View Job Details**.
4. The Job Details dialog box appears, displaying detailed job history in General, Details, Phase Details and Attempts tabs for the selected job.
5. Click **OK**.



If viewing the details of a job with a pending or failed status, the **Reason for Job Delay** field will contain an Error Code, which, if clicked, will launch the customer support website displaying troubleshooting article(s) related to the specific issue.

VIEW THE EVENTS OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

▶ To view the events associated with a job:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then click **Job History**.
 2. From the Job History Filter dialog box, select the filter options that you want to apply and click **OK**.
 3. From the Data Management Job History window, right-click the job whose job details you want to view, and then click **View Events**.
 4. The All Found Events window gets displayed. If no events were found for the backup, a message is displayed to that effect.
 5. Click **Close**.
-

VIEW THE LOG FILES OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

▶ To view the log files of a Job History:

1. From the CommCell Browser, right-click the entity whose job history you want to view, and then click to view a job history.
 2. From the job history filter window select the filter options, if any, that you want to apply, and then click **OK**.
 3. From the job history window, right-click the job whose log files you want to view, and then click **View Logs**.
 4. The contents of the log file related to the selected job history are displayed in the **Log File for Job n** window.
-

[Back to Top](#)

QR Volume Recovery History

Topics | How To | Related Topics

The *Recovery History Filter for QR Agent* dialog box allows you to view detailed historical information about quick recovery jobs.

For information on Job Details displayed in the Job History, see *Viewing Job Information*.

Once your filter options are chosen, the Recovery Job History window displays the quick recovery jobs that meet the criteria you selected in the Recovery History Filter for QR Agent. From this window you can view more detailed information such as the:

- Details of the QR volume recovery or Copyback job
- Events of the QR volume recovery or Copyback job
- Log files of the QR volume recovery or Copyback job
- Source Volume
- Destination Volume



- The source and destination fields are not supported for Copyback history.
- After releasing a QR Volume, only the failed jobs will be retained in the job history.

QR Volume Recovery History - How To

Topics | How To | Related Topics

View QR Volume Creation Job History for the Quick Recovery Agent

View Job History Details

View the Events of a Job History

Viewing the Log Files of a Job History

VIEW QR VOLUME RECOVERY JOB HISTORY FOR THE QUICK RECOVERY AGENT

► To view the job history of QR Volume recovery operations:

1. From the CommCell Browser, right-click an agent whose QR Volume recovery history you want to view, click **View**, then click **Job History > QR Volume Recovery**.
2. From the QR Volume Recovery History Filter, select the desired options and then click **OK**.
3. The system displays the options you selected in the QR Volume Recovery Job History window.
4. Click **OK**.

VIEW JOB HISTORY DETAILS

Required Capability: See Capabilities and Permitted Actions

► To view the details of a job history:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then click job history.
2. From the Job History Filter dialog box, select the filter options that you want to apply and click **OK**.
3. From the Data Management Job History window, right-click the job whose job details you want to view, and then click **View Job Details**.
4. The Job Details dialog box appears, displaying detailed job history in General, Details, Phase Details and Attempts tabs for the selected job.
5. Click **OK**.



If viewing the details of a job with a pending or failed status, the **Reason for Job Delay** field will contain an Error Code, which, if clicked, will launch the customer support website displaying troubleshooting article(s) related to the specific issue.

VIEW THE EVENTS OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

▶ To view the events associated with a job:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then click **Job History**.
 2. From the Job History Filter dialog box, select the filter options that you want to apply and click **OK**.
 3. From the Data Management Job History window, right-click the job whose job details you want to view, and then click **View Events**.
 4. The All Found Events window gets displayed. If no events were found for the back up, a message is displayed to that effect.
 5. Click **Close**.
-

VIEW THE LOG FILES OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

▶ To view the log files of a Job History:

1. From the CommCell Browser, right-click the entity whose job history you want to view, and then click to view a job history.
 2. From the job history filter window select the filter options, if any, that you want to apply, and then click **OK**.
 3. From the job history window, right-click the job whose log files you want to view, and then click **View Logs**.
 4. The contents of the log file related to the selected job history are displayed in the **Log File for Job n** window.
-

[Back to Top](#)

Auxiliary Copy

[Topics](#) | [How To](#) | [Troubleshoot](#) | [How Do I](#) | [Support](#) | [Related Topics](#)

Overview

Auxiliary Copy with Synchronous and Selective Copies

- [Synchronous Copies](#)
- [Selective Copies](#)

Auxiliary Copy and Other Copy Features

- [Auxiliary Copy with Deferred Copies](#)
- [Auxiliary Copy and Spool Copies](#)
- [Auxiliary Copy and Inline Copies](#)
- [Auxiliary Copy and Parallel Copies](#)
- [Auxiliary Copy and Deduplication](#)
- [Auxiliary Copy With Combined Streams](#)

Auxiliary Copy with Multiple Stream Parallelism

- [Allow Maximum Number of Streams Option](#)
- [Limit to Number of Streams Option](#)

Auxiliary Copy with a Specified Source MediaAgent

Auxiliary Copy Operations

Sequence in Which Data is Copied During an Auxiliary Copy Operation

- [Change Job Priorities to Copy during Auxiliary Copy Operation](#)

Recovering Data From Copies

- [Browse/Restore/Recover from Copy Precedence](#)
- [Browsing From Copy Precedence Across Multiple Storage Policies](#)
- [Restoring Data from a Secondary Copy using a Third-Party Command Line](#)

Safeguarding Your Data Using Auxiliary Copy With Selective Copies

Skip Job on Read Errors During Auxiliary Copy

Auxiliary Copy Considerations

Customize Auxiliary Copy Operations through Registry Keys

Auxiliary Copy Encryption

Scheduling

Frequently Asked Questions

Best Practices

Related Alerts

Related Reports

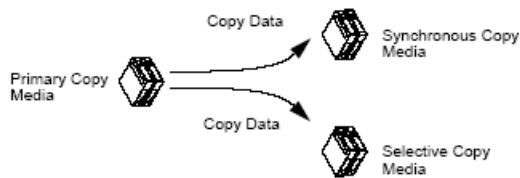
OVERVIEW

An auxiliary copy operation allows you to create secondary copies of data associated with data protection operations, independent of the original copy. For a full understanding, you should have some basic knowledge of storage policy and storage policy copy configurations. See [Storage Policies](#) and [Storage Policy Copies](#) for more information.

The auxiliary copy operation can be useful for creating additional standby copies of data. The primary and secondary copies use different media and often use different libraries, depending on the configuration. Should the primary copy become inoperative, perhaps due to a storage media failure, or a library or network malfunction, you can promote a synchronous copy to become the primary copy. This allows you to continue operations as before and make repairs without interrupting data protection and data recovery operations.

When an auxiliary copy operation is started, all valid data from a source copy is copied to all or one active secondary copies within the storage policy. A source copy can either be the primary copy (the default), or a secondary copy that has been selected as the source copy. The following figure illustrates a primary

copy as the source copy for an auxiliary copy operation:



- If the tape for a requested browse/data recovery operation is outside of a library, you will be prompted to manually input it into the library. The tape from a secondary copy will not be automatically used even if the data exists on the tape for the secondary copy.
- While performing Auxiliary Copy operations, priority is provided to perform the operation in a LAN-free environment.
- When auxiliary copy, data verification, and content indexing operations are initiated, they will all utilize the same single auxiliary copy manager process, thus reducing the load resources on the CommServe computer.

If a job is only partially copied, it can be recopied by using the **Re-Copy** feature. Doing this will re-copy all the chunks of the selected job from the beginning of the job. For more information, see [Re-Copy Fully or Partially Copied Jobs](#).

DISABLING AND ENABLING A BACKUP JOB FOR AUXILIARY COPY

You have the ability to disable a backup job for the auxiliary copy, i.e., once a job is disabled, it will not be copied during an Auxiliary Copy operation. Additionally, if selected, those jobs that are dependent on the selected disabled job will be disabled as well.

Things to consider before you disable a job:

- A job that has been disabled can still be restored/recovered.
- If a primary copy has a disabled job, and during a data recovery operation the software cannot find any data, data from the disabled job will be used.
- If you disable a backup of the last cycle that has occurred, this forces the next backup to be a full backup.
- For the Exchange Database and Image iDataAgents, if you disable an incremental or differential backup, all subsequent backups will be disabled up to the next full backup.

For step-by-step instructions, see [Disable/Enable a Job From a Storage Policy Copy](#).

AUXILIARY COPIES VS. STANDARD DATA PROTECTION OPERATIONS

An auxiliary copy should not be confused with a standard data protection operation. The two operations are unrelated, except, of course, that a data protection operation must precede an auxiliary copy. In all other ways the two operations are distinct and must be initiated or scheduled individually. A data protection operation is specific to a particular subclient, copying the subclient content from the client computer to the primary storage policy copy. An auxiliary copy, however, does not involve clients; instead, it copies backed up data from a source copy to one or more secondary copies. If you want the auxiliary copy operation to capture the data of only one subclient, then you must ensure that subclient has a dedicated storage policy.

AUXILIARY COPY AND HARDWARE COMPRESSION

Auxiliary copy does not manipulate software compression on the data. The data is transferred as it is. The hardware compression is transparent. Thus, hardware compressed data is uncompressed by the tape device on read, and recompressed during tape write.

AUXILIARY COPY AND MEDIA

If the media currently associated with your source copy is not readable or simply cannot be used, you can [Disable/Enable All Jobs Associated with a Media](#) so that all jobs associated with this media will be skipped during auxiliary copy operations.

If the media associated with the secondary storage policy copy becomes unreadable, you can [Re-Copy all Jobs Associated with a Media](#). This will recopy all the jobs associated with the specific media.

AUXILIARY COPY WITH SYNCHRONOUS AND SELECTIVE COPIES

An auxiliary copy operation copies valid data from a source copy of a specific storage policy to all or one active secondary copy within a storage policy. Data from source copies are not copied over to inactive secondary copies.

These secondary copies can be either synchronous or selective copies. The following sections describe how data is copied during an auxiliary copy job on both types of copies.

SYNCHRONOUS COPIES

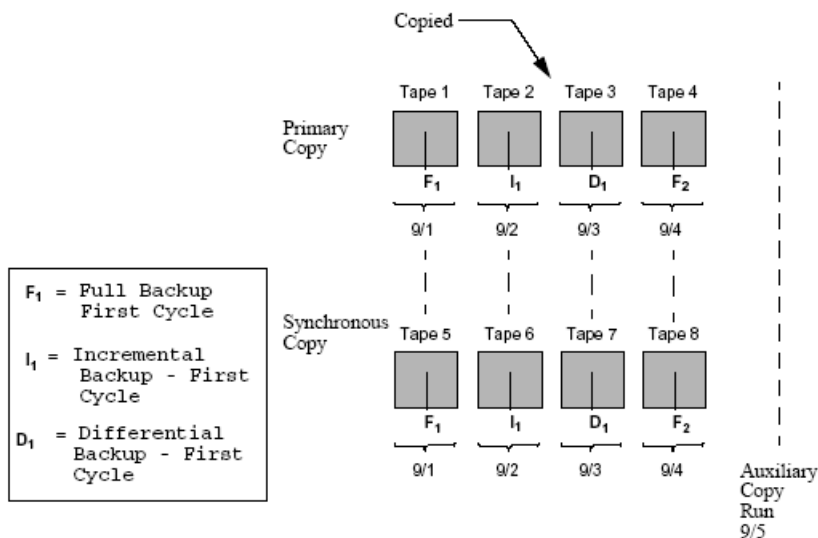
The auxiliary copy operation will copy full, incremental, and differential backup data from a source copy to other synchronous copies based on the [All Backups](#) option or the [Backups On And After](#) date you selected from the [Copy Policy](#) tab of the [Copy Properties](#) dialog box.

If a primary copy has the Spool Copy (no retention) option enabled, and there is no coverage for all of the subclients in the secondary copies, the synchronous copy cannot be deleted. Instead, users will be prompted with a message to change the retention period of the primary copy or create another synchronous copy.

ALL BACKUPS OPTION

If you select the All Backups option when creating a synchronous copy, all data protection operations on a source copy will be copied to the synchronous copy.

In the following example, if an auxiliary copy is run on 9/5, F₁, I₁, D₁, and F₂ will be copied to the synchronous copy. The source copy for the operation is the primary copy.



When the All Backups option is selected, all data protection operations on a source copy will be copied to the synchronous copy.

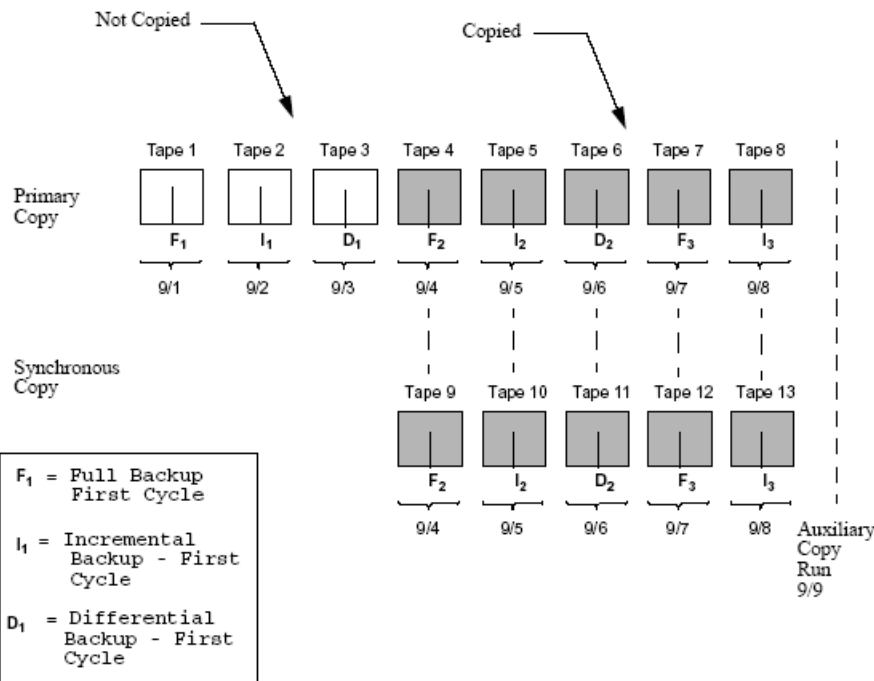
When auxiliary copies are run on storage policies used by DataArchiver Agents, all archiving operations will be copied, regardless if a new Index exists.

BACKUPS ON AND AFTER OPTION

If you select a date from the Backups On and After field, then all data protection operations on or after the date you select, starting from 12:00 A.M., will be copied to the synchronous copy. This option is useful if you do not want all the data protection operations of a source copy to be copied to the synchronous copy.

Note that the date entered can be on, before, or after the current CommServe date. When the date entered is after the current CommServe date, jobs (up to the date specified) that are to be copied, as well as partially copied jobs will be disabled for copy. If no date is entered, all backup data will be copied from the primary copy to the secondary copy.

In the following example, the Backups On and After date was set to 9/4. All data protection operations starting from 9/4 are copied to the synchronous copy when an auxiliary copy operation is run on 9/9. All data protection operations prior to 9/4 are not copied.



When you enter a date that is earlier than (before) the date already specified, all data protection operations after the date specified or after the first copied/selected job, whichever is later, will be copied to the secondary copy.

For example, let's assume the current date is January 1, 2009, and you created a storage policy copy with the **Backups On and After** option set to January 1, 2010. This would indicate that all jobs up to January 1, 2010 would be disabled for copy. With this, you manually pick a job for copy on May 1, 2009. On June 1, 2009, you revise the Storage Policy Copy **Backups On and After** option to be January 1, 2009. This will automatically select all jobs that are run after May 1, 2009 (the first copied job), for auxiliary copy. Any jobs that were run before May 1, 2009 would not be copied (in this scenario). To copy job(s) from any date before May 1, 2009, manually select the job(s) for copy. If you had not selected any job manually and modified the **Backups On and After** to January 1, 2009, all jobs from January 1, 2009 to current date would have been picked up for auxiliary copy.

SELECTIVE COPIES

Selective copies only contain full backup data that has occurred on or after a specified date and are copied based on the following selective criteria:

- **Automatically select Full Backups** (all).
- **Automatically select Full Backups** (weekly, monthly, quarterly, half yearly, or yearly). This is a **time-based** Selective copy.
- **Do not Automatically select jobs**

The selective copy type can be selected from the **Selective Copy** tab of the **Copy Properties** dialog box. Once you set the **Backups On and After** date from the **Copy Properties** dialog box, then all data protection operations starting on or after the date you select (starting from 12:00 A.M.) will be copied to the selective copy, based on the selective copy type.

ALL FULLS BACKUPS

If a selective copy is defined as an **All Full Backups** copy, all full backups associated with the storage policy are copied to the selective copy.

TIME BASED SELECTIVE COPY

If a selective copy is defined as time based, an auxiliary copy operation copies the first or last full backup of a time period based on the following parameters:

- Weekly** The first or last full backup of a specified starting day of a week will be copied from 12:00 A.M. of that day up to 11:59 P.M. on the last day of that week.
- Monthly** The first or last full backup of a specified starting day of a month will be copied from 12:00 A.M. on that day up to 11:59 P.M. on the last day of that month.
- Quarterly** The first or last full backup of the first day of a quarter will be copied from 12:00 A.M. on that day up to 11:59 P.M. on the last day of that quarter.
- Half Yearly** The first or last full backup of the first day of a half year will be copied from 12:00 A.M. on that day up to 11:59 P.M. on the last day of that half year.
- Yearly** The first or last full backup of the first day of a year will be copied from 12:00 A.M. on that day up to 11:59 P.M. on the last day of that year.
- Advanced** This option allows you to select the First or Last full backup performed after a specific time period. The time period can be specified in cycles/days/weeks/months.

Note that for cycle based criteria, the copy selection is based on the mod logic. For more information, see **For Selective Copy, how does the job selection work with Advanced - cycle based criteria?**

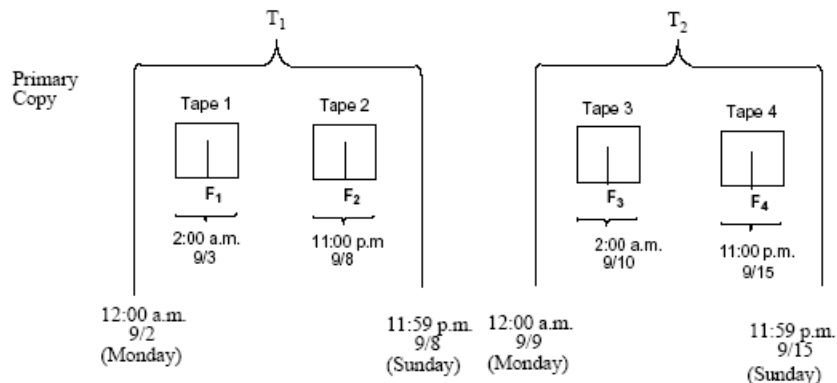
A backup job will be selected based on its start time. For example: If a backup job starts at 11:55 pm on August 31st and ends at 1 am on September 1st,

then it will be selected as the last full backup for the month of August.

Selective storage policy copies associated with custom calendars will have data copied during auxiliary copy operations monthly, quarterly, half yearly, or yearly based on the days defined in the calendar. See Custom Calendar for more information.

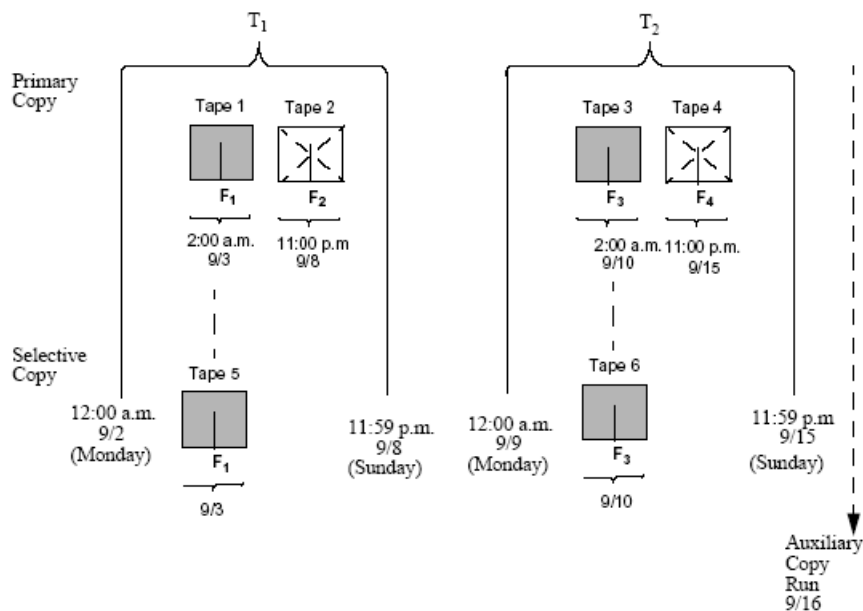
Example

The following example illustrates the time interval of a primary copy with four full backups that were run across two weekly time intervals, T_1 and T_2 , every one week starting on Monday.



In the following example, a time based selective copy was specified as every one week starting on Monday, with the First full backup option enabled on the copy. Data protection operations were run across two time intervals on the primary copy, T_1 and T_2 .

If an auxiliary copy operation is run on Monday 9/16, the first full backup within each weekly time interval (F₁ and F₃) will be copied to the selective copy.



If the Last full backup option is enabled on the copy instead of the First full backup option, then F₂ and F₄ will be copied instead of F₁ and F₃.

DO NOT AUTOMATICALLY SELECT JOBS

If a selective copy is defined as a Do Not Automatically Select Jobs copy no backups will be copied to this copy unless they are manually selected for copy from the Job for Storage Policy Copy dialog box or the **Select most recent full backup when auxiliary copy starts** option has been selected from the Auxiliary Copy Options dialog box.

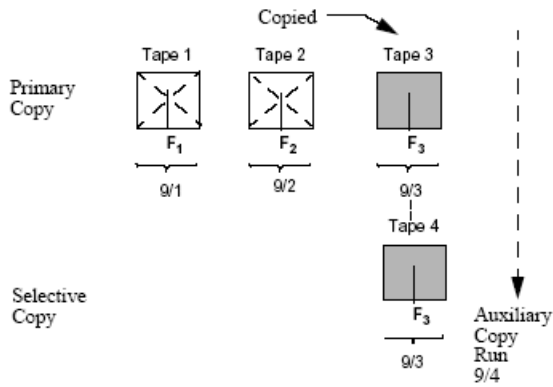
MANUALLY SELECT FULL BACKUPS

You can manually select a backup to be copied to a selective copy from the Backups for Copy window of the selective copy. See Manually Select a Backup To be Copied to a Selective Copy for more information.

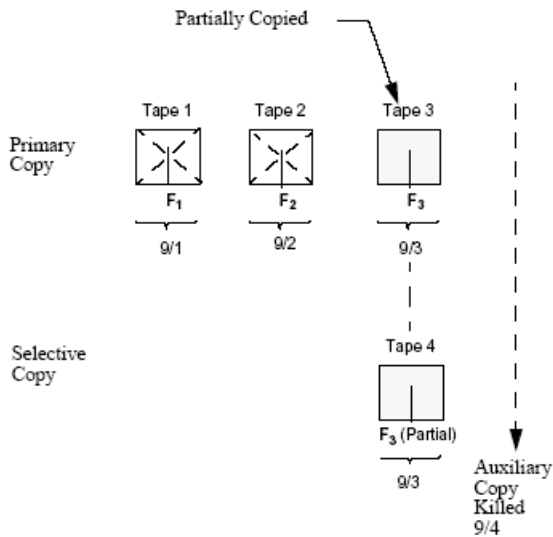
MOST RECENT FULL BACKUP SELECTIVE COPY

If you enable the **Select Most Recent Full Backup when Auxiliary Copy Starts** option when you initiate the auxiliary copy operation in the Auxiliary Copy (Options) dialog box, by default, when the auxiliary copy starts, the most recent full backup of each subclient, including those partially copied, and the previously selected full backup for each subclient will be copied.

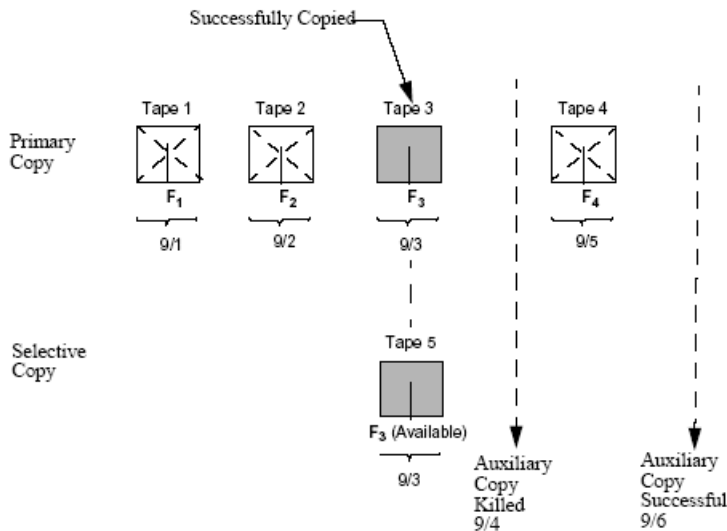
In the following example, three full backups are on the primary copy, F_1 , F_2 , and F_3 . When an Auxiliary Copy is run on 9/4, F_3 will be copied because it is the most recent full backup.



In another example, if the same auxiliary copy is run on 9/4, but is killed before it is completely copied, F_3 may only be partially copied or selected for copy.



If another full backup (F_4) occurs on 9/5, and an auxiliary copy is run on 9/6, the partially copied full backup F_3 as well as F_4 will be copied. If while configuring the Auxiliary Copy Job, you disable the **Select Most Recent Full Backup When Auxiliary Copy Starts** option in the Auxiliary Copy (Options) dialog box, only the previously selected backup will be copied, thus F_4 would not be copied.

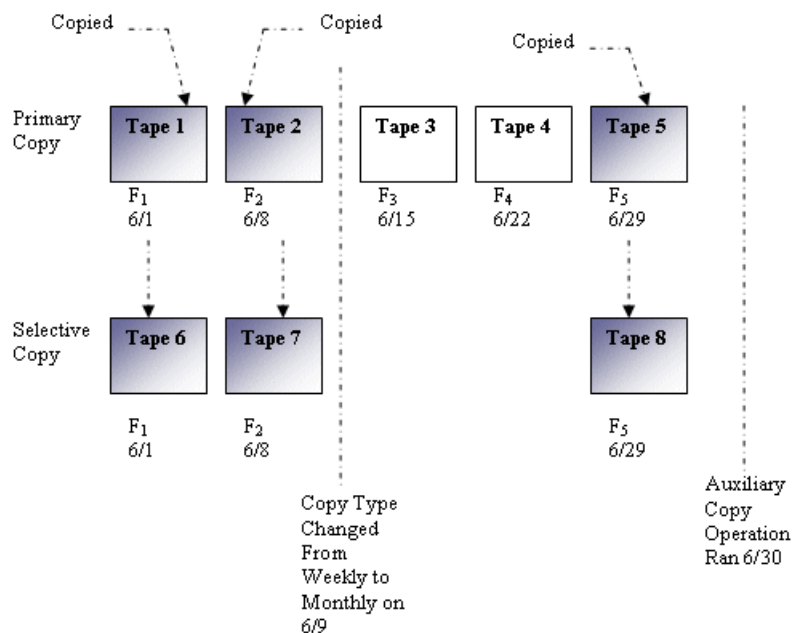


CHANGING THE SELECTIVE COPY TYPE OR SELECTIVE CRITERIA

If you change the selective copy type or selective criteria and then run an auxiliary copy operation, the auxiliary copy operation will copy the data based on the old and new selective copy criteria.

In the following example, on 6/9 the criteria of a selective copy was changed from being weekly based to monthly based.

If an auxiliary copy is run on 6/30, F_1 and F_2 are copied because they meet the weekly based criteria. F_5 is also copied because it meets the monthly based criteria.



AUXILIARY COPY AND OTHER COPY FEATURES

The section describes how auxiliary copy is performed on copies that have other copy features enabled, such as:

- Combined Streams
- Inline Copy
- Deferred Copy

AUXILIARY COPY WITH DEFERRED COPIES

An auxiliary copy operation on a copy that has the `Defer Auxiliary Copy for <n> day(s)` option enabled, data will be copied starting at 12:01 A.M. on the set number of days after valid data becomes available on the source copy. See [Deferred Copy](#) for an overview.

AUXILIARY COPY AND SPOOL COPIES

An auxiliary copy must be performed on a primary copy that has the `Spool Copy (no retention)` option enabled, before data on that copy can be pruned the next time data aging is run. It is recommended that regular or automatic auxiliary copy operations are performed for storage policies using spool copies. See [Spool Copy](#) for an overview.

Spool Copy data are aged upon the successful completion of the auxiliary copy job. If a primary copy has the `Spool Copy (no retention)` option enabled, and there is no coverage for all of the subclients in the secondary copies, the synchronous copy cannot be deleted. Instead, users will be prompted with a message to change the retention period of the primary copy or create another synchronous copy.

AUXILIARY COPY AND INLINE COPIES

If a data protection operation of a subclient whose storage policy has an inline copy enabled does not successfully create an Inline Copy, then the data will be copied to a secondary copy the next time an auxiliary copy is run. See [Inline Copy](#) for an overview.

AUXILIARY COPY AND PARALLEL COPIES

If storage policy copies are configured with an auxiliary parallel copy, after reading the source copy (only once) data can be copied to multiple secondary copies concurrently rather than sequentially. This optimizes use of media, therefore, decreases the time needed to run auxiliary copy operations. For more information, see [Parallel Copy](#).

AUXILIARY COPY AND DEDUPLICATION

If a secondary storage policy copy is enabled with deduplication, then the deduplication store gets created for the copy and the associated data is deduplicated for that copy. See Deduplication for an overview.

- Data in a storage policy copy enabled for Deduplication can not be multiplexed. Therefore, Data Multiplexing is not supported if the storage policy copy is enabled with Deduplication. However, a SILO copy supports Data Multiplexing even if the storage policy copy is enabled with Deduplication.
- Multiplexed data cannot be copied to a storage policy copy enabled for Deduplication. Therefore, a storage policy copy enabled for Deduplication can not have a direct or indirect source copy enabled for Data Multiplexing.
- An Auxiliary Copy can be configured with Data Multiplexing when the source copy is enabled for Deduplication.

For more information, see Data Multiplexing.

DASH COPIES

When both primary copy and secondary copy are deduplicated, you can reduce the copy duration using the DASH Copy feature on the source computer while creating secondary copies. To optimize the disk read operations, enable the **Disk Read Optimized Copy**.

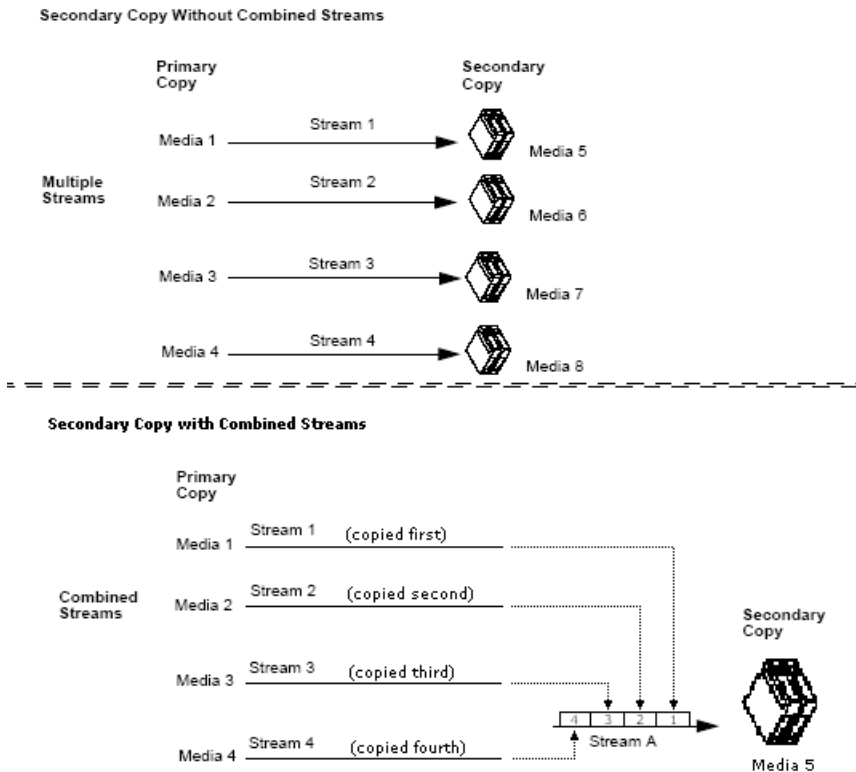
If you wish to process the signature on the source, to see if the signature is present on the target, and if present, send only the signature, you can enable **Network Read Optimized Copy**.

For more information, see DASH Copy.

AUXILIARY COPY WITH COMBINED STREAMS

Auxiliary Copy normally copies data stream by stream, meaning, if there were four data streams on the primary copy, then the auxiliary copy operation would use four data streams to copy on the secondary copy. Alternatively, auxiliary copy can copy data from a primary copy that has multiple streams to a secondary copy that has less than that number of streams, by using the `Combined to <n> Streams` option on the copy.

By combining the data streams to less media, this improves media usage as the media storage is optimized. Media recycling is also more efficient, as data aging is more effective as secondary copies of the data reside on less media than what was required for the original data protection operation. The following example illustrates an auxiliary copy operation performed for a copy that combined data streams into one stream:

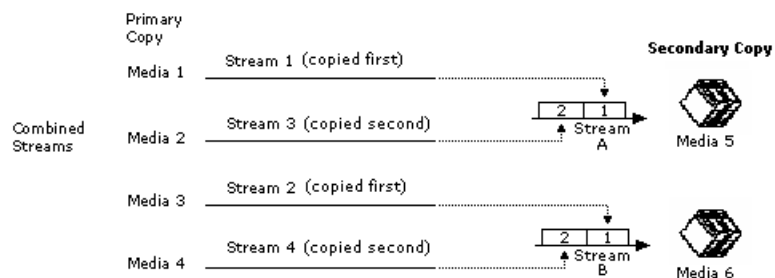


Multi-stream backups of the Microsoft SQL, DB2, DB2 DPF and Sybase agents will be copied during an auxiliary copy operation to a copy that combines streams; however, restore operations may have limitations. See Browse and Restore for more information.

In order to restore SQL, DB2, DB2 DPF and Sybase agent backups from combined streams of Storage Policy copies, a new Storage Policy copy to disk library must be created and an auxiliary copy should be executed. A restore must be performed from this new copy.

The following example illustrates an auxiliary copy operation performed for a copy that combined data streams into two streams:

Secondary Copy With Combined Streams

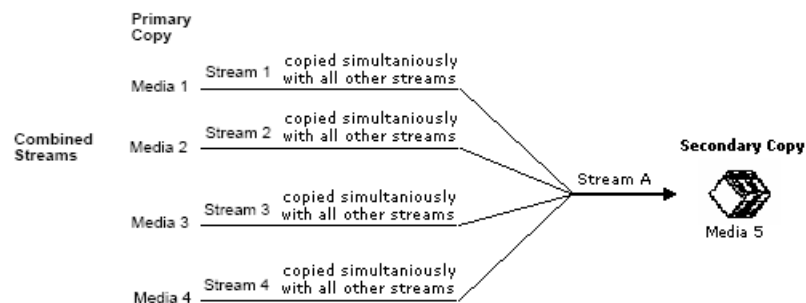


Data Multiplexing

When a copy is configured to combine streams, thereby utilizing less media when copying data to a secondary copy, multiplexing can be enabled as well. Data Multiplexing allows data protection operations of multiple data streams to be run concurrently to the same media, which optimizes performance of the auxiliary copy operation in a disk environment.

The following example illustrates an auxiliary copy operation performed for a copy that combined data streams into one stream with multiplexing enabled:

Secondary Copy with Combined Streams - Multiplexing Enabled



For more information, see:

- Combine the Data Streams of a Storage Policy Copy
- Enable Multiplexing for a Storage Policy Copy with Combined Data Streams
 - Data in a storage policy copy enabled for Deduplication can not be multiplexed. Therefore, Data Multiplexing is not supported if the storage policy copy is enabled with Deduplication. However, a SILO copy supports Data Multiplexing even if the storage policy copy is enabled with Deduplication.
 - Multiplexed data cannot be copied to a storage policy copy enabled for Deduplication. Therefore, a storage policy copy enabled for Deduplication can not have a direct or indirect source copy enabled for Data Multiplexing.
 - An Auxiliary Copy can be configured with Data Multiplexing when the source copy is enabled for Deduplication.

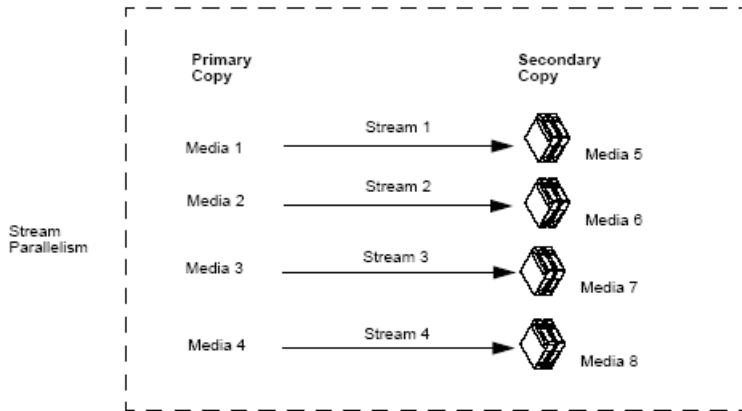
AUXILIARY COPY WITH MULTIPLE STREAM PARALLELISM

You can select the number of data streams to be copied at the same time during an auxiliary copy operation. This can be achieved by using the maximum number of available streams or from a specified number of streams.

ALLOW MAXIMUM NUMBER OF STREAMS OPTION

If enough storage resources are available, you can use the `Allow Maximum` option so that all data streams are copied concurrently during an auxiliary copy operation.

For example, if four streams were required for the auxiliary copy job, then all four streams will be copied in parallel.



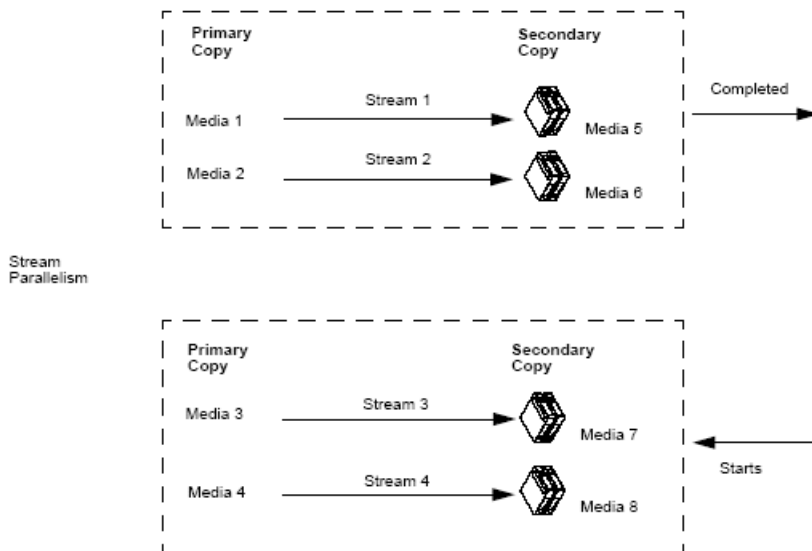
Data balancing occurs across multiple streams so that an auxiliary copy will continue to copy in parallel. Note that multiple streams will not be copied in parallel to a copy that combines streams.

- If an auxiliary copy is configured to copy with parallel streams, and the associated storage policy copy is configured with combined streams, the auxiliary copy operation will attempt to use no more than the number of streams defined in the storage policy copy's *Combined to n streams* field.
- Auxiliary Copy operations only use streams to perform copies of jobs with a "to be copied" status. Therefore, all available streams may not be used when performing an auxiliary copy.

LIMIT TO NUMBER OF STREAMS OPTION

If not enough storage resources are available, or you do not want to use all available resources, you can select the number of data streams that will be copied at the same time during an auxiliary copy operation.

For example, if four streams were required for the auxiliary copy job, and two streams are selected to copy in parallel, then the auxiliary copy operation will copy two streams at a time. Note that Stream 3 will start when Stream 1 or Stream 2 is completed. Hence, Stream 3 does not have to wait for both Stream 1 and Stream 2 to complete before starting.



STREAM RANDOMIZATION

When a storage policy is configured to use more than one data stream, it is important that the data streams are equally used; parallel copying using multiple source and destination drives may not be effective if the data is concentrated in one stream. The stream randomization feature enables random choosing of the data streams, increasing the rate of data transfer by copying data from different streams in parallel. See [Enable Stream Randomization](#) for instructions.

Also, it is recommended that you configure the tuning parameters to evenly distribute the data across all the streams. You can specify the interval to check the data size in the streams and the threshold to decide data distribution among the streams. See [Tune Stream Randomization](#) for instructions.

AUXILIARY COPY WITH A SPECIFIED SOURCE MEDIAAGENT

An auxiliary copy operation copies valid data from a specified source copy of a specific storage policy to all or one active secondary copy within a storage policy. If the source copy for the auxiliary copy operation is configured with a shared library, you will have the ability to select the source MediaAgent from which the auxiliary copy operation will read the data.

- All configured MediaAgents are displayed as options for the source MediaAgent. If an invalid MediaAgent is selected as the source for the copy, i.e., the source copy is not configured with the selected MediaAgent, the auxiliary copy operation will not produce the corresponding secondary copy, and the job may fail. Therefore, if the source copy for the auxiliary copy operation is not configured with a shared library, do not select a source MediaAgent for the operation; leave the field blank.
- An auxiliary copy operation configured with a source MediaAgent cannot be included in a **Schedule Policy** or the **Save As Script** feature.

For step-by-step instructions, see [Select a Source MediaAgent for an Auxiliary Copy Operation](#).

AUXILIARY COPY OPERATIONS

You can start or schedule an auxiliary copy at the storage policy level from the Auxiliary Copy (Options) dialog box.

From this dialog box, you can:

- Select the Source MediaAgent from which this auxiliary copy operation will be performed. (Only if source copy is configured with a shared library.)
- Copy the data to all secondary copies.
- Copy the data to a specific secondary copy.
- Start new media for all secondary copies.
- Mark a media full after a successful operation.
- Select a number of streams to copy in parallel.
- Select vault tracking, change priority, start suspended.
- Specify Job Running Time, and Job Restart interval options. (You can also specify the maximum number of allowed restart attempts and the interval between restart attempts for all auxiliary copy jobs. For procedures, see [Specify Job Restartability for the CommCell.](#))

Additionally, from the Auxiliary Copy (Job Initiation) dialog box, you can schedule the auxiliary copy operations that you configured.

From this dialog box, you can:

- Run the auxiliary copy operation immediately.
- Schedule the auxiliary copy operations via the Schedule Details dialog box.
- Save the operation as a script.
- Set an Automatic Copy schedule: The auxiliary copy operation will be performed every 30 minutes, unless another interval has been specified. See [Automatic Copy](#) for more information.
- Configure an alert for the operation.

SEQUENCE IN WHICH DATA IS COPIED DURING AN AUXILIARY COPY OPERATION

Data is copied to secondary copies during auxiliary copy operations according to the media of the original data protection operations, per destination copy and data stream. More specifically, the media that contains the oldest job is copied first. From this media, jobs from the primary copy are copied sequentially from oldest to newest so that all jobs from this media are copied before unmounting it. Once all the jobs are copied from this media, auxiliary copy will continue with the next media containing the oldest job within the same drive pool. When all the media in this drive pool are copied, auxiliary copy will start copying the oldest media of the other drive pools that belong to the same library. When all the media in this library are copied, auxiliary copy will continue copying the oldest media of the other libraries for the same MediaAgent. When all the media of this MediaAgent is copied, auxiliary copy will start copying the oldest media of other MediaAgents. Upon completion, if there is more than one stream, auxiliary copy will continue copying on the next stream in the same manner. Therefore, data is copied in the following sequence:

- Media
For example, J₁ and J₂ used media M₁. J₃ and J₄ used media M₂. J₁ and J₂ are copied first, and then J₃ and J₄.
- Drive Pool
For example, J₁, J₂, J₃ and J₄ used drive pool D₁. J₅, J₆, J₇ and J₈ used drive pool D₂. J₁, J₂, J₃ and J₄ are copied first grouped by media and volume. J₅, J₆, J₇ and J₈ are copied second.
- Library
For example, J₁ and J₃ used library L₁, and J₂ and J₄ used library L₂. J₁ and J₃ are copied first grouped by media and volume. J₂ and J₄ are copied second.
- MediaAgent

For example, J₁, J₂, J₃, J₄, J₅, J₆, J₇, and J₈ use MediaAgent MA₁. J₉, J₁₀, J₁₁, J₁₂, J₁₃, J₁₄, J₁₅, and J₁₆ use MediaAgent MA₂. J₁ through J₈ are copied first grouped by media, volume, and drive pool. J₉ through J₁₆ are copied second.

See View the Media Not Copied for step-by-step instructions.

CHANGE JOB PRIORITIES TO COPY DURING AUXILIARY COPY OPERATION

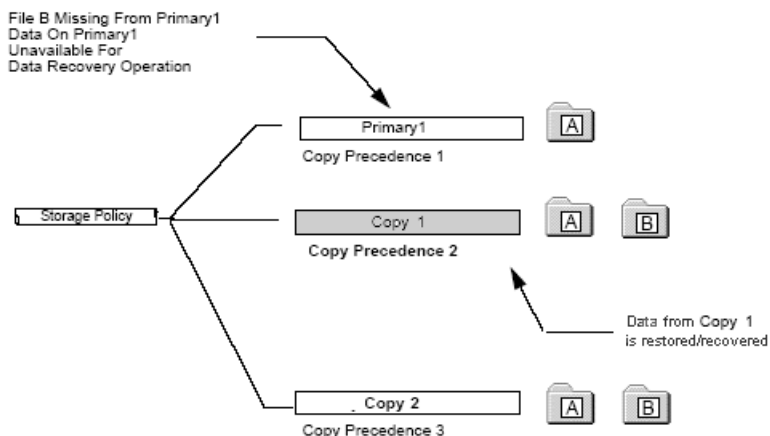
When Auxiliary Copy operation is performed, jobs (data) from primary copy to secondary copy are copied sequentially from oldest to newest jobs. During this process, you can set the priorities for jobs to be copied to secondary storage. See Set Job Priorities to Copy during Auxiliary Copy operation for step-by-step instruction.

RECOVERING DATA FROM COPIES

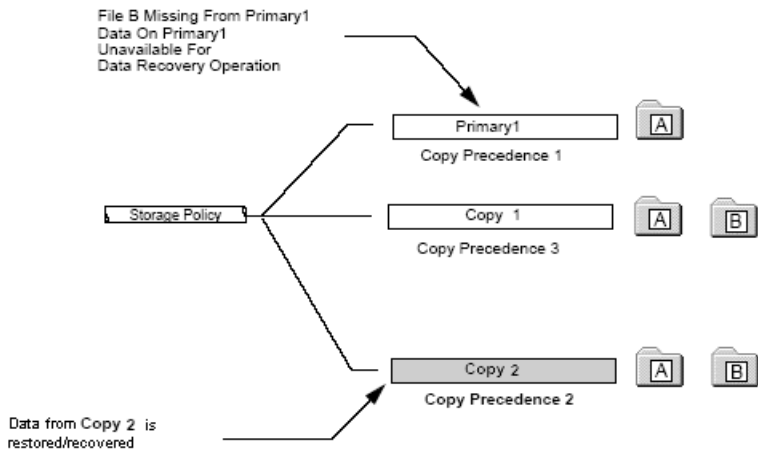
By default, when a browse or data recovery operation is requested (without specifying copy precedence), the software attempts to browse/restore/recover from the storage policy copy with the lowest copy precedence. If the media for the copy with the lowest precedence is offsite, damaged, or if hardware resources are unavailable, then a specific storage policy copy must be specified in the Copy Precedence tab of the **Storage Policy Properties** dialog box. For more information, see Change the Copy Precedence.

If the data that you want to browse/restore/recover was already pruned from that copy, the software will search for the requested data from a copy with the lowest copy precedence number to copy with the highest copy precedence number.

In the following example, a storage policy includes three copies, a primary copy (with copy precedence 1) and two additional copies. If File B is unavailable from the primary copy, then, when performing a data recovery operation, data will automatically be restored/ recovered from Copy₁ that has a copy precedence of 2.



If, however, the copy precedence of the two copies was changed so that Copy 1 has a copy precedence of 3 and Copy 2 has a copy precedence of 2, then the data recovery operation will be performed from data obtained from Copy 2 that has a copy precedence of 2.



BROWSE/RESTORE/RECOVER FROM COPY PRECEDENCE

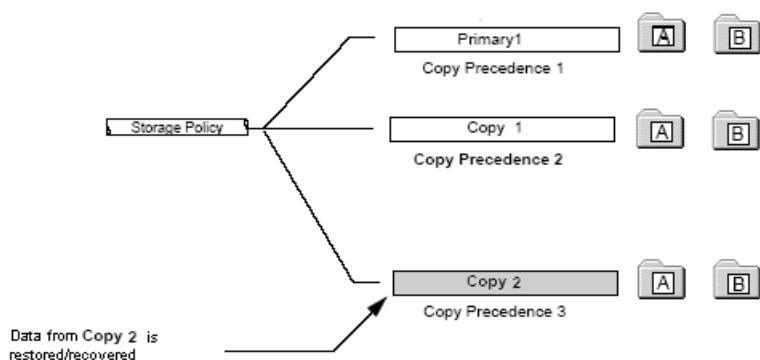
When a copy is configured, the system automatically assigns it a copy precedence number, which you can change at any time.

If you specify a copy precedence number for a data recovery operation, the software searches only the storage policy copy with that precedence number in each of the storage policies through which the data was secured. If data does not exist in the specified copy, the data recovery operation fails even if the data exists in another copy of the same storage policy.

Copy precedence is useful if:

- The primary copy is no longer available for a data recovery operation due to a hardware failure.
- You know that the media containing the data from data protection operations for a particular copy have been removed from the storage library. In this case, you can choose to browse/restore/recover from a copy whose media are inside the library.
- You want to browse/restore/recover from a selective copy.
- You want to browse/restore/recover from a copy that accesses faster disk media rather than slower tape media.
- You know that the media drives used by a particular copy are busy with another operation and want to browse/restore/recover from a different copy to avoid resource conflicts.

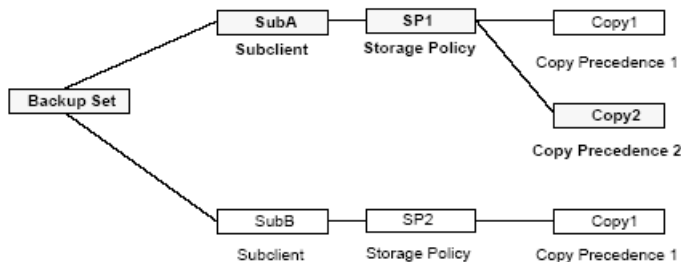
In the following example, a storage policy has a primary copy, Primary1, two copies, Copy 1, and Copy 2. If you choose to browse/restore/recover your data from Copy 2, you must specify that you want to browse/restore/recover from copy precedence 3 so that data will be restored/recovered from that copy.



BROWSING FROM COPY PRECEDENCE ACROSS MULTIPLE STORAGE POLICIES

When you browse at the client, agent, or backup set levels, keep in mind that the data for the subclients included in these levels may have been secured through more than one storage policy. If you specify a copy precedence for a data recovery operation, the data is restored/recovered from the storage policy that has data on the specified copy.

For example, data is restored/recovered at the backup set level that has two subclients, SubA and SubB. SubA uses storage policy SP1 and SubB uses storage policy SP2. SP1 has two copies, Copy1 and Copy2. Copy1 has a copy precedence of 1, and Copy2 has a copy precedence of 2. If copy precedence 2 was selected for the data recovery operation, only data from SubA will be restored/recovered.



RESTORING DATA FROM A SECONDARY COPY USING A THIRD-PARTY COMMAND LINE

The Oracle, SAP for Oracle, and SAP for MAXDB iDataAgents provide the capability of restoring data from secondary copies using a third-party command line, such as RMAN and the SAP command line. Using a third-party command line for this operation provides an alternative to the CommCell Console, and is useful for restoring data when the primary copy is unavailable. To utilize this feature, some minor setup configuration is required depending on the agent, as described briefly below:

- For Oracle, the setup involves adding the `PARMS="ENV=(CV_restCopyPrec=2)"` parameter statement into the RMAN restore script.
- For SAP for Oracle or SAP for MAXDB, the setup consists of adding the `CV_restCopyPrec` parameter followed by the copy precedence number 2 into the

parameter file prior to running the restore.

See [Restore Data from a Secondary Copy using a Third-Party Command Line](#) for step-by-step instructions.

SAFEGUARDING YOUR DATA USING AUXILIARY COPY WITH SELECTIVE COPIES

You can use the Auxiliary Copy feature to copy your data to selective copies, and then use the Export Media option to keep these copies of your data in a safe offsite location. By defining your selective copy to contain one full backup in a three month period, and by using the `Export Media` option, you can guarantee that you can keep a secondary copy of full backup data every three months in a safe location. This provides for extra protection in the event of data loss.

To accomplish this:

- Create a Selective Copy
- Schedule an Auxiliary Copy

To guarantee that data will be copied to the selective copy you have defined, create an Auxiliary Copy schedule. This schedule will dictate when the full backup(s) will be copied from the primary copy to the selective copy media. If resources permit, create a schedule to run every day, for example, every day at 9:00 A.M. New, eligible full backups will be copied when the Auxiliary Copy operation is run. No drive resources will be used if no eligible full backups have occurred since the last Auxiliary Copy was performed for the Storage Policy.

- Perform an Export Media Operation Using Vault Tracker

Once you have copied your data to selective copies using auxiliary copy operations, you can now export your media to keep it in a safe offsite location.

- Perform a Manual Export Based on a Report

If you want to take the tapes out manually (either by opening the library door or through selecting a list), run the `Media Information` report. Based on the report, (which you can run at the same frequency and options as above) the tapes may be manually exported.

SKIP JOB ON READ ERRORS DURING AUXILIARY COPY

The **Skip job on read errors during Auxiliary copy** option specifies whether the Auxiliary Copy job will skip data protection jobs that encounter errors during auxiliary copy operations. If you have many data protection jobs that need to be copied, this option will allow the auxiliary copy job to continue copying other data protection operations while skipping over those jobs encountering errors. This option is enabled by default. However, if you disable the option and the Auxiliary Copy job encounters an error, it will return with a Pending status and not continue. The **Skip job on read errors during Auxiliary copy** option can be modified from the Media Management Configuration (Auxiliary Copy Configuration) dialog box available in the Control Panel. If you continue to encounter errors, contact your software provider.

Pending reasons are displayed in the **Reason for Job delay** field, which is located in the Administration Job Details (General) tab.

For more information regarding the effects if an error is encountered during auxiliary copy operations, please refer to the following table.

If The Following Error Occurs	Then
Source Media Error/Source Media Not Available	The auxiliary copy job will continue copying other data protection jobs while skipping over that media. Upon completion of all jobs that need to be copied, the jobs on the skipped media will be attempted to be copied again. Note that when it skips the media "â€" it skips all the jobs on that media. If the first source media is not available, wait.
Read Error	The auxiliary copy job will continue copying data protection jobs while skipping over the portion of the job with the read errors. Upon completion of all jobs that need to be copied, the skipped portions will be attempted to be copied again.
Target Media Mount Error	The auxiliary copy job will retry the operation. If error still exists, the job will go into Pending state.

AUXILIARY COPY CONSIDERATIONS

- Software compressed data is not uncompressed during an auxiliary copy operation.
- If you disable a data protection operation associated with a primary copy, that backup will not be copied during an Auxiliary Copy operation.
- Once started, if an auxiliary copy job cannot be completed, the Job Manager will retry the job up to a total of two days at 20-minute intervals for a maximum of 144 times.
- Multiple streams will not be copied in parallel to a copy that combines streams.
- To avoid possible media contention, which can affect performance, it is recommended that you do not start an auxiliary copy operation if the selected storage policy is already being used by a data protection or data recovery operation. To determine the jobs scheduled for a storage policy:
 - Identify the storage policy associated with a job, see the Storage Policy column of the Job Controller.
 - To view a list of jobs scheduled in the CommServe, click the CommServe icon or a specific storage policy, then select **View Schedules**.

- When defining the rules for a selective copy in the Copy Properties (Selective Copy) dialog box, it is recommended to select the **Select Full Backups at frequency** option. Selecting the **Copy most recent full backups when Auxiliary Copy starts** option will copy the most recent full backup of each subclient, including those partially copied, and the previously selected full backup for each subclient. For more information, see Most Recent Full Backup Selective Copy.
- The amount of data transferred for an Auxiliary Copy job is updated every 512 MB or when a data chunk is closed. The progress for the entire job is displayed on the Administration Job Details (General) tab, and the per copy progress is displayed on the Auxiliary Copy Job Details (Streams) tab. The data chunk size can be changed from the Media Management Configuration (Chunk Size) or storage policy copy's Data Path Properties dialog boxes.
- The priority of an auxiliary copy job can be changed using the Change Job Priority feature.
- Data paths can be added to secondary copies to enable LAN free Auxiliary Copy operations, so that network resources can be freed wherever possible. For more information, see Configuring Alternate Data Paths for Secondary Copies.
- An excessive number of concurrent read/writes may affect performance. For a single disk, a maximum of two (2) concurrent I/O streams is recommended. For a RAID 5 volume, a maximum of five (5) concurrent I/O streams is recommended.
- If the source copy is disk and managed by a Windows MediaAgent, enable the **Use Unbuffered I/O** option for each mount path. Use of unbuffered I/O can significantly improve performance. For more information, see Administering Mount Paths.
- If the default data path on the primary copy of a storage policy points to a drive pool configured on a MediaAgent enabled with NDMP Remote Server (NRS), then the secondary copy must also point to a drive pool configured on a MediaAgent with NRS installed in order to restore the data to a NAS file server.
- Only for EMC Celerra 5.5 must the library be directly attached to the Celerra file server. For EMC Celerra 5.6 or higher, when a Celerra file server is backed up using the Volume-Based Backup option, three-way backups, three-way restores, and NDMP Remote Server (NRS) are available. For this reason, you can perform an Auxiliary Copy operation that would copy a Volume-Based Backup to a library that is not attached to the Celerra file server, because it is possible to restore that data.
- Auxiliary copy operations will maintain the data format of multiplexed data. If not all of the multiplexed data is required by the auxiliary copy operation (e.g., destination copy is a Selective type), the auxiliary copy operation will perform slower as un-required data is read and discarded. For better performance, reduce the level of multiplexing. For more information, see De-Multiplexing Multiplexed Data.
- To prevent a job from being copied to the same library during auxiliary copy operations, select the **Write to a Different Library Compared to Source Copy** option in the Copy Properties (Media) dialog box.
- During auxiliary copy operations for Oracle instances, the job status may go pending if the RMAN delete command is initiated to delete pieces of the backup job being copied. This is because the auxiliary copy manager can no longer retrieve the archive file information created from the archive manager. The auxiliary copy operations will automatically resume; however, the oracle backup job will be copied to second copy without the deleted pieces, which makes the job unrecoverable.

Inline Copy

- The multiplexing factor of the primary storage policy copy will be automatically used as the multiplexing factor for the secondary storage policy copy.

Network Load

The Copy Properties (Data Path Configuration) dialog box includes the following options for auxiliary copy operations that will assist with controlling network load.

- **Use LAN Free MediaAgent Only** This option allows users to opt for a LAN Free MediaAgent (drive pool) to be used for auxiliary copy operations. Selecting this option reduces network load because data is not transferred across a network.
- **Throttle Network Bandwidth per stream (MB/HR)** This option allows you to reduce (control) the Auxiliary Copy throughput so that the entire network bandwidth is not consumed. By default, the value is set to 500 megabytes per hour per stream. Increasing this value increases the bandwidth consumption, while decreasing the value decreases the bandwidth consumption. Note that the auxiliary copy throughput is restricted to the maximum bandwidth on the network.

CUSTOMIZE AUXILIARY COPY OPERATIONS THROUGH REGISTRY KEYS

- Periodically, Auxiliary Copy operations update the status of the jobs that are currently being copied. By default the status will be updated every 60 minutes, as well as at the end of the Auxiliary Copy operation. The time interval for the status updates can be modified using the AUXCOPY_MARKCOPIED_MINUTES registry key.
 - Auxiliary Copy operations copy all eligible data, even from data protection operations that have finished after the auxiliary copy operation has started. Auxiliary Copy operations can be prevented from copying this new data by configuring the AUXCOPY_NOT_PICK_NEW_BACKUPS registry key.
 - Auxiliary Copy operations prune copied jobs from the spool copy every hour or upon completion. This can be modified using the AUXCOPY_NOT_PRUNE_SPOOL_COPY registry key. If defined and enabled, the auxiliary copy will not prune any job from the spool copy.
 - You can enable the Auxiliary copy operations on migrated storage policies using the AUXCOPY_LOCAL_COMMCELL_ONLY registry key.
-

AUXILIARY COPY ENCRYPTION

While data encryption provides pass-phrase, key management, and network encryption support, you can also encrypt storage policy copies using auxiliary copy

encryption. This capability allows you to select portions of data you wish to encrypt, does not require client encryption configuration, and provides faster encryption performance.

See Auxiliary Copy Operations and Encryption for more information.

SCHEDULING

Operations for this feature can be scheduled to run on a regular basis. To create a job-based schedule for this feature in your CommCell environment, see [Create a Job Schedule](#).

If you have a large number of clients/backup sets/subclients, or storage policies in your CommCell that require the same schedule, it may be more beneficial to create a schedule policy for this operation; see [Create a Schedule Policy](#).

BEST PRACTICES

ENABLE AND CONFIGURE THE AUXILIARY COPY FALLEN BEHIND ALERT

Configure the **auxiliary copy fallen behind alert** so that you are notified when the data to be copied for the associated storage policy exceeds the threshold and/or the number of days the jobs for the associated storage policy have not been copied exceeds the set threshold. The thresholds for this alert can be set in the Storage Policy Properties (Advanced) window. For more information, see [Alerts: Job Management](#).

FREQUENTLY ASKED QUESTIONS

FOR SELECTIVE COPY, HOW DOES THE JOB SELECTION WORK WITH ADVANCED - CYCLE BASED CRITERIA?

On a Selective Copy, if you have selected **Automatically select Full Backups at frequency** option with **Advanced - Every <x> Cycle(s)** option, then the job selection will be done based on the Mod Logic.

The Mod Logic is implemented as follows:

$N \text{ mod } x$

- If $N \text{ mod } x$ is 1 then only first full backup jobs will be selected.
- If $N \text{ mod } x$ is 0 then the last full backup jobs will be selected.

Where:

N - is the cycle number of a backup job as seen under **Cycles/Sequence** column in the **Job for Storage Policy/Storage Policy copy** window, which will appear by right-clicking the **Storage Policy**, pointing to **All Tasks** and then clicking **View Jobs**.

x - is the number of cycles defined in the **Every <x> Cycle(s)** option in the **Advanced Options** dialog box.

Example:

- If $N = 3$ and $x = 2$, then $N \text{ mod } x \Rightarrow 3 \text{ mod } 2 = 1$ - the backup will qualify as a first full backup.
- If $N = 2$ and $x = 2$, then $N \text{ mod } x \Rightarrow 2 \text{ mod } 2 = 0$ - which means that backup will qualify as last full backup for the copy, if last full backup option is selected.
- If you have specified **Every <x> Cycles (s)** values as 4 (i.e., $x = 4$) during selective copy creation and selected **First Full Backup** option and during copy creation if the number of backup cycles on a source copy is 16 (i.e., $N = 16$), then:
 - $16 \text{ mod } 4 = 0$ and this backup will not qualify as first full backup for this newly created selective copy as the mod value is 0.
 - If the backup cycle value is 17 (i.e., $N = 17$), then $17 \text{ mod } 4 = 1$, this backup will be qualified for copy as first full backup for this copy.

In case of backup cycles $N = 18, 19, 20$ e.t.c., these backups will not qualify for copy selection because of mod logic.

CAN I COPY ALTERNATE CYCLE JOBS TO TWO DIFFERENT SELECTIVE COPIES?

If you wish to copy alternate cycle jobs (i.e., one odd and one even) to different copies then perform the following:

- Configure two selective copies.
 - On one copy, right-click the copy, and then click the Properties.
 - In the **Selective Copy** tab, from the **Automatically select Full Backups at frequency** list select **Advanced**.
 - In the **Advanced** dialog box select **Every <x> Cycles** and specify the value as **2**.
 - Select **First Full Backup** option.
 - Click **OK**.
 - On another copy, right-click the copy, and then click the **Properties**.

In the **Selective Copy** tab, from the **Automatically select Full Backups at frequency** list select **Advanced**.

In the **Advanced** dialog box select **Every <x> Cycles** and specify the value as **2**.

Select **Last Full Backup** option.

Click **OK**.

This allows you to copy the alternate cycles jobs to two different copies by implementing the mod logic explained in the above FAQ.

RELATED ALERTS

The following Job Management Auxiliary Copy alerts can be configured from the Alerts Wizard:

- Job Succeeded
- Job Skipped
- Job Failed
- Job Activity
- Auxiliary Copy fallen behind alert
 - The thresholds for this alert must be configured in the Storage Policy Properties (Advanced) window.
- Delayed by *n* Hrs
- Alert every *n* attempt (Phase failures)
- Alert every *n* attempt (Network failures)

For more information, see:

- Alerts: Job Management
 - Configure Alerts
-

RELATED REPORTS

ADMINISTRATIVE JOB SUMMARY REPORT

The Administrative Job Summary Report displays a summary of all or select Administrative jobs.

AUXILIARY COPY JOB SUMMARY REPORT

The Auxiliary Copy Job Summary Report displays auxiliary copy jobs and associated details.

JOBS IN STORAGE POLICY COPIES REPORT

The Jobs in Storage Policy Copies Report displays the data protection jobs associated with the storage policy copies.

[Back To Top](#)

Auxiliary Copy - How To

[Topics](#) | [How To](#) | [Troubleshoot](#) | [How Do I](#) | [Support](#) | [Related Topics](#)

[Schedule an Auxiliary Copy](#)

[Start an Auxiliary Copy](#)

[Create Automatic Copy Schedule](#)

[Disable/Enable a Job From a Storage Policy Copy](#)

[Disable/Enable All Jobs Associated with a Media](#)

[Enable/Disable Stream Randomization](#)

[Tune Stream Randomization](#)

[Re-Copy Fully or Partially Copied Jobs](#)

[Re-Copy All Jobs Associated with a Media](#)

Recover Your Data From Copies

Restore Data from a Secondary Copy using a Third-Party Command Line (Oracle, SAP for Oracle and SAP for MAXDB ;DataAgents)

Select a Source MediaAgent for an Auxiliary Copy Operation

Export Media Using Vault Tracker

Set Job Priorities to Copy during Auxiliary Copy operation

SCHEDULE AN AUXILIARY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To schedule an auxiliary copy:


1. From the CommCell Browser, right-click the storage policy for which you want to perform an auxiliary copy, click **All Tasks**, and then click **Run Auxiliary Copy**.
2. From the Job Initiation tab on the **Auxiliary Copy** dialog box, select **Schedule**, and click **OK**.
 - From the Schedule Details tab, select the necessary scheduling options.
 - To view the job summary for the auxiliary copy job that you have scheduled, click the Job Summary tab.
3. Click **OK** to save the schedule.

START AN AUXILIARY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To start an auxiliary copy:

1. From the CommCell Browser, right-click the storage policy for which you want to perform an auxiliary copy, click **All Tasks**, and then click **Run Auxiliary Copy**.
 2. In the **Auxiliary Copy** dialog box, the Storage Policy field is already populated with the name of the Storage Policy you selected.
 3. If the source copy is configured with a shared library, select the **Source MediaAgent** for the auxiliary copy.
 4. Select **All Copies** to copy data from the source copy to all secondary copies defined, or select a copy from the **Select a Copy** list box.
 5. Select **Start new media** to copy the data to a different tape or optical media. On a disk, this option, when selected, creates a new volume folder for the operation.
 6. Select the number of streams to copy in parallel from the **Number of Streams to Copy in Parallel** pane, or select **Allow Maximum**.
 7. Select **Mark media full after successful operation** to mark the media that is used for this operation full after the auxiliary copy operation has successfully completed.
 8. Select **Select Most Recent Full Backup When Auxiliary Copy Starts** to have the most recent successful full backup for each subclient copied when the Auxiliary Copy job is run.
 9. From the Job Initiation tab on the **Auxiliary Copy** dialog box, select the time for this job to run or choose to **Run Immediately**. You can also configure an alert for this job.
 10. Click **Advanced** to configure the **Vault Tracker**, **Startup** and **Job Retry** options.
 - Click **Vault Tracking** to select additional Vault Tracker options for this operation from the Vault Tracking dialog box.

Note: This option is only available if a Vault Tracker license is available in the CommServe.
 - Click **Startup** to change the priority of this job and, if necessary, to start this job in a suspended state from the Startup dialog box.
 - Click the **Job Retry** tab to specify the job running time and the number of job retries. See Restarting Jobs and Job Running Time for more information.
-  The **Number of Retries** specified for this particular job will only be used by the system if Auxiliary Copy was configured as a **Restartable** job type in the Job Management Control Panel. For procedures, see Specify Job Restartability for the CommCell.
11. Click **OK** to start the auxiliary copy operation. A progress bar displays the progress of the operation.

CREATE AUTOMATIC COPY SCHEDULE

Required Capability: See Capabilities and Permitted Actions

▶ To create an automatic copy schedule:

1. Right-click the storage policy associated with the secondary storage policy copy for which you wish to enable Auxiliary Copy operations, and then click **Run Auxiliary Copy**. To configure the copy options, refer to Start an Auxiliary Copy.
2. From the Job Initiation tab of the **Auxiliary Copy** dialog box, select **Automatic Copy**, and if necessary, change the **Interval** time in which the copy should run; the default is set to every 30 minutes.
You can set the time interval between 15 to 1440 minutes.
3. Click **OK** to save your changes.

DISABLE/ENABLE A JOB FROM A STORAGE POLICY COPY

Required Capability: See Capabilities and Permitted Actions

▶ To disable a job associated with a primary copy:

1. From the right pane of the CommCell Browser, right-click the copy whose jobs you want to disable, click **View** and then click **Jobs**.
2. Select the necessary filter options in the Job Filter for Storage Policy Copy dialog box.
3. Click the **Advanced** button for additional filter options in the Jobs in Storage Policy Advanced Filter Options dialog box. Click **OK**.
4. A list of jobs associated with a storage policy copy is displayed in the Jobs for Storage Policy Copy window.
5. Right-click on a job, and click **Prevent Copy** (for primary copies) or **Do Not Copy** (for secondary copies).
 - To select multiple jobs, hold down the **Ctrl** key, and right click on the jobs.
6. Select whether you want to prevent the associated incremental jobs in the **Prevent Copy** dialog box.
7. A list of all jobs that will be disabled in addition to the job you selected are displayed in the Prevent Copy dialog box.
8. Click **OK**.
9. Click **Yes** on the Confirmation pop-up window.

▶ To enable a job associated with a primary copy:

1. From the right pane of the CommCell Browser, right-click the primary copy whose jobs you want to disable, click **View** and then click **Jobs**.
2. Filter the necessary options in the Job Filter for Storage Policy Copy dialog box. Click **OK**.
3. A list of jobs associated with a storage policy copy is displayed in the Jobs for Storage Policy Copy window.
4. Right-click on a job, and click **Allow Copy**.
 - To select multiple jobs, hold down the **Ctrl** key, and right click on the jobs.
5. Click **Yes** on the Confirmation pop-up window.

DISABLE/ENABLE ALL JOBS ASSOCIATED WITH A MEDIA

Required Capability: See Capabilities and Permitted Actions

▶ To disable all jobs associated with a media:

1. From the right pane of the CommCell Browser, right-click the copy containing the media to which you want to disable jobs, click **View** and then click **Media**.
2. From the Media List dialog box, right-click on the media for which you wish to disable jobs and select **Prevent Copy**.
 - To select multiple media items, hold down the **Ctrl** key, and right click on the media.
3. Click **Yes** on the Confirmation pop-up window.

▶ To enable all jobs associated with a media:

1. From the right pane of the CommCell Browser, right-click the copy containing the media to which you want to enable jobs, click **View** and then click **Media**.
2. From the Media List dialog box, right-click on the media for which you wish to enable jobs and select **Allow Copy**.
 - To select multiple media items, hold down the **Ctrl** key, and right click on the media.
3. Click **Yes** on the Confirmation pop-up window.

ENABLE/DISABLE STREAM RANDOMIZATION

Required Capability: See Capabilities and Permitted Actions

▶ To enable stream randomization:

1. From the CommCell Browser, right click the storage policy for which you want to enable stream randomization, then click **Properties**.
2. From the General tab of the **Storage Policy Properties** dialog box, mark the checkbox for **Enable Stream Randomization**. Note that this field is only enabled when the storage policy is configured to use more than one (1) data stream.
3. Click **OK**.

To disable this feature, deselect the checkbox.

TUNE STREAM RANDOMIZATION

Required Capability: See Capabilities and Permitted Actions

▶ To tune the stream randomization feature:

1. From the **Control Panel**, double-click **Media Management**.
2. From the **Resource Manager Configuration** tab of the **Media management Configuration** dialog box, perform the following:
 - In the **Interval (in minutes) to calculate valid data size for streams** field specify the interval to calculate the data size for streams.
 - In the **Threshold (in GB) to decide how to distribute data among streams for backup** field specify the threshold to decide data distribution among streams.
3. Click **OK** to save the changes.

RE-COPY FULLY OR PARTIALLY COPIED JOBS

Required Capability: See Capabilities and Permitted Actions

▶ To recopy fully or partially copied jobs:

1. From the right pane of the CommCell Browser, right-click the storage policy copy whose data protection operations you want to recopy, click **View** and then click **Jobs**.
2. Select the necessary filter options in the Job Filter for Storage Policy Copy dialog box.
3. Click the **Advanced** button for additional filter options in the Jobs in Storage Policy Advanced Filter Options dialog box.
4. Click **OK**.
5. A list of jobs associated with a storage policy copy is displayed in the Jobs for Storage Policy Copy window.
6. Right click on a job to be recopied and select **Re-Copy** from the popup menu.

NOTES

- Data can only be recopied if it still exists in the source copy.

RE-COPY ALL JOBS ASSOCIATED WITH A MEDIA

Required Capability: See Capabilities and Permitted Actions

▶ To re-copy all jobs associated with a media:

1. From the right pane of the CommCell Browser, right-click the copy whose media you want to disable, click **View** and then click **Media**.
2. From the Media List dialog box, right-click on the media for which you wish to recopy jobs and select **Re-Copy**.
3. Click **Yes** on the Confirmation pop-up window.

RECOVER YOUR DATA FROM COPIES

Required Capability: See Capabilities and Permitted Actions

▶ To browse/restore/recover data from a specific synchronous or selective copy:

1. Identify the storage policy that will be accessed by the data recovery operation.
2. Identify the copy precedence number for each copy type of your storage policy using the Copy Precedence tab of the **Storage Policy Properties** dialog box.
3. From the Advanced Browse Options dialog box, select the **Browse from copy precedence** option and then type or specify the precedence number in **Copy Precedence**.
4. Data will be restored/recovered from the storage policy copy that has the selected copy precedence.

RESTORE DATA FROM A SECONDARY COPY USING A THIRD-PARTY COMMAND LINE

Related Topics

- Third-Party Command Line Operations

Restore the Oracle Database and Control File from a Secondary Copy using the RMAN Command Line

Before You Begin

- Ensure that you have run a backup of the Oracle database with one or more streams and, if applicable, the control file.
- Ensure that you have run an auxiliary copy operation after completing the backup(s).

Required Capability: See Capabilities and Permitted Actions

▶ To restore the Oracle database and control file from a secondary copy using the RMAN command line:

1. If applicable, restore the control file from autobackup using a secondary copy (otherwise skip to Step 2). To do this, run the script below from the RMAN command line:

```
run {
  allocate channel ch1 type 'sbt_tape'
  PARMS="ENV=(CV_restCopyPrec=1)" TRACE 0;
  allocate channel ch2 type 'sbt_tape'
  PARMS="ENV=(CV_restCopyPrec=2)" TRACE 0;
  restore controlfile from autobackup ;
}
```

2. Run the script below from the RMAN command line to restore the Oracle database from a secondary copy:

```
run {
  allocate channel ch1 type 'sbt_tape'
  PARMS="ENV=(CV_restCopyPrec=1)" TRACE 0;
  allocate channel ch2 type 'sbt_tape'
  PARMS="ENV=(CV_restCopyPrec=2)" TRACE 0;
  restore database;
}
```

Restore the SAP Database from a Secondary Copy using the SAP Command Line

Before You Begin

- Ensure that you have run a backup of the SAP database.
- Ensure that you have run an auxiliary copy operation after completing the backup.

Required Capability: See Capabilities and Permitted Actions

▶ To restore the SAP database from a secondary copy using the SAP command line:

1. Edit the parameter file for the SAP for Oracle iDataAgent or SAP for MAXDB iDataAgent to include the following two parameter lines:

```
CV_restCopyPrec
2
```

- For SAP for Oracle on Unix, include the above lines in the `initCER.utl` file located under the `db`s directory.
- For SAP for Oracle on Windows, create a parameter file to include the above lines then execute `brrestore` with option `-r`.

- For SAP for MAXDB on Unix, include the above lines in the parameter file located under the `$(software_install_folder)\SapMaxDbAgent` directory.
 - For SAP for MAXDB on Windows, include the above lines in the parameter file located in the same directory as `BSI_ENV`. To determine the directory where `BSI_ENV` resides, open the `test1.cfg` file located in the install directory then find the PATH for `BSI_ENV` (for example: `D:\MaxDB\sdb\test1\files\backint.conf`).
2. After editing the parameter file as described in Step 1, execute a restore from the SAP command line, and the data will be restored from a secondary copy.

SELECT A SOURCE MEDIAAGENT FOR AN AUXILIARY COPY OPERATION

Required Capability: See Capabilities and Permitted Actions



Do not select a source MediaAgent for this operation unless the source copy is configured with a shared library. If an invalid MediaAgent is selected for the operation, it will fail.

▶ To select a source MediaAgent for an auxiliary copy operation:

1. From the CommCell Browser, right-click the storage policy for which you want to perform an auxiliary copy, click **All Tasks**, and then click **Run Auxiliary Copy**.
2. Select the **Source MediaAgent** for the auxiliary copy.
3. Continue configuring the auxiliary copy operation as outlined in Start an Auxiliary Copy.

EXPORT MEDIA USING VAULT TRACKER

Required Capability: See Capabilities and Permitted Actions

▶ To export media using Vault Tracker:

1. From the CommCell Browser, right-click the **VaultTracker Policies** icon under the Policies node, and then click **New Tracking Policy**.
2. From the wizard, enter a name and description in the **Policy Name** and **Description** boxes. Click **Next**.
3. Click **Standard** and then click **Next**.
4. Select only the secondary copies whose tapes need to be taken offsite. Click **Next**.
5. Select the library from which you want the media exported. Click **Next**.
6. Select the media status to be managed by the policy. Click **Next**.
7. Select an export location from the **Export** dropdown list. Click **Next**.
8. Click **Yes**, and then click **Next**.
9. Define the Vault Tracker policy schedule to occur either every day or every week depending upon how often you need to take the media offsite. Click **Next**.
10. Select the time of day when you need the tapes to start appearing in the mail slot. Click **Next**.
11. Select the start date, and end date and time. Click **Next**.
12. Confirm your selections for the policy. Click **Finish**.
13. Manually remove media from the mail slot.

SET JOB PRIORITIES TO COPY DURING AUXILIARY COPY OPERATION

1. Logon to CommServe computer.
2. Create a text file with the following name under `<Software_Installation_Directory>\Base` folder.
<StoragePolicyName>_<CopyName>_Jobs.txt
3. In the text file specify **JobID** and **CommCellID** in the following format:

Syntax

```
JobID, CommCellID
```

Where

- JobID - The job id of the jobs for which you are setting up the priority
- CommCellID - The CommCell ID of the CommServe. The value of this parameter is 2.

Note that this value is not the same as the CommCell ID value in the **License Administration** dialog box

For example:

If 8287, 8288, 8289, 8290 jobs are available on primary copy then specify the jobs in the following format:

8288, 2

8290, 2

4. Perform the Auxiliary Copy operation on the Storage Policy that is specified in the text file name.
5. Once the Auxiliary Copy operation is run, the jobs specified in the text file (e.g., 8288 and 8290) will be copied first and then the other jobs will be copied. Jobs may not necessarily be copied in the exact order as in the text file but will be copied before other jobs that are not listed in the text file.

During this process, if Auxiliary Copy job goes into **Waiting/Suspended/Pending** state (e.g., if the job is interrupted by Job Manager or suspended by the user), then the priority of the jobs using text file will not be considered when the Auxiliary Copy job is resumed. It will copy all the jobs sequentially to secondary storage.

[Back to Top](#)

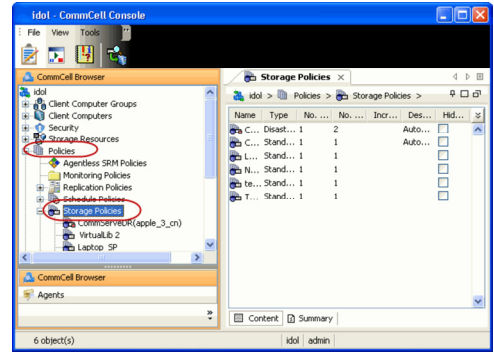
Data Aging - Getting Started

- Getting Started
- Advanced
- Troubleshooting
- FAQ
- Support

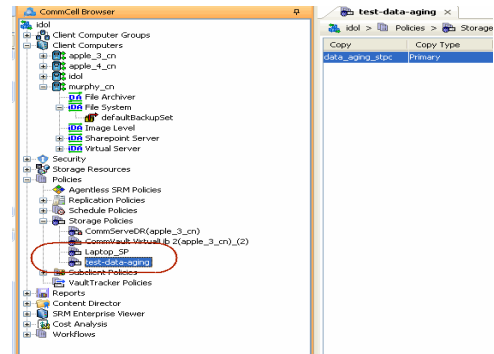
Data Aging is the process of removing old data from secondary storage to allow the associated media to be reused for future backups.

By default, all backup data is retained infinitely. However, you should change the retention of your data based on your needs. Note that if you continue to have infinite retention, you will also need infinite storage capacity.

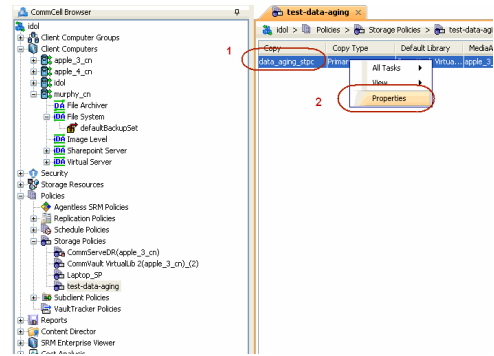
- From the CommCell Browser, navigate to **Policies | Storage Policies**.



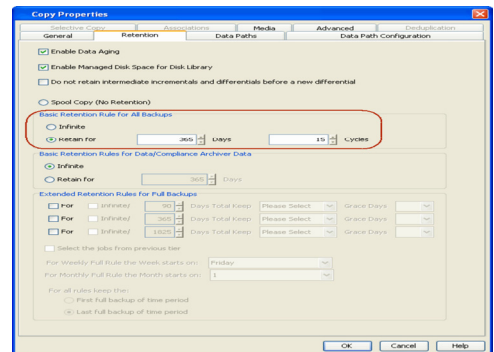
- Highlight the **Storage Policy**.



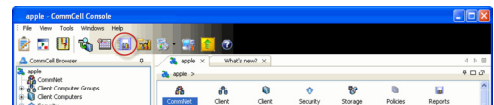
- From the right pane, right-click the **Storage Policy Copy** and click the **Properties**.



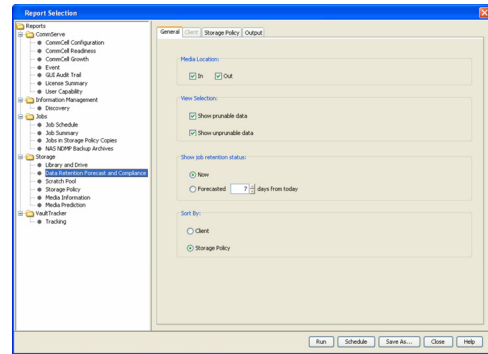
- Click the **Retention** tab.
 - Click the **Retain For** in the **Basic Retention Rules for All Backups** area.
 - Enter number of days to retain the data.
 - Enter number of cycles to retain the data.
 - Click **OK**.



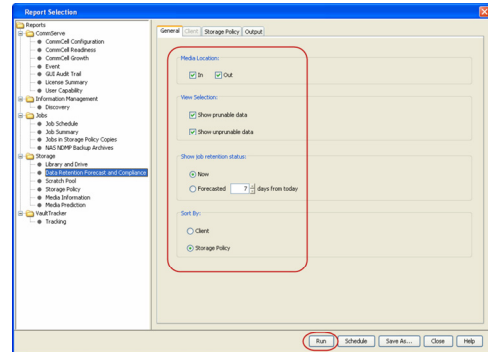
- From the CommCell Browser, click the **Reports** icon.



6. Expand Reports and select **Data Retention Forecast and Compliance**.



7. Click **Run**.

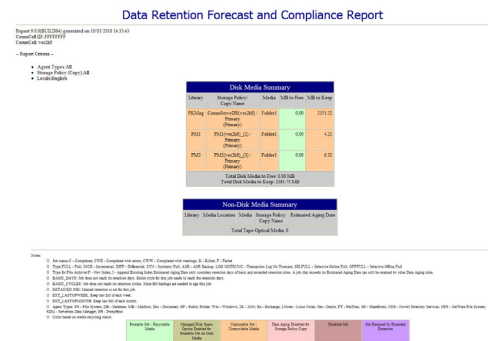


8. The report will display the data to be pruned when a data aging job is run.

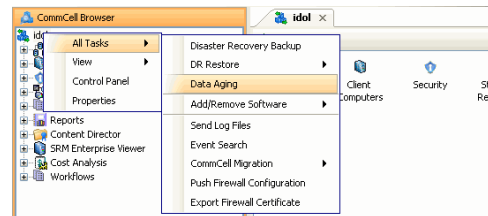
To ensure only data intended for aging is actually aged, it is important to identify the data that will be aged based on the retention rules you have configured. Hence, ensure this report includes only the data you intend to age.

If necessary, fine-tune your rules so that only the intended data is aged.

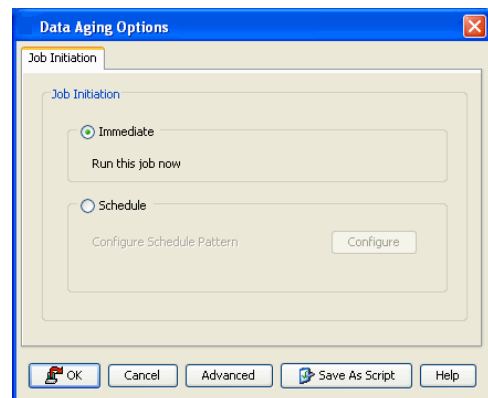
Once you run a data aging job, the data will be lost.



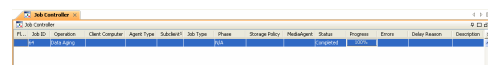
9. From the CommCell Console, right click the CommServe icon and click **All Tasks | Data Aging**.



10. Select **Immediate** in the Job Initiation section and click **OK**.



11. You can track the progress of the job from the **Job Controller** window. When the job has completed, the Job Controller displays **Completed**.



Make sure that the job completes successfully. If the job did not complete successfully, re-run the job.

Data Verification

Topics | How To | Troubleshooting | Related Topics

Overview

Configure a Copy for Data Verification

Pick a Job for Data Verification

Perform a Data Verification Operation

Data Verification Considerations for NetApp NAS Client

License Requirement

Audit Trail

Support Information - Storage Policy Copy

Related Reports

OVERVIEW

The software typically protects/archives data on various types of media. Once these operations have been performed, there is no way to ascertain if the data is valid for recovering until a data recovery operation has been performed on that data.

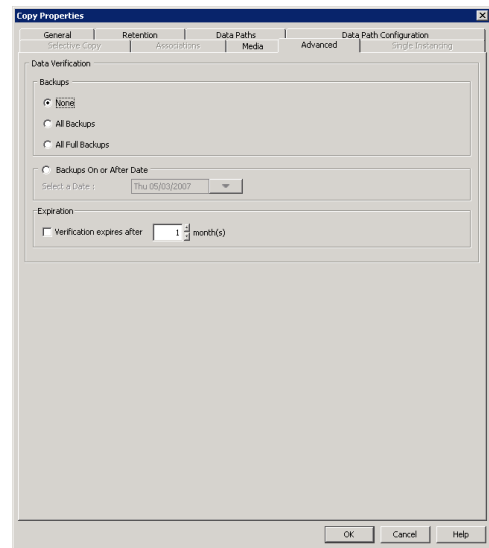
During a data verification operation, data is checked to see that it is valid for recovering and for being successfully copied during an auxiliary copy operation. You can verify data on all copies, or on a specific copy, and in parallel streams. A specific data protection/archive operation can also be verified on a copy. It is also possible to define a time interval of how long data verification for a data protection job is valid for a storage policy copy.

When auxiliary copy, data verification, and content indexing operations are initiated, they will all utilize the same single auxiliary copy manager process, thus reducing the load resources on the CommServe computer.

CONFIGURE A COPY FOR DATA VERIFICATION

You can configure a copy for data verification so that all, full, or those data protection/archive operations occurring on or after a certain date will be verified during a data verification operation. A copy can be configured for data verification from the **Advanced** tab.

Note that data verification is not set by default for any agents.



PICK A JOB FOR DATA VERIFICATION

You can select individual jobs to be verified during a data verification operation from the **Jobs for Copy** window. You can verify jobs on all types of storage policies. The example below is for an *iDataAgent Backup* storage policy.

The following table describes the data verification status that is displayed in the **Data Verification Status** column:

Status	When Displayed
Not Picked	A job has not been picked for a data verification operation.

Picked for Verification	A job has been picked for a data verification operation.
Successful	A data verification operation ran and successfully verified this job.
Failed	A data verification operation ran and failed to verify this job.
Partial	A data verification operation ran and has not yet completed verifying this job.

Once a job is picked, its status in the Data Verification Status field is displayed as Picked for Verification.

Job ID	Status	Client	Data Agent	Inst.	Backup Set	Subclient	Backup Type	Failed Files	Failed Files	Start Time	End Time	Data Transferred	User Name	Data Verification Status	Date & Time of Last Verification
276	View	00...	defaultBa...	defaultBa...	Purple_P...	Incremental	0	0	0	2003/07/...	2003/07/1...	1.61 MB	cvadmin	Not picked	
275	View Failed Items	00...	defaultBa...	defaultBa...	Purple_P...	Incremental	0	0	0	2003/07/...	2003/07/1...	35.81 MB	cvadmin	Not picked	
273	View Job Details	00...	defaultBa...	defaultBa...	System ...	Full	0	0	0	2003/07/...	2003/07/1...	239.73 MB	cvadmin	Not picked	
266	View Media	00...	defaultBa...	defaultBa...	System ...	Full	0	0	0	2003/07/...	2003/07/1...	239.73 MB	cvadmin	Not picked	
263	View Events	00...	defaultBa...	defaultBa...	Purple_P...	Full	0	0	0	2003/07/...	2003/07/1...	299.44 MB	cvadmin	Not picked	
262	Retain Job	00...	defaultBa...	defaultBa...	Purple_P...	Full	0	0	0	2003/07/...	2003/07/1...	2.29 GB	cvadmin	Not picked	
260	Do Not Retain Job	00...	defaultBa...	defaultBa...	System ...	Full	0	0	0	2003/07/...	2003/07/1...	239.73 MB	cvadmin	Not picked	
259	Disable For Copy	00...	defaultBa...	defaultBa...	default	Full	0	0	0	2003/07/...	2003/07/1...	1.60 GB	cvadmin	Not picked	
257	Prune Job	00...	defaultBa...	defaultBa...	Purple_P...	Differential	0	0	0	2003/07/...	2003/07/1...	4.18 MB	cvadmin	Not picked	
256	Pick for Data Verification	00...	defaultBa...	defaultBa...	Purple_P...	Differential	0	0	0	2003/07/...	2003/07/1...	15.83 MB	cvadmin	Not picked	
254	Available purple Windows 2000...	00...	defaultBa...	defaultBa...	System ...	Full	0	0	0	2003/07/...	2003/07/1...	239.73 MB	cvadmin	Not picked	
253	Available purple Windows 2000...	00...	defaultBa...	defaultBa...	default	Differential	0	0	0	2003/07/...	2003/07/1...	8.96 MB	cvadmin	Not picked	
251	Available purple Windows 2000...	00...	defaultBa...	defaultBa...	Purple_P...	Incremental	0	0	0	2003/07/...	2003/07/1...	1.62 MB	cvadmin	Not picked	
250	Available purple Windows 2000...	00...	defaultBa...	defaultBa...	Purple_P...	Incremental	0	0	0	2003/07/...	2003/07/1...	15.21 MB	cvadmin	Not picked	
248	Available purple Windows 2000...	00...	defaultBa...	defaultBa...	System ...	Full	0	0	0	2003/07/...	2003/07/1...	239.73 MB	cvadmin	Not picked	
247	Available purple Windows 2000...	00...	defaultBa...	defaultBa...	default	Incremental	0	0	0	2003/07/...	2003/07/1...	5.56 MB	cvadmin	Not picked	
245	Available purple Windows 2000...	00...	defaultBa...	defaultBa...	Purple_P...	Full	0	0	0	2003/07/...	2003/07/1...	297.18 MB	cvadmin	Not picked	

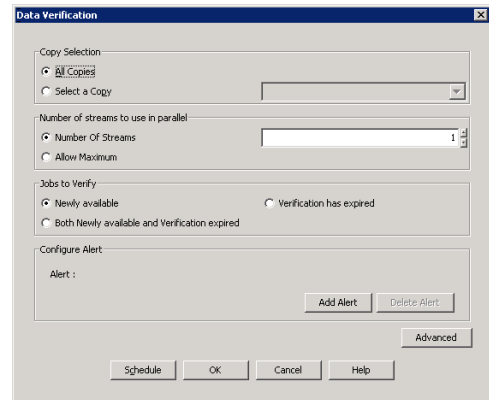
Once a data verification operation is run, the date and time of the operation is displayed in the Date and Time of Last Verification column.

Job ID	Status	Client	Data Agent	Inst.	Backup Set	Subclient	Backup Type	Failed Files	Failed Files	Start Time	End Time	Data Transferred	User Name	Data Verification Status	Date & Time of Last Verification
276	Available	purple	Windows 2000...	defaultBa...	Purple_...	Incremental	0	0	0	2003/07/...	2003/0...	1.61 MB	cvadmin	Successful	7/15/03 2:17 PM
275	Available	purple	Windows 2000...	defaultBa...	Purple_...	Incremental	0	0	0	2003/07/...	2003/0...	35.81 MB	cvadmin	Successful	7/15/03 2:17 PM
272	Available	purple	Windows 2000...	defaultBa...	default	Incremental	0	0	0	2003/07/...	2003/0...	5.57 MB	cvadmin	Successful	7/15/03 2:17 PM
273	Available	purple	Windows 2000...	defaultBa...	System ...	Full	0	0	0	2003/07/...	2003/0...	239.73 MB	cvadmin	Successful	7/15/03 2:17 PM
266	Available	purple	Windows 2000...	defaultBa...	System ...	Full	0	0	0	2003/07/...	2003/0...	239.73 MB	cvadmin	Not picked	
263	Available	purple	Windows 2000...	defaultBa...	Purple_...	Full	0	0	0	2003/07/...	2003/0...	299.44 MB	cvadmin	Not picked	
262	Available	purple	Windows 2000...	defaultBa...	Purple_...	Full	0	0	0	2003/07/...	2003/0...	2.29 GB	cvadmin	Not picked	
260	Available	purple	Windows 2000...	defaultBa...	System ...	Full	0	0	0	2003/07/...	2003/0...	239.73 MB	cvadmin	Not picked	
259	Available	purple	Windows 2000...	defaultBa...	default	Full	0	0	0	2003/07/...	2003/0...	1.60 GB	cvadmin	Not picked	
257	Available	purple	Windows 2000...	defaultBa...	Purple_...	Differential	0	0	0	2003/07/...	2003/0...	4.18 MB	cvadmin	Not picked	
256	Available	purple	Windows 2000...	defaultBa...	Purple_...	Differential	0	0	0	2003/07/...	2003/0...	15.83 MB	cvadmin	Not picked	
253	Available	purple	Windows 2000...	defaultBa...	default	Differential	0	0	0	2003/07/...	2003/0...	8.96 MB	cvadmin	Not picked	
254	Available	purple	Windows 2000...	defaultBa...	System ...	Full	0	0	0	2003/07/...	2003/0...	239.73 MB	cvadmin	Not picked	
251	Available	purple	Windows 2000...	defaultBa...	Purple_...	Incremental	0	0	0	2003/07/...	2003/0...	1.62 MB	cvadmin	Not picked	
250	Available	purple	Windows 2000...	defaultBa...	Purple_...	Incremental	0	0	0	2003/07/...	2003/0...	15.21 MB	cvadmin	Not picked	
247	Available	purple	Windows 2000...	defaultBa...	default	Incremental	0	0	0	2003/07/...	2003/0...	5.56 MB	cvadmin	Not picked	

If this copy has already been configured for data verification, then individual backups do not have to be selected on the copy.

PERFORM A DATA VERIFICATION OPERATION

The operation can then be performed from the Data Verification dialog box.



More advanced options are available from the Advanced Options for Data Verification dialog box, in which you can identify the media in which data should be verified.

DATA VERIFICATION CONSIDERATIONS FOR NETAPP NAS CLIENT

In addition to verifying data which has been backed up using NRS, data which has been backed up to a library attached to a NetApp file server can also be verified to ensure that it is valid for recovery.

Three Windows registry keys are provided which allow you to redirect NetApp NAS NDMP data verification operations:

- **sSaveFileHistory:** If turned on, all files in the backup will be written to the AuxCopy log as they are encountered in the backup image. Note that this can be a large amount of data. If you choose to turn this option on, it is recommended you increase the log file size.
- **sVerifyHeaderOnly:** If turned on, the data verification operation will not run through the entire backup image. Instead, it will only process the dump header of the backup.
- **sDATAVERIFICATION_DESTINATIONDIR:** If turned on, data verification can be performed for Read-Only volumes when a writable location is specified on the file server. This is useful if backing up a Snap mirror destination volume to a tape drive on the file server.

For more information on these registry keys, see Registry Keys and Parameters.

LICENSE REQUIREMENT

This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

AUDIT TRAIL

Operations performed with this feature are recorded in the Audit Trail. See Audit Trail for more information.

RELATED REPORTS

ADMINISTRATIVE JOB SUMMARY REPORT

The Administrative Job Summary Report displays a summary of all or select Administrative jobs.

DATA VERIFICATION JOB SUMMARY REPORT

The Data Verification Job Summary Report displays all data verification jobs with a specified status during a specified time period.

[Back to Top](#)

Data Verification - How To

[Topics](#) | [How To](#) | [Troubleshooting](#) | [Related Topics](#)

[Configure a Storage Policy Copy for Data Verification](#)

[Picking a Job on a Storage Policy Copy for Data Verification](#)

[Schedule a Data Verification Operation](#)

[Start a Data Verification Operation](#)

CONFIGURING A STORAGE POLICY COPY FOR DATA VERIFICATION

Required Capability: Capabilities and Permitted Actions

▶ To configure a storage policy copy for data verification:

1. From the right pane of the CommCell Browser, right-click the storage policy, and then click **Properties**.
2. From the Copy Properties (Advanced) tab of the **Copy Properties** dialog box, click the **All Backups** option if you want all backups to be verified during a data verification operation, or click **All Full Backups** if you want only full backups to be verified. You can also click the **Backups On or After Date** option and select a date from the **Select a Date** list. Only those backups that occur on or after the date you select will be verified.

Additionally, you can select the **Verification Expires after** option and choose the appropriate number of months from the list.

3. Click **OK** to save the changes.

PICK A JOB ON A STORAGE POLICY COPY FOR DATA VERIFICATION

Required Capability: See Capabilities and Permitted Actions

▶ To select a job for data verification:

1. From the right pane of the CommCell Browser, select a storage policy, then right click the storage policy copy whose job(s) you want to pick for data verification, click **View** and then click **Jobs**.
2. Filter the necessary options in the Job Filter for Storage Policy Copy dialog box. Click **OK**.

3. From the Jobs for Storage Policy Copy window, right-click a job, then click **Pick for Data Verification**. If you then decide that you do not want this job to be verified during a data verification operation, right-click the backup and click **Do Not Verify Data**.
 4. Click **Close**.
-

SCHEDULE A DATA VERIFICATION OPERATION

Required Capability: Capabilities and Permitted Actions

▶ To schedule a data verification operation.

1. From the CommCell Browser, right-click the storage policy for which you want to verify the data, click **All Tasks**, and then click **Verify Data**.
 2. From the Copy Properties (Advanced) dialog box, select either **All Copies**, or a select copy from the **Select a Copy** list.
 3. Select the number of streams to verify in parallel from the **Number of Streams to Copy in Parallel** pane, or select **Allow Maximum**. You may also select **Jobs to Verify** if you wish to select specific jobs to verify, as well as **Configure Alert** if you wish to configure a Data Verification Alert.
 4. To select more advanced options, click Advanced. Select the appropriate options from the Advanced Options for Data Verification dialog box. Click **OK**.
 5. Click **Schedule**.
 6. From the Schedule Details tab, select the necessary scheduling options
 7. To view the job summary for the data verification operation that you have scheduled, click the Copy Properties (Advanced) tab.
 8. Click **OK** to save the schedule.
-

START A DATA VERIFICATION OPERATION

Required Capability: Capabilities and Permitted Actions

▶ To start a data verification operation:

1. From the CommCell Browser, right-click the storage policy for which you want to verify the data, click **All Tasks**, and then click **Verify Data**.
 2. From the Copy Properties (Advanced) dialog box, select either **All Copies**, or a select copy from the **Select a Copy** list.
 3. Select the number of streams to verify in parallel from the **Number of Streams to Copy in Parallel** pane, or select **Allow Maximum**. You may also select **Jobs to Verify** if you wish to select specific jobs to verify, as well as **Configure Alert** if you wish to configure a Data Verification Alert.
 4. To select more advanced options, click Advanced. Select the appropriate options from the Advanced Options for Data Verification dialog box. Click **OK**.
 5. Click **OK**.
-

[Back to Top](#)

Media Refresh

Getting Started | **Advanced** | FAQ

Media Refresh operation enables you to consolidate data on media and/or to replace existing old media.

PREREQUISITES

Media Refresh requires the following:

- Library and Drivers are configured.
- Storage Policies are configured.
- Regular client backups are scheduled.

ENABLING MEDIA REFRESH

This section provides an example for running a Media Refresh operation based on the following criteria:

- Retention period for all backups that you want to retain is set to 90 days (3 months)

Also, the number of full backup cycle is set to 0 in the retention criteria

- Media refresh jobs are configured to run as follows:

1 month after the media is written

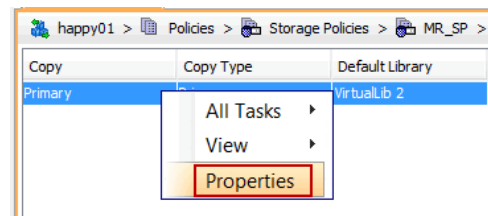
1 month before the media is aged

Active Media is Full

Use the following steps to configure the Media Refresh job using the above mentioned criteria:

1. From the CommCell Console, navigate to **Policies | Storage Policies | <Storage_Policy>**.

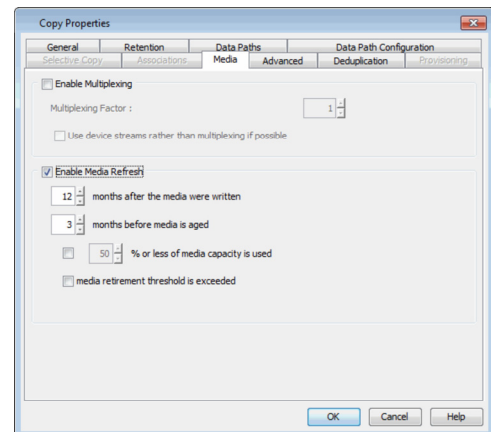
Right-click the Primary copy and then click **Properties**.



2.
 - Click the **Media** tab.
 - Select **Enable Media Refresh** check box.
 - By default, the Media gets refreshed with the below two criteria:

Months after the media were written - Media that were not written to in the specified number of months will be picked up for refresh. Type or select **1** month from the list.

Months before the media is aged - Media with specified number of months or more before aging will be picked up for refresh. Type or select **1** month from the list.

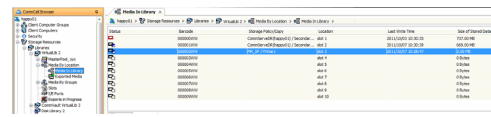
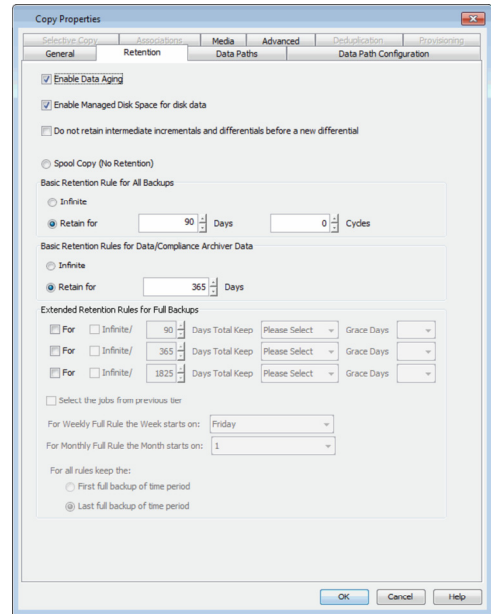


3.
 - Click the **Retention** tab.
 - From the **Basic Retention Rule for All Backups**, select **Retain for** option and set **90** Days and **0** Cycles.
 - Click **OK**.

4. Once you perform the backup, specific media will be assigned to the storage policy.

Note down the **Barcode** of the Media by performing the following steps:

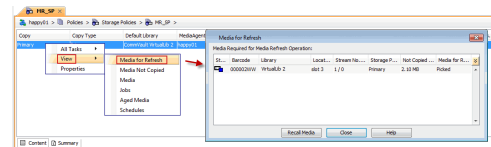
- From the CommCell Browser, navigate to **Storage Resources | Libraries. | <Tape Library> | Media By Location | Media In Library.**
- In the **Media In Library** window displayed in the right-pane, you can see a **Storage Policy / Copy** associated to a particular media.



VIEW A LIST OF MEDIA THAT CAN BE REFRESHED

Once the media is full and criteria's specified in the step 2 are satisfied, the media will be automatically picked for refresh. Use the following steps to see the list of medias that are picked for refresh operation.

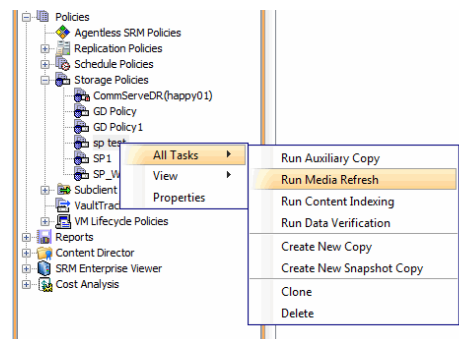
- Right-click the **Primary** copy, point to **View** and then click **Media for Refresh.**
 - In the **Media for Refresh** dialog box, the list of Media's required for Media Refresh operation are displayed.
 - Click **Close.**



RUN THE MEDIA REFRESH JOB

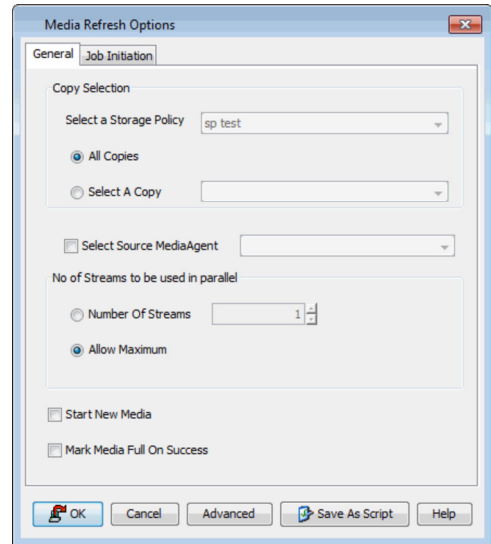
6. From the CommCell Browser, navigate to **Policies | Storage Policies.**

Select and right-click the **<Storage_Policy>** on which the Media Refresh was enabled, point to **All Tasks** and then click **Run Media Refresh.**



7. Click **OK.**

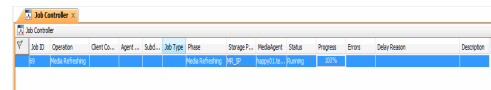
The data stream structure set at the Storage Policy is preserved during media refresh; streams are not combined during a media refresh job.



8. You can track the progress of the media refresh job from the **Job Controller** window. Ensure that the job completes successfully.

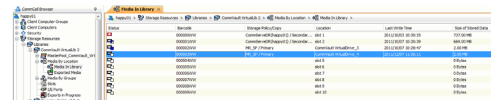
Once you run the Media Refresh job, run the data aging job to release the media.

See Data Aging for step-by-step instructions.



VERIFY THE NEW MEDIA

9.
 - From the CommCell Browser, navigate to **Storage Resources | Libraries. | <Tape Library> | Media By Location | Media In Library.**
 - In the **Media In Library** window displayed in the right-pane, you can see a **Storage Policy / Copy** associated to a New media.



Back to Top

Network

Topics | How To | Tools | FAQ | Troubleshoot | Related Topics

Overview

Network Agents

Network Bandwidth Throttling

- Setup Throttling for Client Computer Groups
- Setup Throttling for Clients
- Setup Throttling for MediaAgents
- Disable Throttling

Setup Throttling for Subclients

Data Pipe Buffers

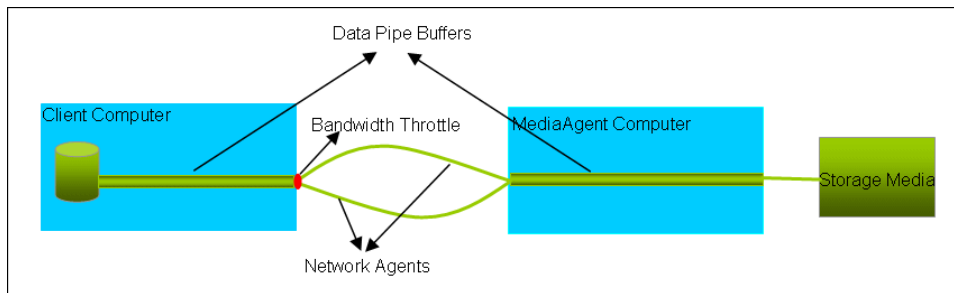
Client Connectivity

OVERVIEW

This page provides information on the following:

- Network Agents and Network Bandwidth Throttling provide information on the configurable options for Data Protection Operations using a network.
- Data Pipe Buffers provides information on using pipeline buffers to transfer data between the Client the MediaAgent computers.

The following diagram provides a visual representation of the above mentioned parameters:



NETWORK AGENTS

Network Agents are used to establish the data pipes which are used to transfer data to the MediaAgent. By default, the system uses 2 network agents and this may be suitable for 100 megabit networks. Increasing this value may increase the data transfer throughput from the Client. Note that the other network features, such as Network card speed, Network switch speed, etc., will also impact the network throughput and therefore it is recommended that you use this as an experimental parameter, based on your environment, to see if faster data throughput can be accomplished.

For most Agents, network agents can be established from the following dialog boxes:

- From the Subclient Properties, using the *Data Transfer Options* tab. For some database Agents this option is available at the Instance level. (See *Set the Network Bandwidth and Network Agents for a Data Protection Operation* for step-by-step instructions.)
- For Agents that support Subclient Policy, the option can be established in the policy template. (See *Create a New Subclient Template for an Existing Subclient Policy* for step-by-step instructions.)

For the QR Agent:

- To control network bandwidth settings, use the *Throttle Network Bandwidth* section in the General tab of the Subclient Properties dialog box.
- To control the number of network agents, you must create a `nQRNetworkAgents` registry key.

NETWORK BANDWIDTH THROTTLING

The network traffic for Clients and MediaAgents can be throttled based on the network bandwidth in your environment. This is useful to regulate network traffic and minimize bandwidth congestion.

By default, network throttling is disabled. You can enable the throttling options for an individual client, a client group consisting multiple clients, or a MediaAgent. Once configured, the throttling options are applied to all data transfer and control message operations, such as Data Protection operations including Laptop Backups, Copy operations including DASH copy, Data Recovery Operations, etc.

The throttling values setup in the throttling rule regulates the rate at which the data is sent and received.

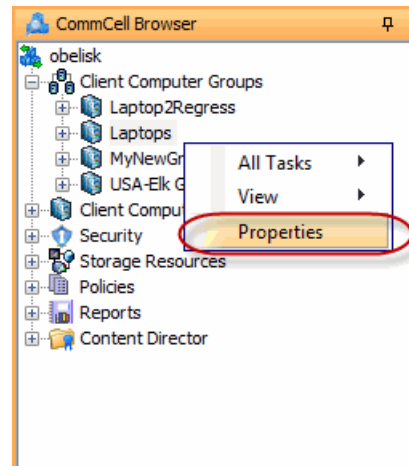
You can also setup relative bandwidth throttling to ensure performance when the client machine connects with limited bandwidth. Multiple rules can be created for same client/client group, however the lowest values set up in different rules takes precedence for each time that intersects.

Use the following steps to set up network throttling options for Client Computer Group and thereafter disable throttling from the automatic schedules:

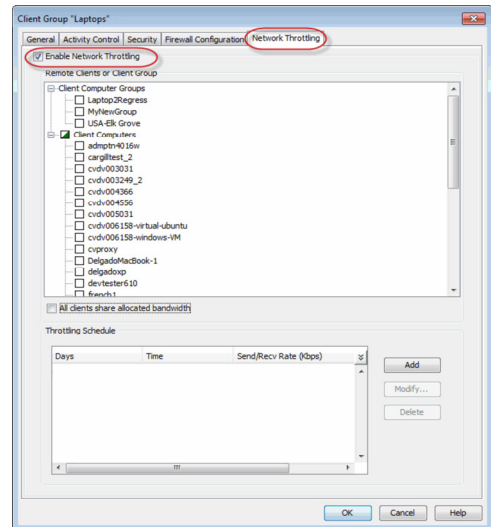
You can setup throttling for the following:

SETUP THROTTLING FOR CLIENT COMPUTER GROUPS

1.
 - From the CommCell Browser, navigate to **Client Computer Groups | <Client Group>**.
 - Right click the **<Client Group>** and click **Properties**.



2.
 - Click the **Network Throttling** tab.
 - Select **Enable Network Throttling**.




3. Select **Client Computer Groups** or **Client Computers** under **Remote Client or Client Groups** area to setup throttling from the selected client computer group. By default **All clients share allocated bandwidth** is selected to share the throttling settings among all selected clients cumulatively.

If this option is cleared, each client will throttle at the configured rate instead of a combined and shared rate.

4. Click **Add** to setup throttling rules.

- In **Days of Week** select a day or multiple days for the schedule to run.
- In **Time Interval** select whole day or a specific time interval for the schedule to run.

 Select one of the following under **Throttling Rate**:

- Absolute Throttling
- Relative Throttling
- **Use Absolute Throttling**

Select **Throttle Send** and/or **Throttle Receive** rate and enter appropriate values for each to throttle at the specified speed irrespective of the available bandwidth.

• **Throttle Relative to bandwidth**

- Select **If send bandwidth is less than (Kbps)** to specify a minimum bandwidth required for send throttling to take affect and then specify the percentage rate to throttle the network bandwidth when the minimum bandwidth is available.
- Select **If receive bandwidth is less than (Kbps)** to specify a minimum bandwidth required for receive throttling to take affect and then specify the percentage rate to throttle the network bandwidth when the minimum bandwidth is available.

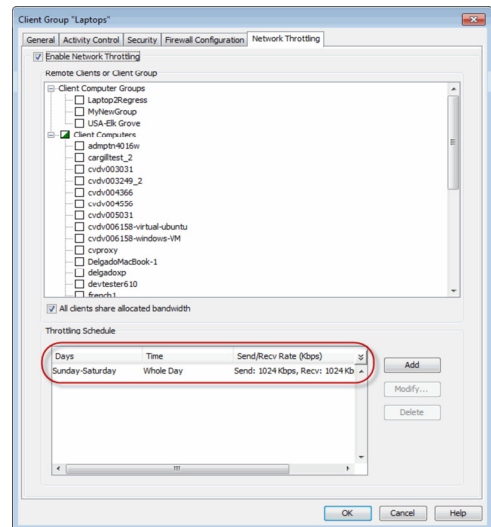
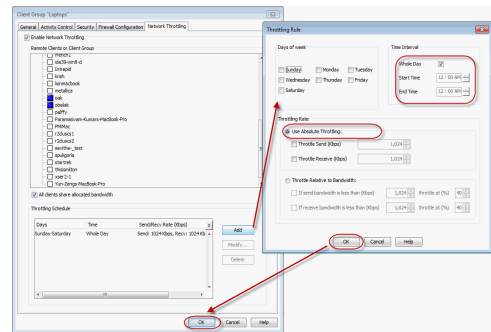
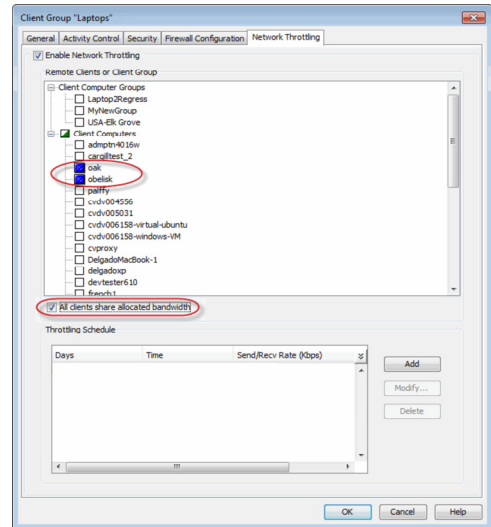
If the throttle bandwidth is higher than the amount specified in **Kbps**, then the job will run without throttling.

Click **OK**.

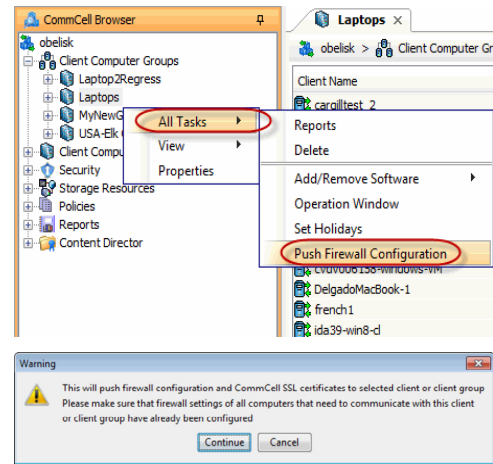
5. The newly added throttling rules will be displayed in Throttling Schedule.

Click **OK**.

6. From the CommCell Browser, navigate to **Client Computer Groups | <Client Group> | All Tasks** and click **Push Firewall Configuration**.

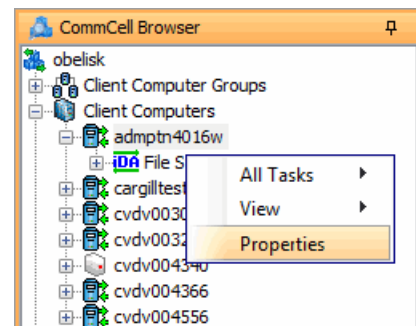


7. Click **Continue**.

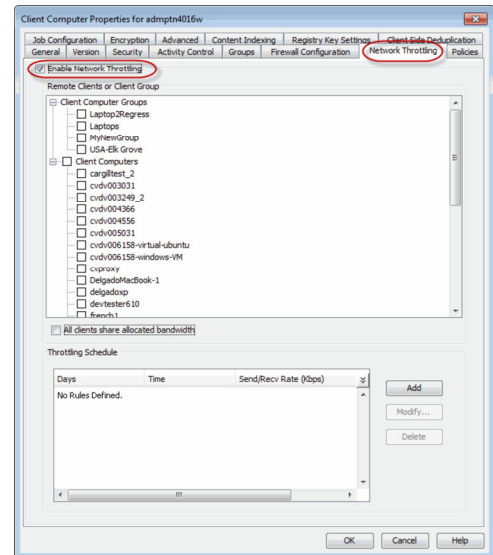


SETUP THROTTLING FOR CLIENTS

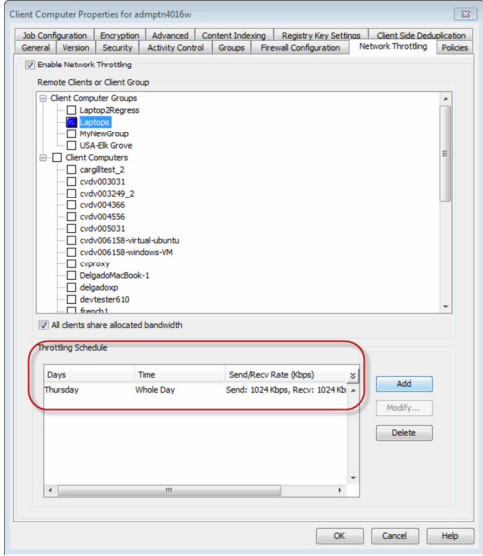
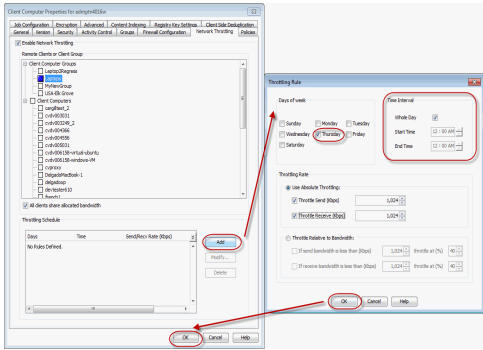
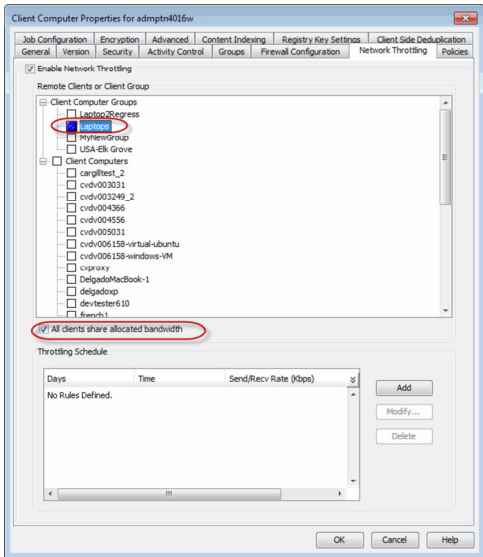
1.
 - From the CommCell Browser, navigate to **Client Computers | <Client>**
 - Right click the **<Client>** and click **Properties**.




2.
 - Click the **Network Throttling** tab.
 - Select **Enable Network Throttling**.



3.
 - Select **Client Computer Groups** or **Client Computers** under **Remote Client or Client Groups** area to setup throttling.
 - Select **All clients share allocated bandwidth**.



4. Click **Add** to setup throttling rules.
 - In **Days of Week** select a day or multiple days for the schedule to run.
 - In **Time Interval** select whole day or a specific time interval for the schedule to run.
-  Select one of the following under **Throttling Rate**:
- Absolute Throttling
 - Relative Throttling
 - **Use Absolute Throttling**

Select **Throttle Send** and/or **Throttle Receive** rate and enter appropriate values for each to throttle at the specified speed irrespective of the available bandwidth.
 - **Throttle Relative to bandwidth**
 - Select **If send bandwidth is less than (Kbps)** to specify a minimum bandwidth required for send throttling to take affect and then specify the percentage rate to throttle the network bandwidth when the minimum bandwidth is available.
 - Select **If receive bandwidth is less than (Kbps)** to specify a minimum bandwidth required for receive throttling to take affect and then specify the percentage rate to throttle the network bandwidth when the minimum bandwidth is available.

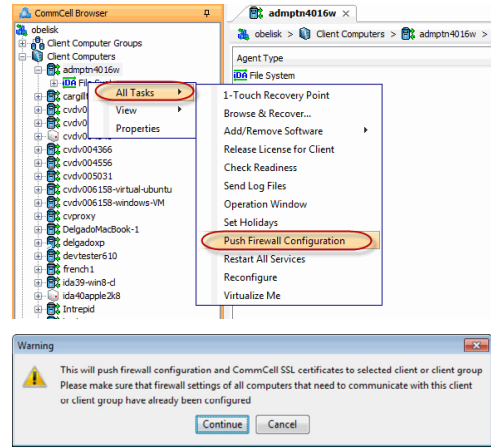
If the throttle bandwidth is higher than the amount specified in **Kbps**, then the job will run without throttling.
- Click **OK**.
5. The newly added throttling rules will be displayed in Throttling Schedule.

Click **OK**.

6. From the CommCell Browser, navigate to **Client Computer Groups | <Client> | All**

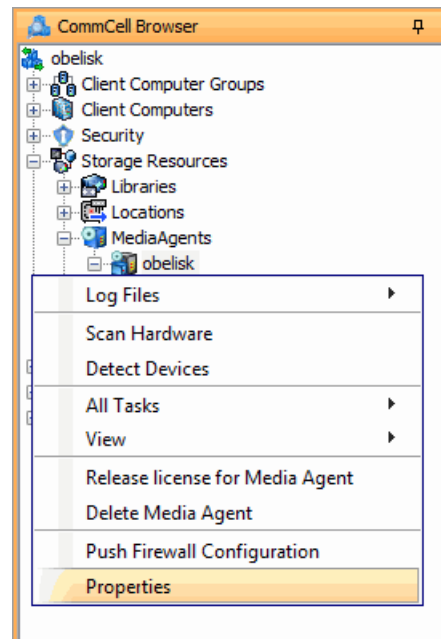
Tasks and click **Push Firewall Configuration**.

7. Click **Continue**.

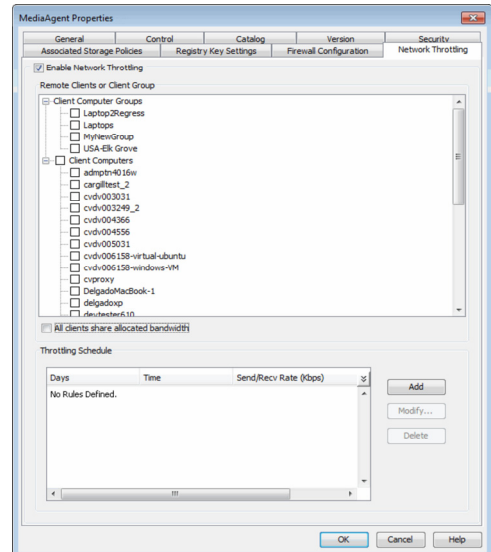


SETUP THROTTLING FOR MEDIAAGENTS

- From the CommCell Browser, navigate to **Storage Resources | MediaAgents | <MediaAgent>**
 - Right click the **<MediaAgent>** and click **Properties**.



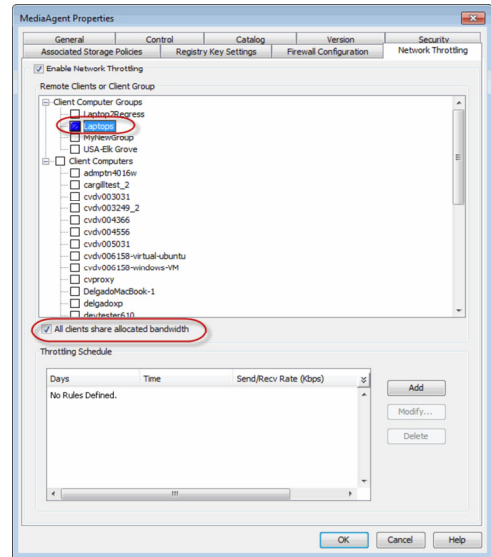
- Click the **Network Throttling** tab.
 - Select **Enable Network Throttling**.



- Select **Client Computer Groups** or **Client Computers** under **Remote Client or**

Client Groups area to setup throttling.

- Select **All clients share allocated bandwidth**.



4. Click **Add** to setup throttling rules.

- In **Days of Week** select a day or multiple days for the schedule to run.
- In **Time Interval** select whole day or a specific time interval for the schedule to run.



Select one of the following under **Throttling Rate**:

- Absolute Throttling
- Relative Throttling

- **Use Absolute Throttling**

Select **Throttle Send** and/or **Throttle Receive** rate and enter appropriate values for each to throttle at the specified speed irrespective of the available bandwidth.

- **Throttle Relative to bandwidth**

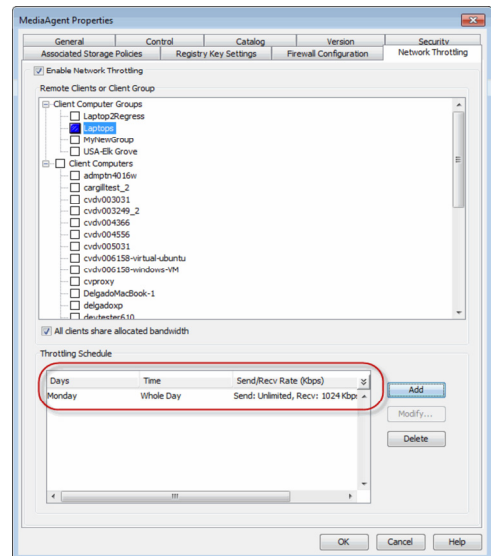
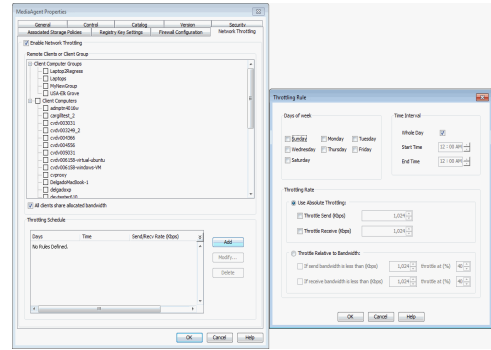
- Select **If send bandwidth is less than (Kbps)** to specify a minimum bandwidth required for send throttling to take affect and then specify the percentage rate to throttle the network bandwidth when the minimum bandwidth is available.
- Select **If receive bandwidth is less than (Kbps)** to specify a minimum bandwidth required for receive throttling to take affect and then specify the percentage rate to throttle the network bandwidth when the minimum bandwidth is available.

If the throttle bandwidth is higher than the amount specified in **Kbps**, then the job will run without throttling.

Click **OK**.

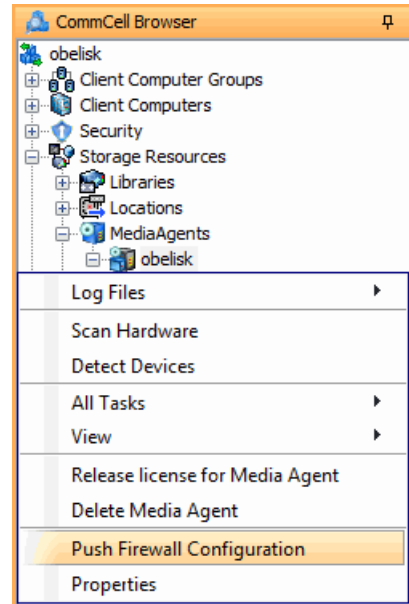
5. The newly added throttling rules will be displayed in Throttling Schedule.

Click **OK**.

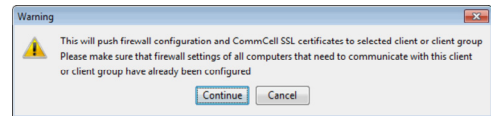


6. From the CommCell Browser, navigate to **Client Computer Groups | <Client> | All**

Tasks and click **Push Firewall Configuration**.

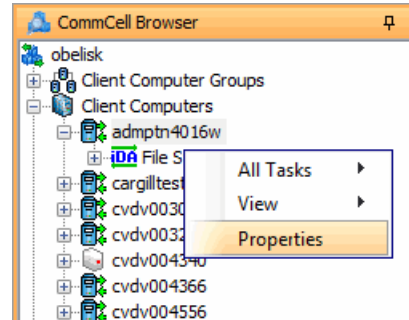


7. Click **Continue**.



DISABLE THROTTLING

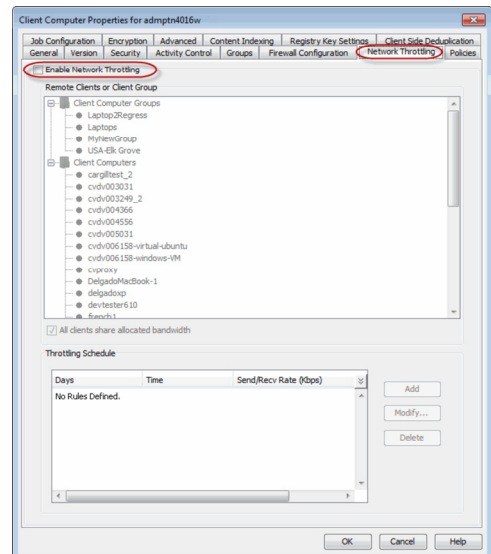
- From the CommCell Browser, navigate to **Client** or **Client Group** or **MediaAgent**
 - Right click the **<Client>** or **<Client Group>** or **<MediaAgent>** and click **Properties**.



- Click the **Network Throttling** tab.
 - Clear **Enable Network Throttling**.

If throttling is unchecked on an existing policy, a warning is issued that all clients will run at full speed unless equivalent throttling is set at the client group level.

- Click **OK**.



SETUP THROTTLING FOR SUBCLIENTS

Note that subclient throttling is done on a per Network Agent basis. For most Agents, network bandwidth can be established from the following dialog boxes:

- From the Subclient Properties, using the `Data Transfer Options` tab. For some database Agents this option is available at the Instance level. (See [Set the Network Bandwidth and Network Agents for a Data Protection Operation](#) for step-by-step instructions.)
- For Agents that support Subclient Policy, the option can be established in the policy template. (See [Create a New Subclient Template for an Existing Subclient Policy](#) for step-by-step instructions.)

For the QR Agent:

- To control network bandwidth settings, use the Throttle Network Bandwidth section in the General tab of the Subclient Properties dialog box.
- To control the number of network agents, you must create a `nQRNetworkAgents` registry key.

All subclients, except the subclients within NAS *iDataAgents* support network bandwidth throttling.

DATA PIPE BUFFERS

Data pipe buffers determines the amount of shared memory allocated on each computer for data pipes. The default size of each buffer is 64K; you can configure this buffer size - see [Configure the Application Read Size](#) for more information. By default, the system allocates 30 pipeline buffers on each computer which is used to transfer data between the client and the MediaAgent. (A total of 30 buffers of size 64K each allocates 2 MB of shared memory on each machine.)

You can use the `nNumPipelineBuffers` registry key to establish additional buffers as needed within the allowable range. Additional pipeline buffers may expedite running dedicated (non-multiplexed) backups to tape devices and therefore improve data transfer performance; on the other hand, allocating additional buffers may take up more shared memory than desired..

Note that this is an advanced feature and we recommend that you exercise extreme caution while modifying this registry key.

CLIENT CONNECTIVITY

You can check whether or not a client is accessible in the CommCell using the **Check Readiness** option in the CommCell Console.

When selected, this option will display a message indicating whether or not the client is accessible. If the client is not accessible, you can check the Service Control Manager to ensure the client's services are running.

For step-by-step instructions, see [Check Client Connectivity](#).

[Back to Top](#)

Network - How To

[Topics](#) | [How To](#) | [Tools](#) | [FAQ](#) | [Troubleshoot](#) | [Related Topics](#)

[Set the Network Bandwidth and Network Agents for a Data Protection Operation](#)

[Check Client Connectivity](#)

SET THE NETWORK BANDWIDTH AND NETWORK AGENTS FOR A DATA PROTECTION OPERATION

Before you Begin

- Do not modify the network bandwidth and network agents for a subclient or instance that is being backed up.

Required Capability: Capabilities and Permitted Actions

▶ To Set the Network Bandwidth and Network Agents for a Data Protection Operation:

1. From the CommCell Browser, right-click a subclient and then click **Properties**.

For the DB2, DB2 DPF, Informix, Oracle, Oracle RAC, SAP, or Sybase *iDataAgent*, right-click an instance and then click **Properties**.

2. Click the **Storage Device** Data Transfer Option tab.

For the QR Agent:

- To control network bandwidth settings, use the Throttle Network Bandwidth section in the General tab of the Subclient Properties dialog box.
- To control the number of network agents, you must create a `nQRNetworkAgents` registry key.

3. Enter a number of **Network Agents** that must be used to perform data protection operations on the subclient/instance.
4. Click the **Throttle Network Bandwidth (MB/HR)** option and then enter the throughput as needed. Note that throttling is done on a per Network Agent basis.
5. Click **OK** to save the changes.

This task is now complete.

CHECK CLIENT CONNECTIVITY

Required Capability: None.

▶ To check client connectivity:

1. From the CommCell Browser, right-click the icon of the client computer whose connectivity you want to check.
 2. Click **All Tasks**, and then click **Check Readiness**.
 3. A message will be displayed indicating whether or not the client is accessible in the CommCell.
 4. Click **Ok**.
-

[Back To Top](#)

Data Interface Pairs

Topics | How To | Related Topics

Overview

Configure Data Interface Pairs

Sample Scenarios

OVERVIEW

A network interface name or address is the identifier by which a computer is known to a network. A computer can have multiple network interfaces when it has multiple Network Interface Cards (NIC) and each NIC may have unique interface names, such as `amber1.company.com` and `amber2.company.com`. These names can be used to recognize the same computer in two different domains (e.g., Local Area Network and Storage Area Network) or in the same domain.

Using multiple NICs may reduce network congestion in situations where the software transfers a high volume of data using a network. This can be done as follows:

- You are prompted for a default network interface during the CommServe and MediaAgent installation. This is the interface used to both communicate and transfer data between the respective computers.
- If the MediaAgent and client have multiple network interfaces, you can define an additional interface to transfer data, using the Data Interface Pairs feature. For example, you can define an interface between a client and a MediaAgent, or between two MediaAgents.

Data Interface Pairs can be defined from the CommCell Console, or created in bulk with the `DataInterfacePairConfig` QScript in the command line interface. For information and instructions, see [Command Line Interface - Qscripts](#). These Data Interface Pairs are then used to transfer data between the specified computers. Keep in mind that the data interface pairs are used to transfer data and control only between the specified pairs of computers. To communicate with all the other computers within the CommCell and the CommServe the default network interface is used. (The default network interface is also always used for conducting control communication with the CommServe computer.) You can also bind the services to a specific NIC as described in [Binding Services to Specific Network Interface Cards \(NIC\)](#).

The default network interface is used to both communicate and transfer data between Clients and MediaAgents, unless specific interface pairs are defined.

In situations where any one these interfaces fail, or is not functional, the software does *not* automatically switch over to the other network interface.

The software also prompts for the CommServe hostname during the MediaAgent and Client installation. In remote computers, it is important to specify either the name of NIC that is visible to the computer or the NIC that will be used for communication.

CONFIGURE DATA INTERFACE PAIRS

Data Interface Pairs can be created between any two computers in a CommCell having multiple interfaces. This can be done in the following ways:

- Using the Data Interface Pairs Wizard from the Control Panel in the CommCell Console. The Wizard can be used to create, modify and delete data interface pairs.
- From the **Job Configuration** tab of the Client Properties dialog box of the corresponding client.

See [Configure Data Interface Pairs](#) for step-by step instructions.

DEFINING DATA INTERFACE PAIRS WHEN MULTIPLE INTERFACES HAVE THE SAME NAME

In this situation, it is necessary to instruct the CommCell components to use a specific Network Interface Card (NIC). You can do this using the following steps:

1. Assign a unique name to the NIC that must be used, using the `hosts` file in the CommServe and all other components in the CommCell.
2. Define the interface pairs that must be used between any two computers using the Data Interface Pairs wizard. You can define one interface pair between the computers. More than one interface pair is not supported.

Alternatively, you can type in the IP address of the specific NIC while defining the Data Interface Pairs.

CONFIGURING DATA INTERFACE PAIRS IN COMMNET

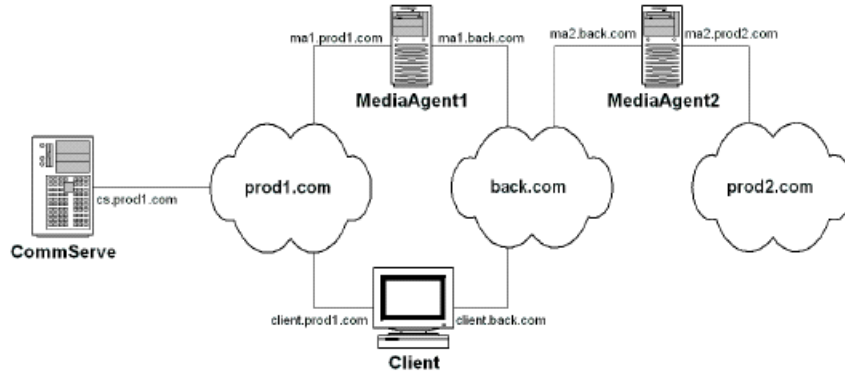
When you have multi-homed computers that has two or more network interface cards (NICs) in both the CommNet Server as well as the CommCell computer, you can configure the software to communicate across a specific NIC using the following procedures:

- Modify the CommCell Network Interface Name Used to Communicate with the CommCell
 - Modify the CommNet Server's Network Interface Name Used to Communicate with the CommCell
-

SAMPLE SCENARIOS

SAMPLES FOR DATA INTERFACE PAIRS USAGE

The following diagrams illustrate a few sample scenarios in which data interface pairs can be used:



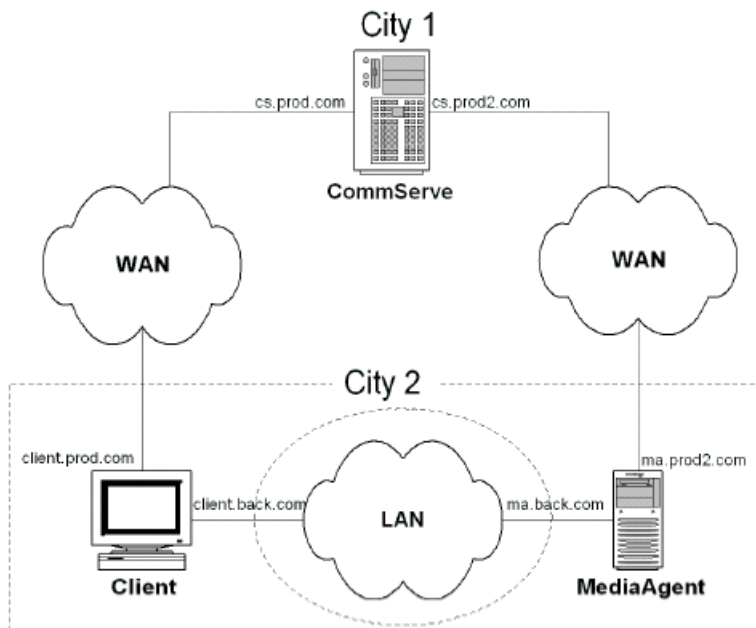
In the above scenario all data is conducted through the *backup* domain `back.com`, thereby reducing network traffic on the production domains. The following data interface pairs have to be defined to accomplish this goal:

- `ma1.back.com` and `client.back.com`

This interface pair can be used to conduct data over the *backup* domain, `back.com`. The default interface for the client is `client.prod1.com`, while the default network interface for MediaAgent1 is `ma1.prod1.com`.

- `ma1.back.com` and `ma2.back.com`

This interface pair can be used to conduct auxiliary copy operations over the *backup* domain, `back.com`. The default network interface for the for MediaAgent2 is `ma2.prod2.com`

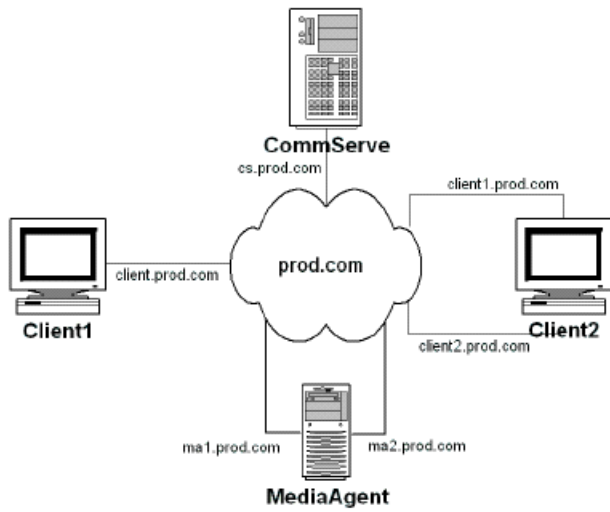


In the above scenario, the CommServe is located in one geographic domain, while the Client and MediaAgent are located in another different geographic domain. In such a situation, adding a third domain and defining the following pipeline pair between the Client and MediaAgent would result in efficient communication:

- `client.back.com` and `ma.back.com`

This interface pair can be used to conduct data over the *backup* domain, `back.com`. The default network interface for the client is

client.prod.com and the default network interface for the MediaAgent is ma.prod2.com

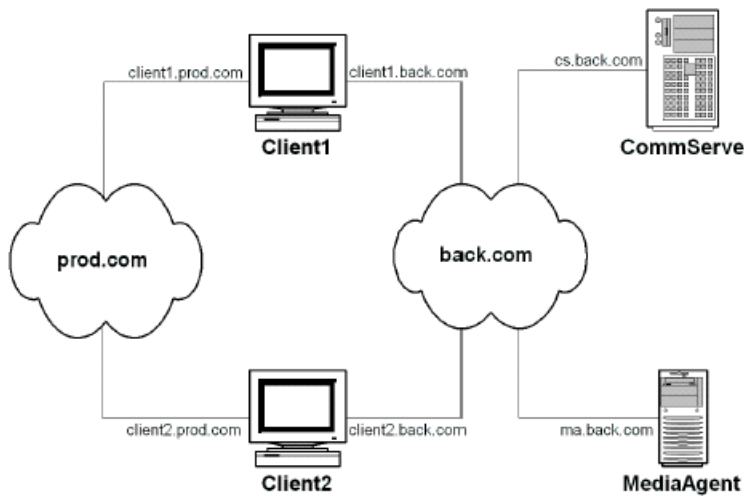


In the above scenario, although all the components are in the same domain, (they could be in a different subnet) defining the following pipeline pair between Client2 and MediaAgent would result in better network communication:

- ma2.prod.com and client2.prod.com

SAMPLE FOR DEFAULT INTERFACE NAME USAGE

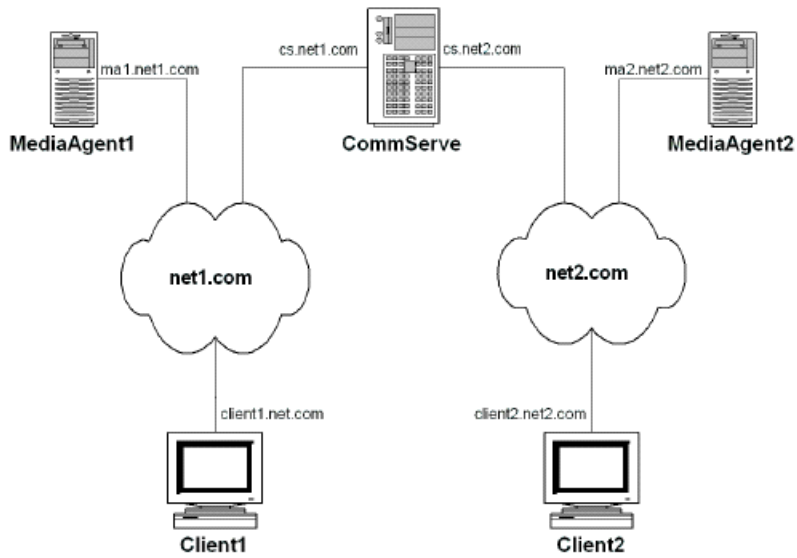
The following diagram illustrates a sample scenario in which defining the correct default interface name is beneficial.



In the above scenario, all the client computers are in the production domain while the MediaAgent and CommServe are attached to the *backup* domain back.com. By using the client1.back.com and client2.back.com as the default interface names for the clients, all the data protection operations and communication with the CommServe will be performed on the *backup* domain back.com.

SAMPLE FOR COMMSERVE HOSTNAME USAGE

The following diagram illustrates a sample scenario in which defining the correct CommServe hostname is beneficial.



In the above scenario, although the CommServe is installed with cs.net1.com as its default network interface, Client2 and MediaAgent2 must use the interface cs.net2.com as the CommServe hostname.

[Back To Top](#)

Data Interface Pairs - How To

[Topics](#) | [How To](#) | [Related Topics](#)

CommCell

- [Configure Data Interface Pairs](#)
- [View the Data Interface Pairs Between Two Computers](#)
- [Modify Data Interface Pairs](#)
- [Delete Data Interface pairs](#)

CommNet

- [Modify the CommCell Network Interface Name Used to Communicate with the CommCell](#)
- [Modify the CommNet Server's Network Interface Name Used to Communicate with the CommCell](#)

CommCell

CONFIGURE DATA INTERFACE PAIRS

Before You Begin

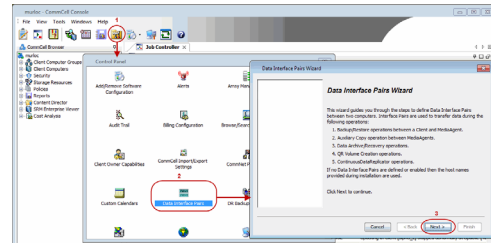
- When you create a data interface between two computers, you must ensure that there is a network path between the two computers. If there is no network path between the two computers all operations will fail. If necessary, check with your network administrator to determine whether a given interface pair is valid.

Required Capability: Capabilities and Permitted Actions

▶ To configure data interface pairs:

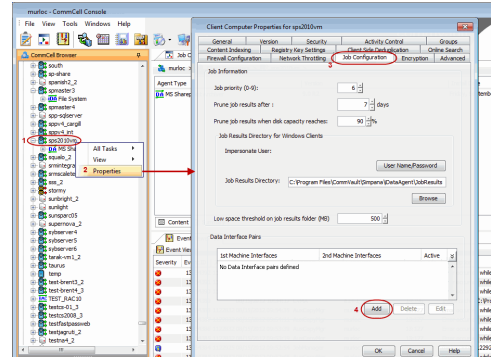
1. From the **Tools** menu in the CommCell Console, click **Control Panel** and then double-click **Data Interface Pairs**.

The **Data Interface Pairs Wizard** guides you through the process of creating Data Interface Pairs between any two computers. Click **Next** to continue.



Alternatively, you can also configure data interface pairs from the client computer:

- From the CommCell Browser, right-click the <Client> for which you wish to configure data interface pair, and click **Properties**.
- Click the **Job Configuration** tab.
- Under the **Data Interface Pairs** section, click the **Add** button.



2. Select the names of computers for which you want to define the Data Interface Pairs and then click **Next**.
3. Click **Add**.
4. Select the network interface name that you want to use for each client, and then click **Next**. This will become the interface pair for communication between the two clients.
 - If you do not find an specific network interface in the list, you can type the name or IP address of the NIC card.
 - In the case of remote computers, it is important to specify a network interface that is visible to the other computer.
5. The interface names between the two computers are displayed. Click **Next** to continue.

No more than one data interface pair should be created between two computers. If you want to establish a new interface pair, delete the existing one and configure the interface you want to use.

6. Click **Finish** to create the new data interface pair.

VIEW THE DATA INTERFACE PAIRS BETWEEN TWO COMPUTERS

Required Capability: Capabilities and Permitted Actions

▶ To view the data interface pairs between two computers:

1. From the **Tools** menu in the CommCell console, click **Control Panel**, and then double-click **Data Interface Pairs**.
2. From the **Data Interface Pairs Wizard** dialog box, click **Next** to continue.
3. Select the names of computers for which you wish to view the Data Interface Pairs and then click **Next**.
4. A list of interface pairs defined for the two computers are listed.
5. Click **Cancel** to exit the dialog box.

MODIFY DATA INTERFACE PAIRS

Required Capability: Capabilities and Permitted Actions

▶ To modify data interface pairs:

1. From the **Tools** menu in the CommCell console, click **Control Panel**, and then double-click **Data Interface Pairs**. Select the names of computers which you want to modify the Data Interface Pairs and then click **Next**.
2. The **Data Interface Pairs Wizard** displays the list of data interface pairs available.

3. Select the data interface pair you wish to modify, and then click the Edit button.
 4. From the **Edit Interface Pairs Dialog**, change the machine interfaces associated with the data interface pair, or change the Active status of the pair. Click **OK** when finished.
 5. Select **Next** to review the details and click **Finish** to modify the selected data interface pair.
-

DELETE DATA INTERFACE PAIRS

Required Capability: Capabilities and Permitted Actions

▶ To delete data interface pairs:

1. From the **Tools** menu in the CommCell console, click **Control Panel**, and then double-click **Data Interface Pairs**. Select the names of computers of which you wish to delete the Data Interface Pairs and then click **Next**.
 2. The **Data Interface Pairs Wizard** displays the list of data interface pairs available.
 3. Select the data interface pair you wish to delete, and then click the Delete button.
 4. Select **Next** to review the details and click **Finish** to delete the selected data interface pair.
-

CommNet

MODIFY THE COMMCELL NETWORK INTERFACE NAME USED TO COMMUNICATE WITH THE COMMCELL

Required Capability: See Capabilities and Permitted Actions

▶ To modify the CommCell Network Interface Name used to communicate with the CommCell:

1. On the **Setup** menu, click **Cell Registration**.
 2. From the Cell Registration dialog box, highlight the CommCell for which you wish to modify the interface name from the **Cell(s)** list, and then click **Modify**.
 3. From the Modify CommCell dialog box, type the following:
 - New name in the **Display Name** box.
 - New network interface name in the **CommCell Interface Name** box.
 4. Click **OK**. The system attempts to connect to the CommCell using the new interface name.
 - If the connection is established using the new network interface name, the new interface name for the CommCell is displayed in the Cell Registration dialog box.
 - If the connection fails, an error message is displayed.

The CommCell Interface Name may be changed in the following situations:

 - When the CommCell network interface name is changed.
 - When you have multiple network interfaces in the CommCell computer, and you wish to configure another network interface.
-

MODIFY THE COMMNET SERVER'S NETWORK INTERFACE NAME USED TO COMMUNICATE WITH THE COMMCELL

Required Capability: See Capabilities and Permitted Actions

▶ To modify the CommNet Server's Network Interface Name used to communicate with the CommCell:

1. On the **Setup** menu, click **Cell Registration**.
2. From the Cell Registration dialog box, highlight the CommCell for which you wish to modify the CommNet Server's network interface name used to communicate with the CommCell from the **Cell(s)** list, and then click **Modify**.
3. From the Modify CommCell dialog box, perform the following:
 - Type the new name in the **Display Name** box.
 - Choose the appropriate interface name from the **CommNet Interface Name** list.
 - Click **OK**.
4. Click **OK** in the **Registration Changed** prompt. The system saves the new Network Interface Name.

This option is useful if you have multiple network interface cards (NIC) on the CommNet Server. In such a situation, you can configure some of the CommCells to communicate through one interface, while others can be configured to use a different interface.

[Back To Top](#)

Firewall

Setup	Advanced	Troubleshooting	Best Practices
-------	----------	-----------------	----------------

Overview

Operating Using Direct Connections

- Client Connects to the CommServe (One-Way Firewall)
- CommServe Connects to the Client (One-Way Firewall)
- Client and CommServe Connect to Each Other (Two-Way Firewall)

Operating Through a Port-Forwarding Gateway

- Configure the Port-Forwarding Gateway
- Setup connection to the CommServe
- Install the Client
- Configure the CommServe, MediaAgent and Client
- Security Considerations

Operating Through a DMZ Using Calypso Proxy

- Set up the Calypso Proxy
- Install the Client
- Configure the CommServe, MediaAgent and Client

Operating Using Public WiFi Connections

- Install the Client
- Configure the Client to Operate across HTTP Proxy

Configuring Windows Firewall to Allow CommCell Communication

OVERVIEW

When CommCell components are separated by a firewall, the components must be configured with the connection route to reach each other across the firewall. Once configured, the components seamlessly communicate across the firewall for all data management operations such as backup, browse, restore, etc.

CommCell components can be configured to operate across the following:

- Port-forwarding gateways
- HTTP proxies
- DMZ
- NAT configurations
- Combinations of the above firewall scenarios.

In addition, you can also create your own Calypso proxy by designating a CommCell component as the proxy and defining the connections rules on the component. Components can communicate using HTTP or HTTPS protocol.

The following sections explain in detail the configuration required to install and operate CommCell components across different types of firewalls.

KEY FEATURES

The software offers the following key features in communication across firewall:

- Centralized configuration from the CommCell Console. Firewall settings can be configured at the individual client or client group levels.
- Lesser port requirements. Having port number 8400 is no longer a requirement to operate across firewalls. Backup and restore operations can be performed through a single open port. However, it is recommended that you open additional ports to enable faster data traffic.
- Support for port-forwarding routers. Multiple CommCell components on the internal network can be exposed to the outside world via a single gateway IP address with necessary port forwarding configured on the gateway. Roaming clients can reach specific internal machines by opening tunnel or data connections to specific ports on the port-forwarding gateway.
- Support for Calypso proxy configurations. For maximum security, the software now supports a special proxy configuration where you can place a Calypso agent in a DMZ, and configure the firewall to allow connections from inside and outside networks into the DMZ only.
- HTTPS encryption in the tunnels. The software now uses HTTPS encapsulation in all tunnel connections. This provides SSL/TLS encryption protecting all data in transit and allows for better compatibility with traffic filtering firewalls.
- Tunnel authentication using CommCell-specific certificate. Due to the use of HTTPS, all tunnel connections are not only encrypted, but also authenticated. For high levels of security, CommCells can be locked down to use CommCell-specific certificates for SSL/TSL authentication which is unique for every CommCell deployment.

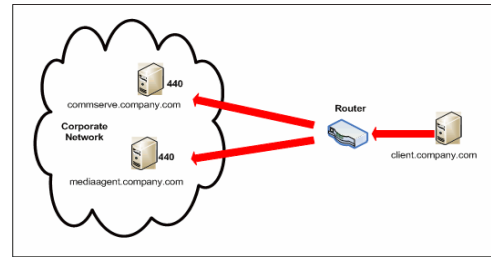
OPERATING USING DIRECT CONNECTIONS

Direct connection with port restrictions is a setup where at least one of any two communicating computers can establish a one-to-one connection towards the other on specific ports. The connection could also be routed if the routing does not include a proxy or an intermediate port-forwarding gateway. This configuration was supported as One-Way Firewall and Two-Way Firewall in previous releases.

CLIENT CONNECTS TO THE COMMSERVE (ONE-WAY FIREWALL)

Consider the diagram that illustrates a direct connection setup where the client opens tunnel connection towards the CommServe and the MediaAgent.

The following sections explain the configuration required on the CommServe, MediaAgent, and the client to operate in this scenario.



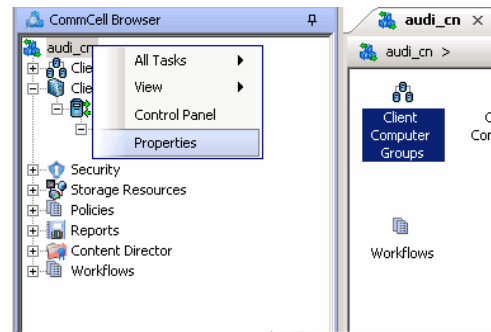
Review the following considerations before you begin.

- Make a note of the port configurations on your firewall and substitute them appropriately in the following instructions.
- Microsoft Internet Information Services (IIS) uses port number 443 by default. So if you have IIS running on a computer, then you will not be able to use port 443 for firewall configuration on that computer.

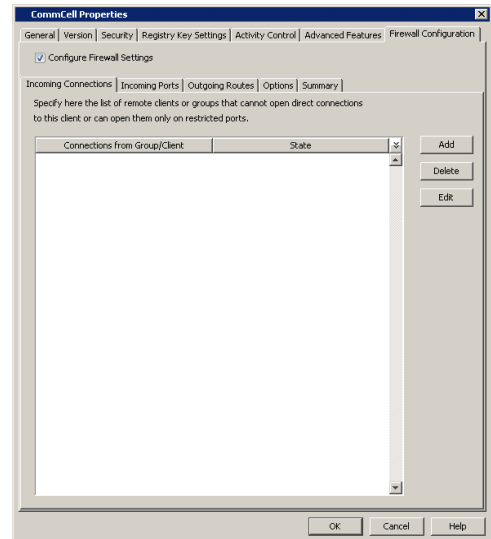
SETUP CONNECTION TO THE COMMSERVE

Before installing the client, you will have to provide an incoming port number on which the CommServe will receive tunnel connections from the client. The following steps explain the configurations required for this purpose.

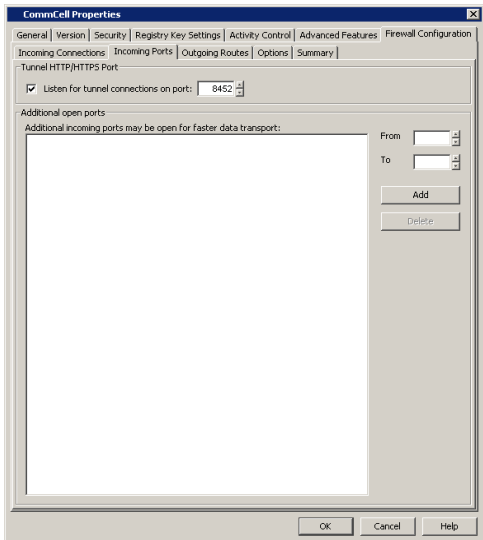
1. From the CommCell Console, right-click the CommServe computer and click **Properties**.



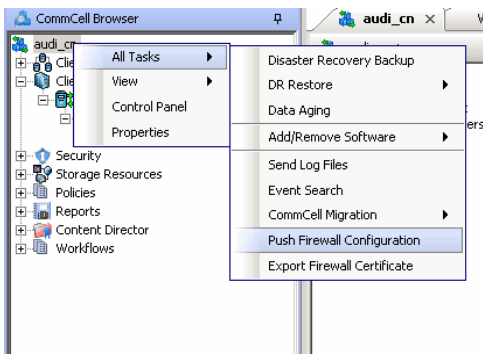
2. Click the **Firewall Configuration** tab.



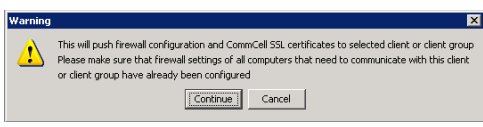
3.
 - Click the **Incoming Ports** tab.
 - Select **Listen for tunnel connections on port** and specify the port number on which the incoming tunnel connection is received.
 - Click **OK**.



- From the CommCell Console, right-click the CommServe computer and click **All Tasks | Push Firewall Configuration**.



- Click **Continue**.
The specified configuration is saved.
Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.



INSTALL THE CLIENT

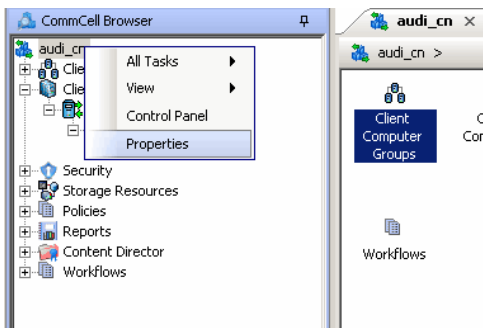
In this configuration the client establishes connection with the CommServe using one or more ports. To install the client across a firewall in this setup, you will have to specify the path to reach the CommServe computer. During installation of the client, use one of the following firewall configuration sequence.

- Client/MediaAgent can reach the CommServe (Windows clients)
- Client/MediaAgent can reach the CommServe (Unix clients)

CONFIGURE THE COMMSERVE, MEDIAAGENT AND CLIENT

Use the following steps to establish incoming and outgoing connectivity details between the CommServe, MediaAgent, and the client computer.

- To configure the CommServe, right-click the CommServe computer from the CommCell Console and click **Properties**.



- Click the **Firewall Configuration** tab.
- From the **Incoming Connections** tab, click **Add**.

4.
 - In the **From** field, select the name of the client you just installed.
 - In the **State** field, specify the status of the connection from the client. Since in this case the client can reach the CommServe, assuming that the firewall is restricting connections to a specific port, select **Restricted**.

Note that if the firewall allowed any connection from the client to the CommServe, then this entry is not required.

- Click **OK**.

5.
 - Click the **Incoming Ports** tab. You will see the tunnel port already specified on the CommServe.
 - **Additional Open Ports:** For components that handle data transfer (for example, MediaAgent, File System iDataAgent, etc.), you can speed up the data transfer by opening additional ports on the firewall and recording them as open in this screen. Specify the range of ports in the **Additional open ports** area, **From** and **To** fields. Click **Add** to add the ports. To remove a port from the listing, select the port and click **Delete**. The ports must be within the range of 1024 - 65000. Ensure that the ports specified here are not used by other applications.

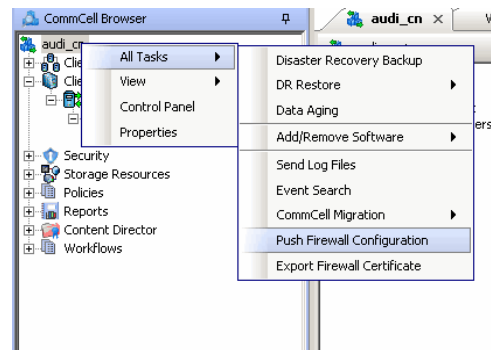
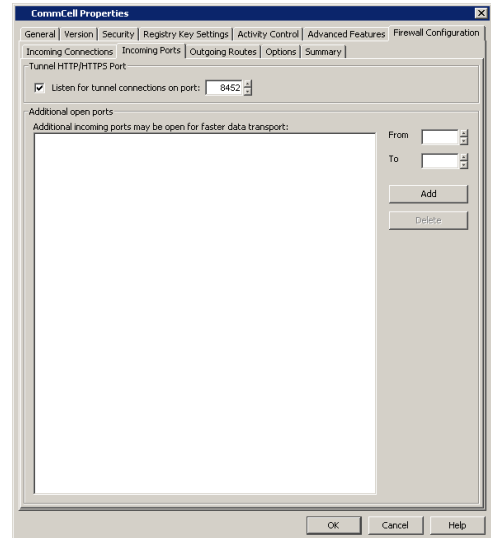
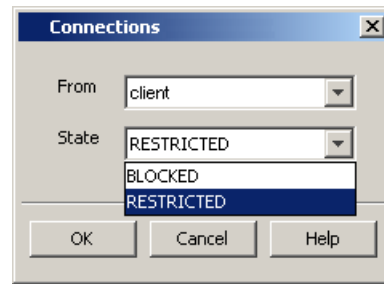
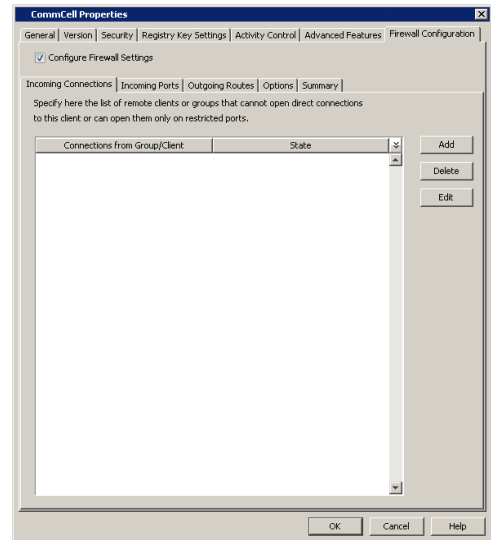
Review the following recommendations.

- For MediaAgents involving multi-stream restores, opening additional ports increases the restore performance. The number of open ports should correspond to the number of simultaneously running restore streams.
- For MediaAgents with **Optimize for concurrent LAN backups** option enabled, opening the incoming port of the Bull Calypso Communications Service improves the backup performance.
- For MediaAgents performing SnapProtect operations with Data Replicator snap engine, opening additional ports increases the backup performance.
- For ContinuousDataReplicator and Workstation Backup destination computers, opening additional incoming ports improves the replication performance.

- Click **OK**.

6. From the CommCell Console, right-click the CommServe computer and click **All Tasks | Push Firewall Configuration**. This updates the firewall configuration on the CommServe and client computer.

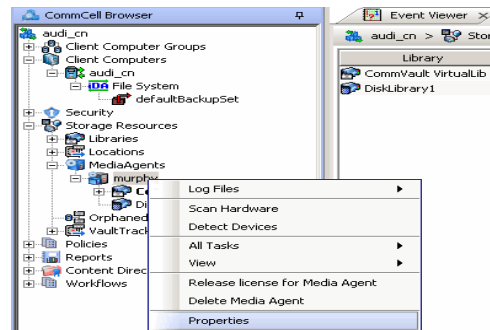
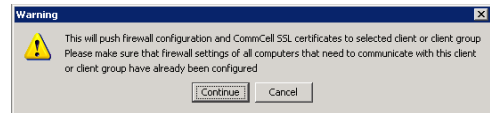
7. Click **Continue**.



The CommServe is configured to receive communication from the client.

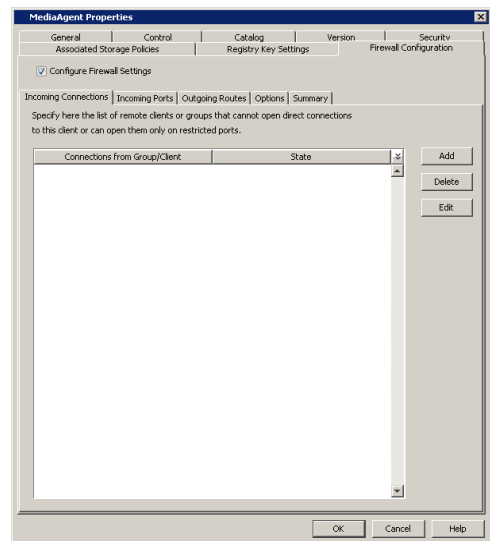
Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.

8. To configure the MediaAgent, right-click the MediaAgent computer from the CommCell Console and click **Properties**.



9. Click the **Firewall Configuration** tab.

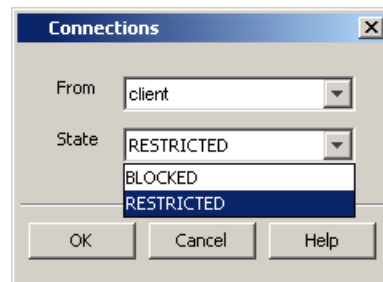
10. From the **Incoming Connections** tab, click **Add**.



11.
 - In the **From** field, select the name of the client you just installed.
 - In the **State** field, specify the status of the connection from the client. Since in this case the client can reach the MediaAgent, assuming that the firewall is restricting connections to a specific port, select **Restricted**.

Note that if the firewall allowed any connection from the client to the MediaAgent, then this entry is not required.

- Click **OK**.



12.
 - Click the **Incoming Ports** tab.
 - Select the **Listen for tunnel connections on port** option and specify the tunnel port through which connections from the client are received on the MediaAgent computer.
 - **Additional Open Ports:** For components that handle data transfer (for example, MediaAgent, File System iDataAgent, etc.), you can speed up the data transfer by opening additional ports on the firewall and recording them as open in this screen. Specify the range of ports in the **Additional open ports** area, **From** and **To** fields. Click **Add** to add the ports. To remove a port from the listing, select the port and click **Delete**. The ports must be within the range of 1024 - 65000. Ensure that the ports specified here are not used by other applications.

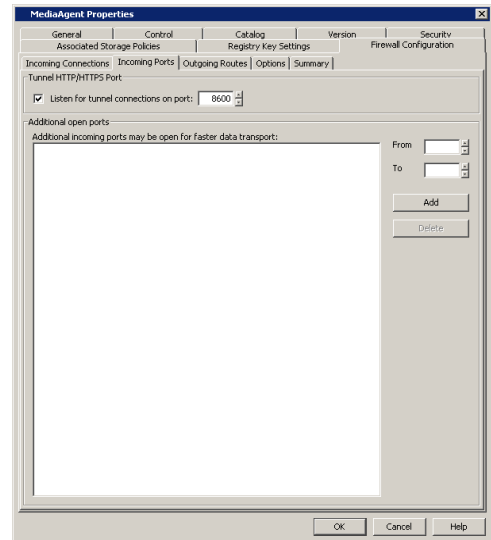
Review the following recommendations.

- For MediaAgents involving multi-stream restores, opening additional ports increases the restore performance. The number of open ports should correspond to the number of simultaneously running restore streams.
- For MediaAgents with **Optimize for concurrent LAN backups** option enabled, opening the incoming port of the Bull Calypso Communications Service

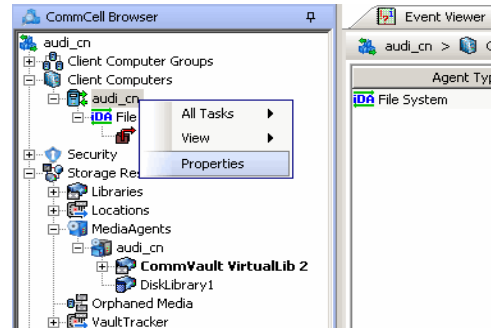
improves the backup performance.

- For MediaAgents performing SnapProtect operations with Data Replicator snap engine, opening additional ports increases the backup performance.
 - For ContinuousDataReplicator and Workstation Backup destination computers, opening additional incoming ports improves the replication performance.
- Click **OK**.

The MediaAgent is now configured to receive communication from the client.

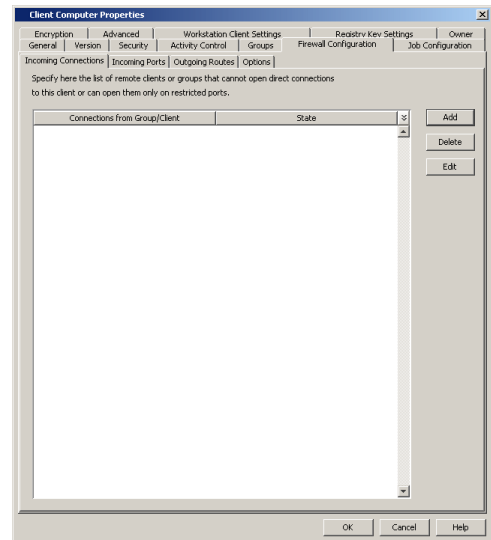


13. To configure the Client, right-click the client computer from the CommCell Console and click **Properties**.

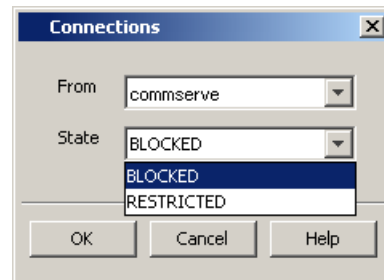


14. Click the **Firewall Configuration** tab.

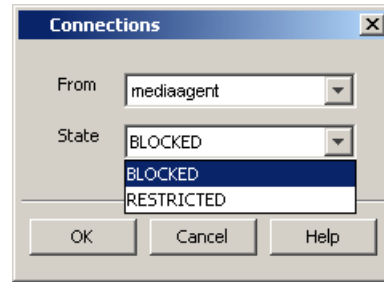
15. From the **Incoming Connections** tab, click **Add**.



16.
 - In the **From** field, specify the name of the CommServe computer.
 - In the **State** field, select **Blocked**, since the CommServe cannot open connections to the Client.
 - Click **OK**.



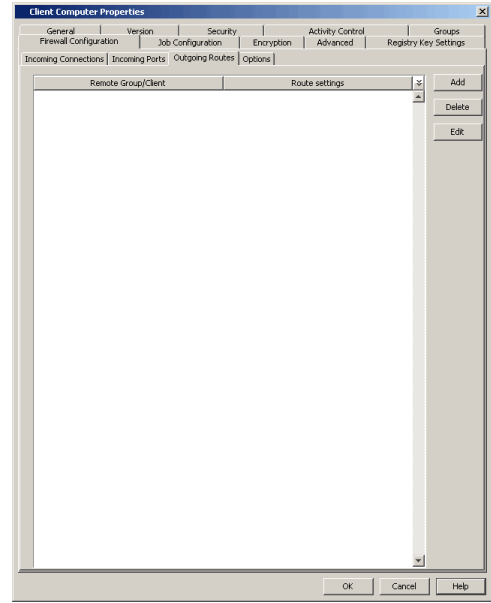
17.
 - Click **Add** again to specify the MediaAgent connection details.
 - In the **From** field, specify the name of the MediaAgent computer.
 - In the **State** field, select **Blocked**, since the MediaAgent cannot open connections to the Client.
 - Click **OK**.



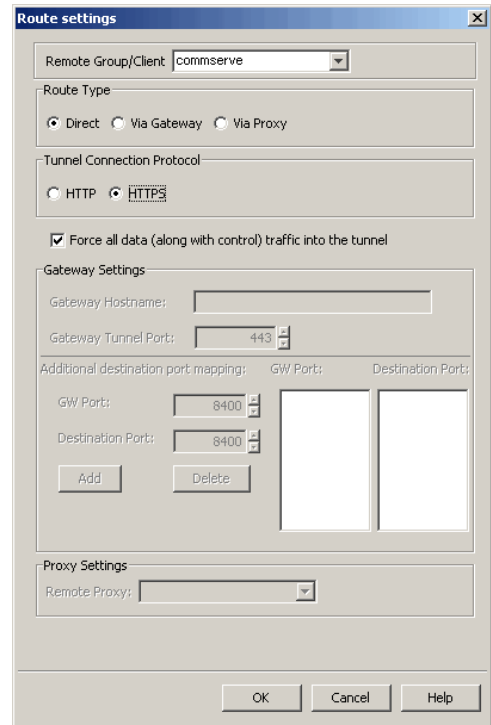
18.
 - Click the **Outgoing Routes** tab.
 - Click **Add**.

Outgoing routes are automatically created in the direct connectivity setup — manual entry is not required. However, you might want to create an entry if you wish to achieve one of the following.

 - Enable HTTPS encryption for the tunnel or data traffic.
 - Encrypt the data connections by forcing the connections into the tunnel. However, consider the following before using this option.
 - Direct connections always work faster. Forcing data connections into the tunnel might degrade performance of data protection operations.
 - If you wish to encrypt your backup data, you must rather configure encryption at the client level which offers more control and stores the data in encrypted form on the backup media as well.



19.
 - Select the CommServe name in **Remote Group/Client**.
 - Select **Direct**.
 - Select **HTTPS** protocol. This will enable authentication and encryption for tunnel connections.
 - **Force all data (along with control) traffic into the tunnel** option is not required as this route is not toward MediaAgent.
 - Click **OK**.

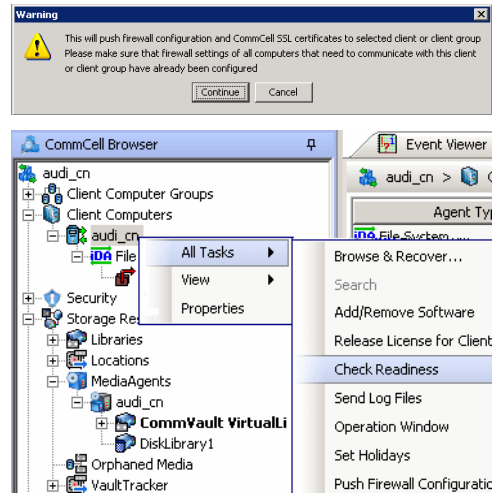


20. From the CommCell Console, right-click the client computer and click **All Tasks | Push Firewall Configuration**. This updates the firewall configuration files on the client computer.

21. Click **Continue**.

The client is configured to communicate with the CommServe and MediaAgent.
Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.

- From the CommCell Console, right-click the client computer and click **All Tasks | Check Readiness**. The results are displayed in **Client Connectivity** dialog box.
If the client computer is not ready, verify your settings with the above recommendations and revise the settings if required.

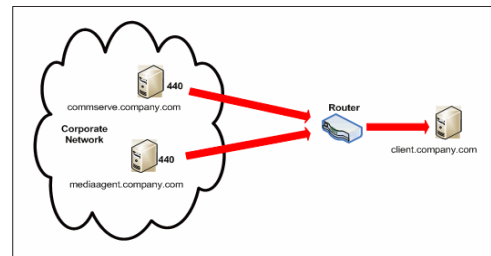


Connectivity between CommServe, MediaAgent, and the client is now established.

COMMSERVE CONNECTS TO THE CLIENT (ONE-WAY FIREWALL)

Consider the diagram that illustrates a direct connection setup where the CommServe opens tunnel connection towards the client.

The following sections explain the configuration required on the CommServe, MediaAgent, and the client to operate in this scenario.



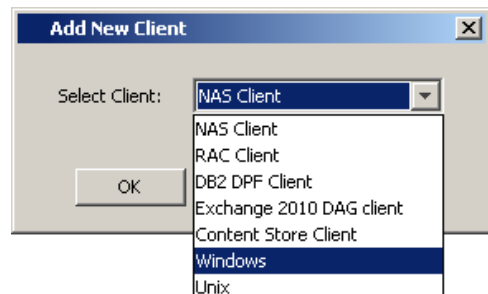
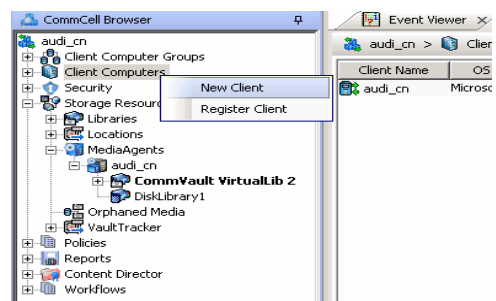
Review the following considerations before you begin.

- Make a note of the port configurations on your firewall and substitute them appropriately in the following instructions.
- Microsoft Internet Information Services (IIS) uses port number 443 by default. So if you have IIS running on a computer, then you will not be able to use port 443 for firewall configuration on that computer.

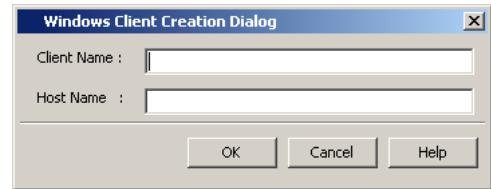
SETUP CONNECTION TO THE COMMSERVE

In this configuration, CommServe establishes tunnel connection with the client. Since the client is not yet available in the CommCell, follow the steps below to create a placeholder client and configure the firewall settings before installing the client.

- From the CommCell Console, right-click on the client computer node, and click **New Client**.
- Select **Windows** or **Unix** as applicable.



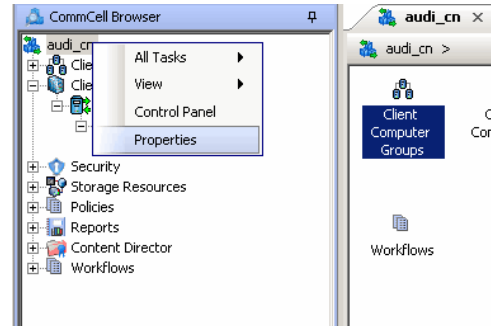
3. Provide the **Client Name** and the **Host Name** of the client computer to be installed.
 - The Client Name must be the same client name that you will provide during the client installation — the name by which the client will be identified in the CommCell Browser after installation. Ensure to provide the correct client name as the firewall program uses it to establish communication.
 - The Host Name must be either the fully qualified domain name of the client or the IP address that the CommServe should use to open tunnel connection to the client. If there is a NAT router between the client and the CommServe, provide the NAT IP address.



Click **OK**.

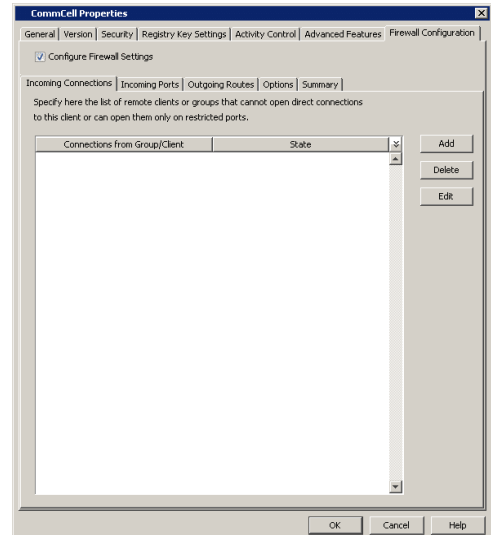
A placeholder client is created for firewall configuration use.

4. From the CommCell Console, right-click the CommServe computer and click **Properties**.

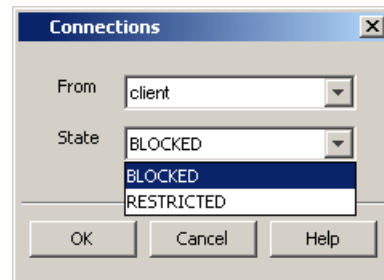


5. Click the **Firewall Configuration** tab.

6.
 - Click the **Incoming Connections** tab.
 - Click **Add**.



7.
 - In the **From** field, select the name of the placeholder client you just added.
 - In the **State** field, select **Blocked**, since the CommServe does not open tunnel connection to the client.
 - Click **OK**.



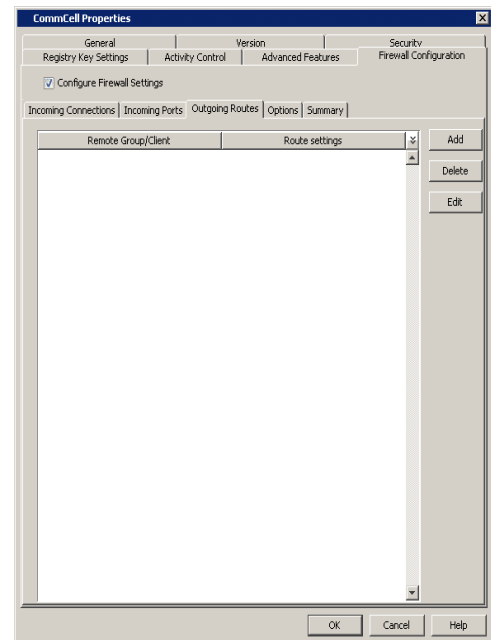
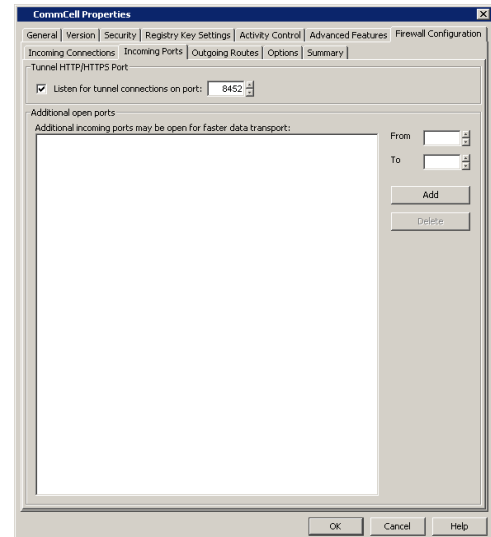
8.
 - Click the **Incoming Ports** tab.
 - As the CommServe does not receive connections from the client, not need to select **Listen for tunnel connections on port**.

9.

- Click the **Outgoing Routes** tab.
- Click **Add** to specify the outgoing route toward the proxy.

Outgoing routes are automatically created in the direct connectivity setup — manual entry is not required. However, you might want to create an entry if you wish to achieve one of the following.

- Enable HTTPS encryption for the tunnel or data traffic.
- Encrypt the data connections by forcing the connections into the tunnel. However, consider the following before using this option.
 - Direct connections always work faster. Forcing data connections into the tunnel might degrade performance of data protection operations.
 - If you wish to encrypt your backup data, you must rather configure encryption at the client level which offers more control and stores the data in encrypted form on the backup media as well.



10.

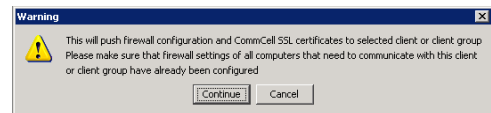
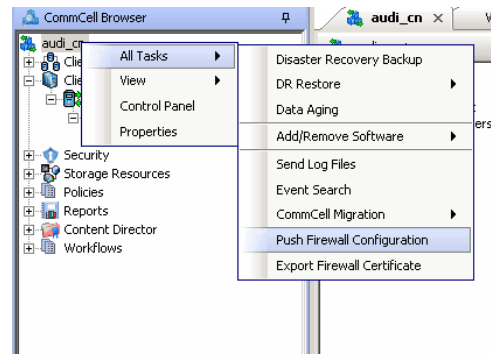
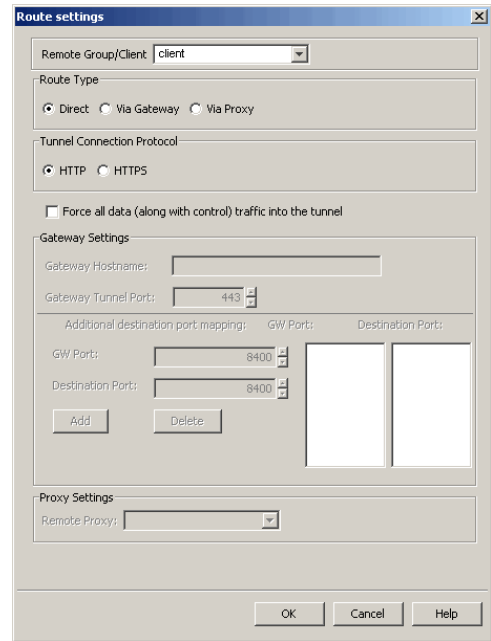
- Select the name of the placeholder client in **Remote Group/Client**.
- Select **Direct**.
- Select **HTTP**.
- **Force all data (along with control) traffic into the tunnel** option is not required as this route is not toward MediaAgent.
- Click **OK**.

- From the CommCell Console right-click the CommServe computer, click **All Tasks**, and click **Push Firewall Configuration**.

- Click **Continue**.

The CommServe is configured to open tunnel connections with the client.

Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.



INSTALL THE CLIENT

See Installation for step-by-step installation procedures to install the client.

During installation of the client, use one of the following firewall configuration sequence.

- CommServe can reach the Client/MediaAgent (Windows clients)
- CommServe can reach the Client/MediaAgent (Unix clients)

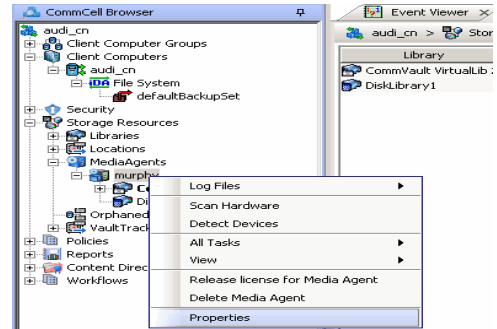
CONFIGURE THE COMMSERVE, MEDIAAGENT AND CLIENT

Use the following steps to establish incoming and outgoing connectivity details between the CommServe, MediaAgent, and the client computer.

The configuration required for the CommServe to connect to the client was done prior to installing the client. No additional configuration is required.

- To configure the MediaAgent, right-click the MediaAgent computer from the CommCell Console and click **Properties**.

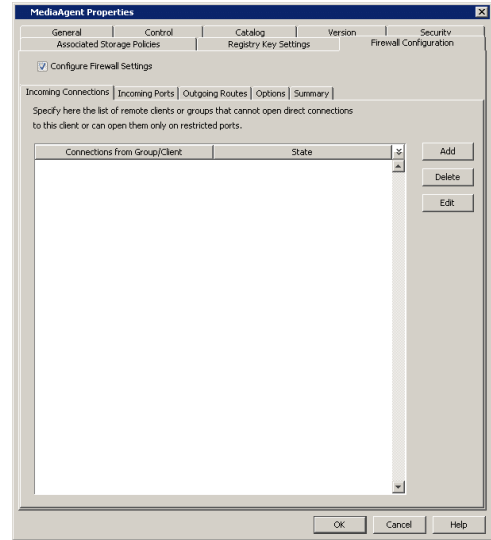
2. Click the **Firewall Configuration** tab.
3. From the **Incoming Connections** tab, click **Add**.



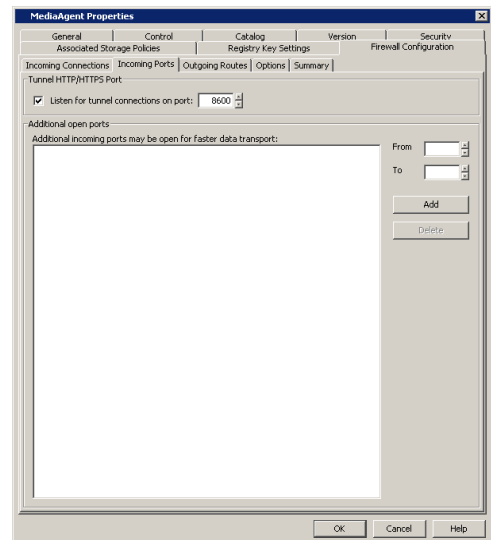
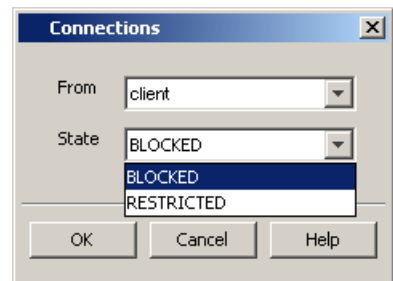
4.
 - In the **From** field, select the name of the client you just installed.
 - In the **State** field, select **Blocked**, since the MediaAgent does not open tunnel connection to the client.

Note that if the firewall allowed any connection from the client to the MediaAgent, then this entry is not required.

 - Click **OK** to continue.



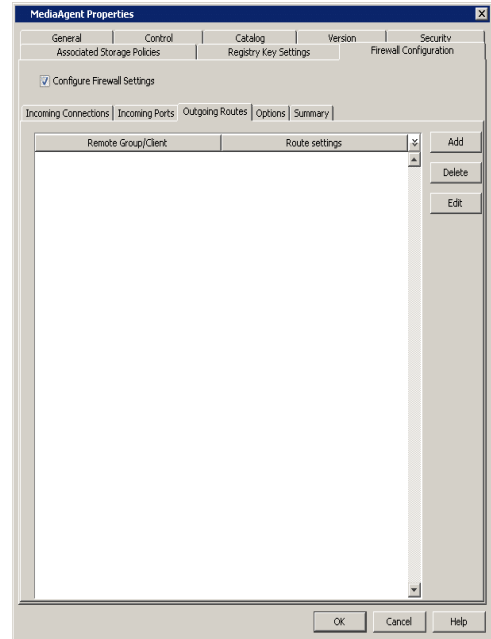
5.
 - Click the **Incoming Ports** tab.
 - Assuming that the MediaAgent opens tunnel connection to the client, there is no need to select **Listen for tunnel connections on port**.
 - Click **OK**.



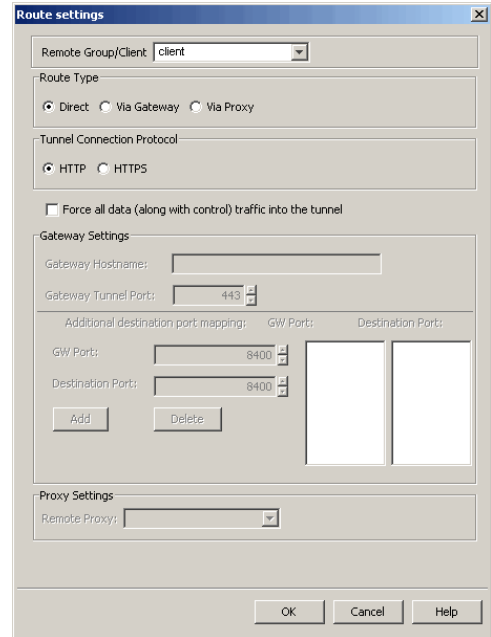
6.
 - Click the **Outgoing Routes** tab.
 - Click **Add** to specify the outgoing route toward the proxy.

Outgoing routes are automatically created in the direct connectivity setup — manual entry is not required. However, you might want to create an entry if you wish to achieve one of the following.

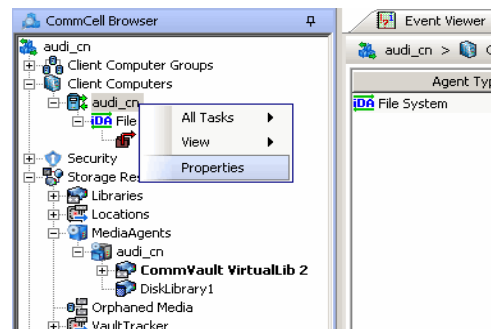
 - Enable HTTPS encryption for the tunnel or data traffic.
 - Encrypt the data connections by forcing the connections into the tunnel. However, consider the following before using this option.
 - Direct connections always work faster. Forcing data connections into the tunnel might degrade performance of data protection operations.
 - If you wish to encrypt your backup data, you must rather configure encryption at the client level which offers more control and stores the data in encrypted form on the backup media as well.



7.
 - Select the client name in the **Remote Group/Client** field.
 - Select **Direct**.
 - Select **HTTP**.
 - Select **Force all data (along with the control) traffic into the tunnel** to force the data traffic into the control tunnel. This automatically encrypts the data connection.
 - Click **OK**.

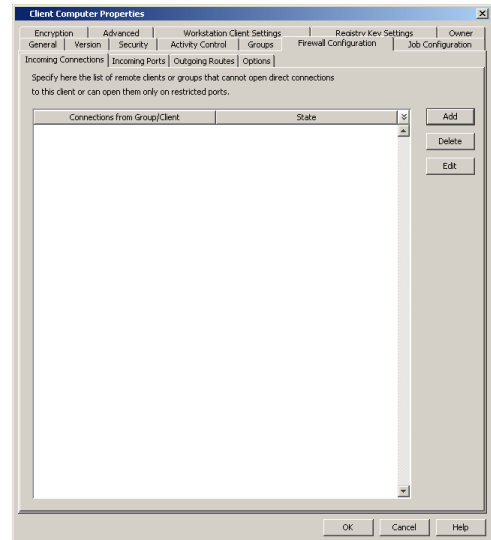


8. From the **Outgoing Routes** tab, click **OK**.
The MediaAgent is now configured to communicate with the client.
9. To configure the Client, right-click the client computer from the CommCell Console and click **Properties**.

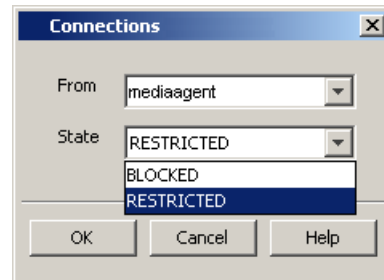
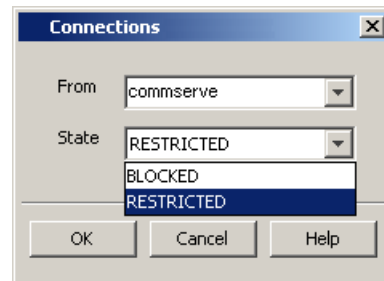


10. Click the **Firewall Configuration** tab.
11. From the **Incoming Connections** tab, click **Add**.

12.
 - In the **From** field, select the name of the CommServe computer.
 - In the **State** field, select **Restricted**, since the CommServe will connect to the Client through a port.
 - Click **OK**.



13.
 - Click **Add** again to specify the MediaAgent connection details.
 - In the **From** field, select the name of the MediaAgent computer.
 - In the **State** field, select **Restricted**, since the MediaAgent will connect to the Client through a port.
 - Click **OK**.

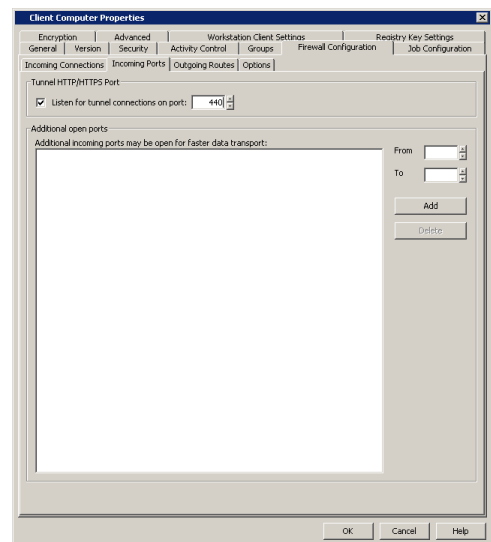


14.
 - Click the **Incoming Ports** tab.
 - Select **Listen for tunnel connections on port** and specify the incoming port number on which the firewall will allow connections from the CommServe and the MediaAgent.
 - **Additional Open Ports:** You can speed up the data transfer by opening additional ports towards the client on the firewall and recording them as open in this screen. Specify the range of ports in the **Additional open ports** area, **From** and **To** fields. Click **Add** to add the ports. To remove a port from the listing, select the port and click **Delete**. The ports must be within the range of 1024 - 65000. Ensure that the ports specified here are not used by other applications.

Review the following recommendations.

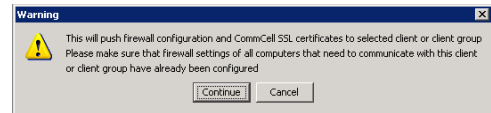
- For backups to MediaAgents with **Optimize for concurrent LAN backups** option unchecked, opening additional incoming ports improves the backup performance. The number of open ports should correspond to the number of simultaneously running backup streams.
- For ContinuousDataReplicator and Workstation Backup destination computers, opening additional incoming ports improves the replication performance.

- Click **OK**.



15. From the CommCell Console, right-click the client computer and click **All Tasks | Push Firewall Configuration**. This updates the firewall configuration files on the client computer.

- Click **Continue**.
The client is configured to communicate with the CommServe and MediaAgent.
Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.
- From the CommCell Console, right-click the client computer and click **All Tasks | Check Readiness**. The results are displayed in **Client Connectivity** dialog box.
If the client computer is not ready, verify your settings with the above recommendations and revise the settings if required.

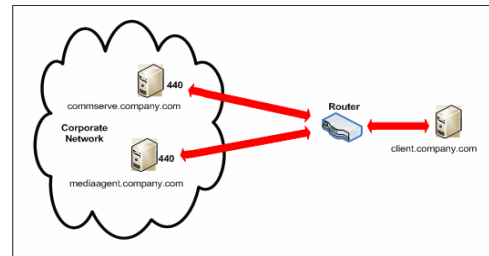


Connectivity between CommServe, MediaAgent, and the client is now established.

CLIENT AND COMMSERVE CONNECT TO EACH OTHER (TWO-WAY FIREWALL)

Consider the diagram that illustrates a direct connection setup where the client, CommServe and MediaAgent open tunnel connection between them.

The following sections explain the configuration required on the CommServe, MediaAgent, and the client to operate in this scenario.



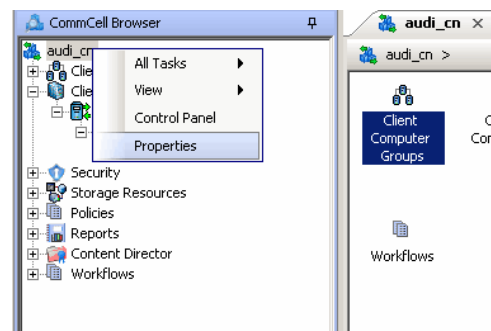
Review the following considerations before you begin.

- Make a note of the port configurations on your firewall and substitute them appropriately in the following instructions.
- Microsoft Internet Information Services (IIS) uses port number 443 by default. So if you have IIS running on a computer, then you will not be able to use port 443 for firewall configuration on that computer.

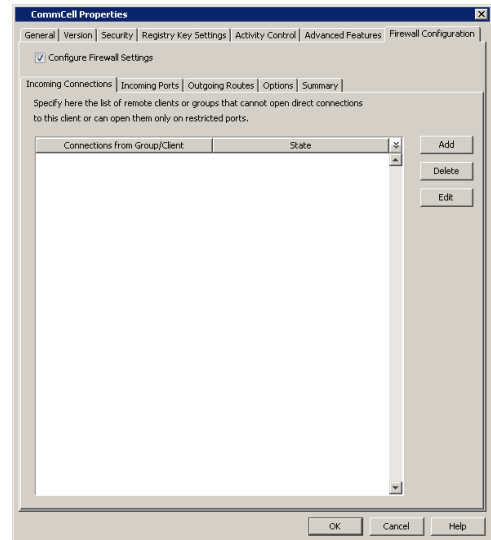
SETUP CONNECTION TO THE COMMSERVE

Before installing the client, you will have to provide an incoming port number on which the CommServe will receive tunnel connections from the client. The following steps explain the configurations required for this purpose.

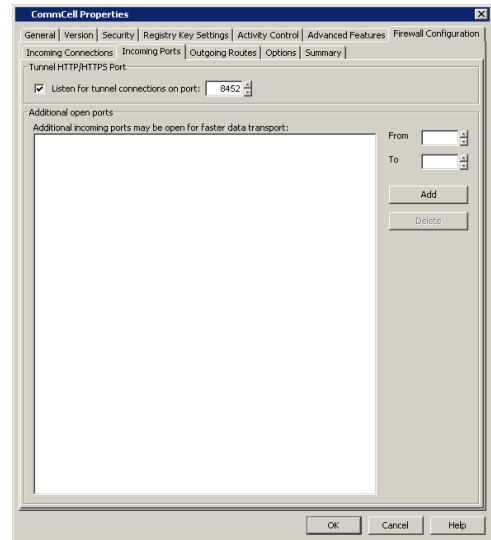
- From the CommCell Console, right-click the CommServe computer and click **Properties**.
- Click the **Firewall Configuration** tab.



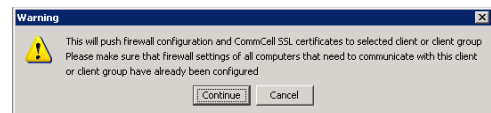
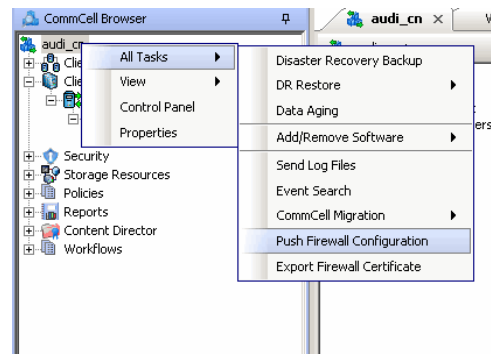
3.
 - Click the **Incoming Ports** tab.
 - Select **Listen for tunnel connections on port** and specify the port number on which the incoming tunnel connection is received.
 - Click **OK**.



4. From the CommCell Console, right-click the CommServe computer and click **All Tasks | Push Firewall Configuration**.



5. Click **Continue**.
The specified configuration is saved.
Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.



INSTALL THE CLIENT

In this configuration the client and the CommServe establish connection between them using one or more ports. To install the client across a firewall in this setup, you will have to specify the path to reach the CommServe computer. During installation of the client, use one of the following firewall configuration sequence.

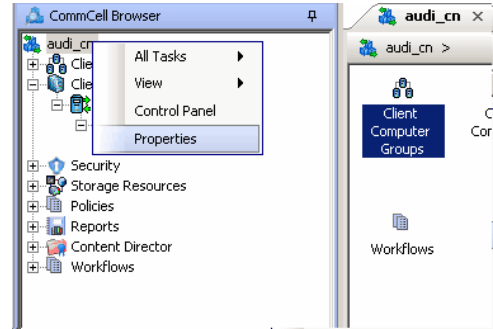
- Client/MediaAgent and CommServe can reach each other (Windows clients)

- Client/MediaAgent and CommServe can reach each other (Unix clients)

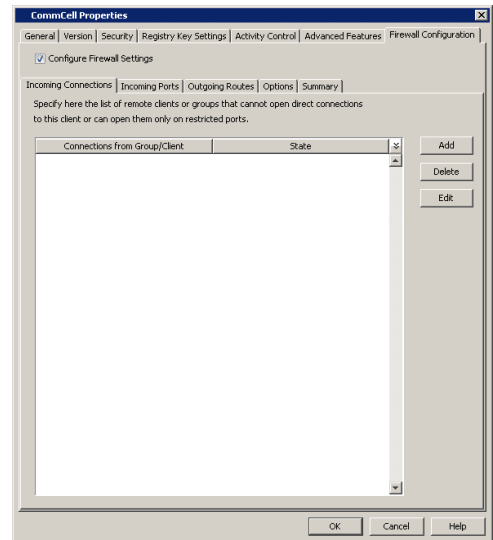
CONFIGURE THE COMMSERVE, MEDIAAGENT AND CLIENT

Use the following steps to establish incoming and outgoing connectivity details between the CommServe, MediaAgent, and the client computer.

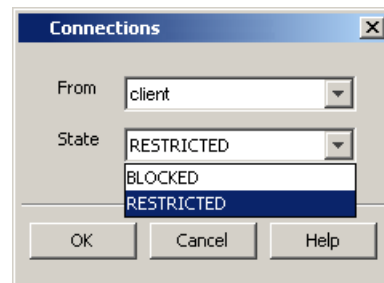
1. To configure the CommServe, right-click the CommServe computer from the CommCell Console and click **Properties**.



2. Click the **Firewall Configuration** tab.
3. From the **Incoming Connections** tab, click **Add**.



4.
 - In the **From** field, select the name of the client you just installed.
 - In the **State** field, select **Restricted**, since the client can reach the CommServe.
 - Click **OK**.



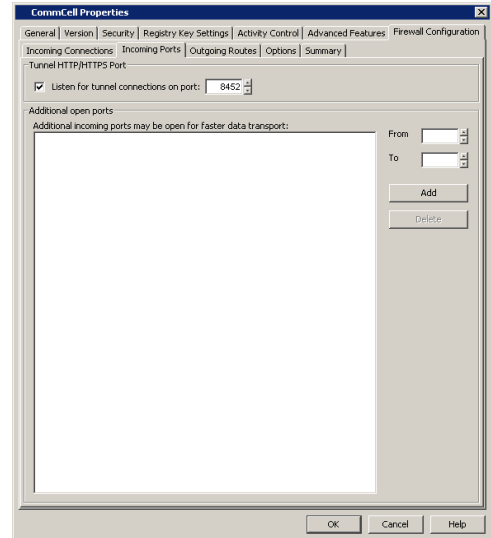
5.
 - Click the **Incoming Ports** tab. You will see the tunnel port already specified on the CommServe.
 - **Additional Open Ports:** For components that handle data transfer (for example, MediaAgent, File System iDataAgent, etc.), you can speed up the data transfer by opening additional ports on the firewall and recording them as open in this screen. Specify the range of ports in the **Additional open ports** area, **From** and **To** fields. Click **Add** to add the ports. To remove a port from the listing, select the port and click **Delete**. The ports must be within the range of 1024 - 65000. Ensure that the ports specified here are not used by other applications.

Review the following recommendations.

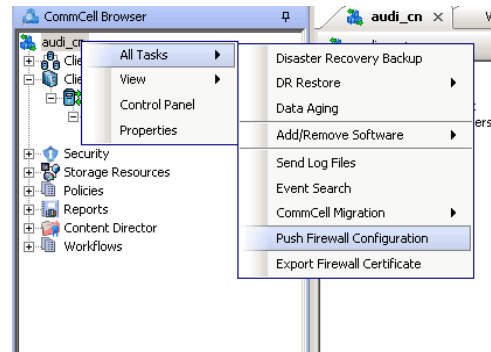
- For MediaAgents involving multi-stream restores, opening additional ports increases the restore performance. The number of open ports should correspond to the number of simultaneously running restore streams.
- For MediaAgents with **Optimize for concurrent LAN backups** option enabled, opening the incoming port of the Bull Calypso Communications Service improves the backup performance.

- For MediaAgents performing SnapProtect operations with Data Replicator snap engine, opening additional ports increases the backup performance.
- For ContinuousDataReplicator and Workstation Backup destination computers, opening additional incoming ports improves the replication performance.

- Click **OK**.



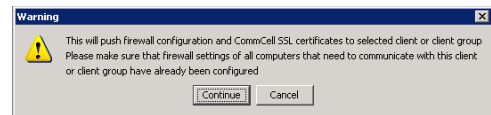
6. From the CommCell Console, right-click the CommServe computer and click **All Tasks | Push Firewall Configuration**.



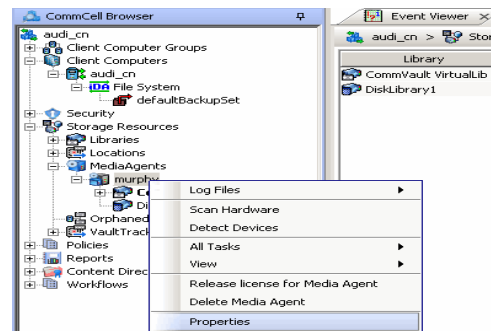
7. Click **Continue**.

The CommServe is configured to receive communication from the client.

Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.



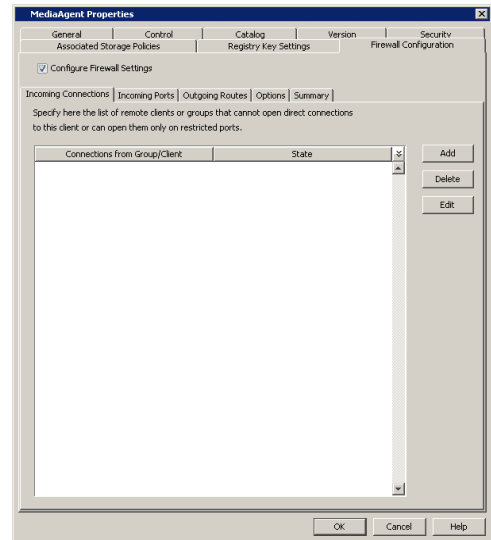
8. To configure the MediaAgent, right-click the MediaAgent computer from the CommCell Console and click **Properties**.



9. Click the **Firewall Configuration** tab.

10. From the **Incoming Connections** tab, click **Add**.

11.
 - In the **From** field, specify the name of the client you just installed.
 - In the **State** field, select **Restricted**, since the client can reach the MediaAgent.
 - Click **OK**.



12.
 - Click the **Incoming Ports** tab.
 - Select the **Listen for tunnel connections on port** option and specify the tunnel port through which connections from the client are received on the MediaAgent computer.
 - **Additional Open Ports:** For components that handle data transfer (for example, MediaAgent, File System iDataAgent, etc.), you can speed up the data transfer by opening additional ports on the firewall and recording them as open in this screen. Specify the range of ports in the **Additional open ports** area, **From** and **To** fields. Click **Add** to add the ports. To remove a port from the listing, select the port and click **Delete**. The ports must be within the range of 1024 - 65000. Ensure that the ports specified here are not used by other applications.

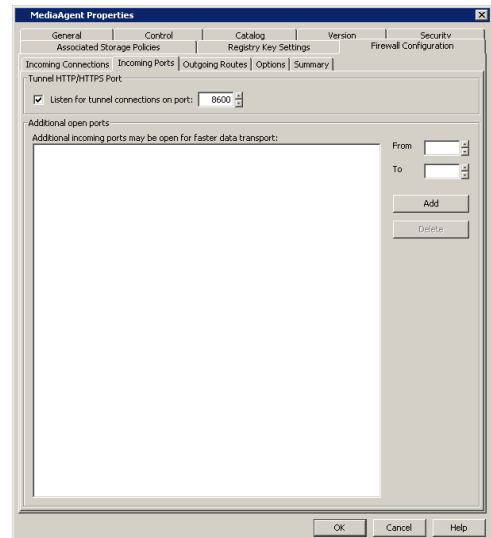
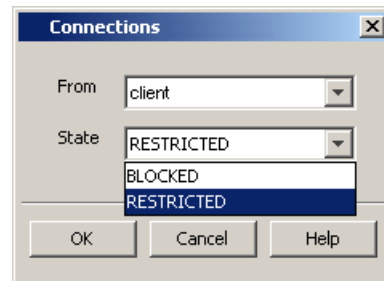
Review the following recommendations.

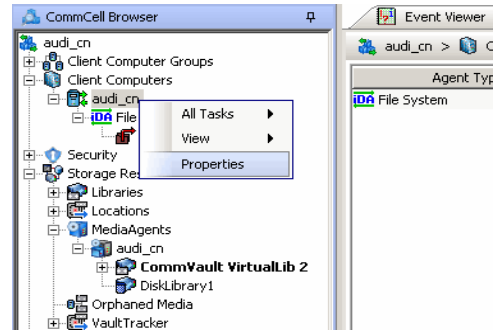
- For MediaAgents involving multi-stream restores, opening additional ports increases the restore performance. The number of open ports should correspond to the number of simultaneously running restore streams.
- For MediaAgents with **Optimize for concurrent LAN backups** option enabled, opening the incoming port of the Bull Calypso Communications Service improves the backup performance.
- For MediaAgents performing SnapProtect operations with Data Replicator snap engine, opening additional ports increases the backup performance.
- For ContinuousDataReplicator and Workstation Backup destination computers, opening additional incoming ports improves the replication performance.

- Click **OK**.

The MediaAgent is now configured to receive communication from the client.

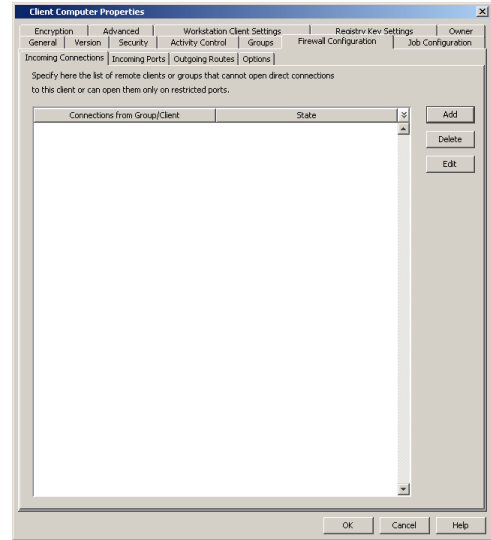
13. To configure the Client, right-click the client computer from the CommCell Console and click **Properties**.



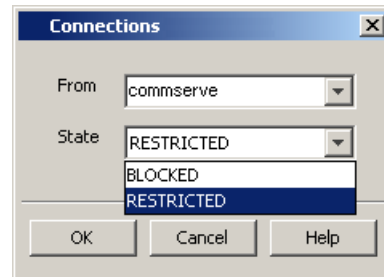


14. Click the **Firewall Configuration** tab.

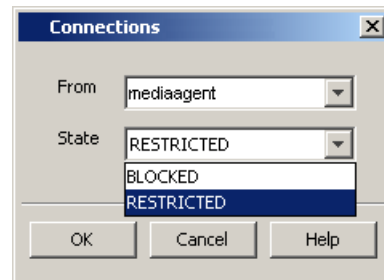
15. From the **Incoming Connections** tab, click **Add**.



- 16.
 - In the **From** field, specify the name of the CommServe computer.
 - In the **State** field, select **Restricted**, since the Client can connect to the CommServe.
 - Click **OK**.



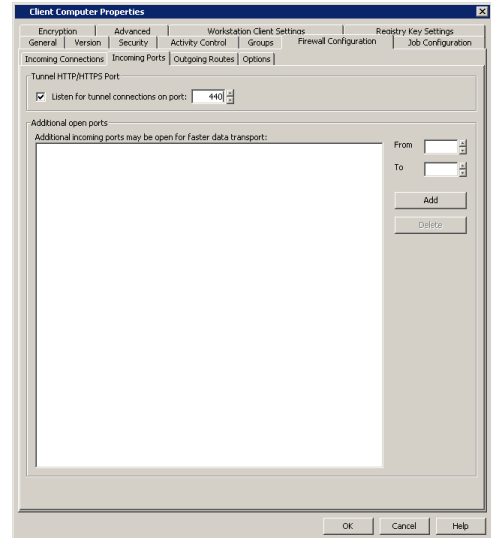
- 17.
 - Click **Add** again to specify the MediaAgent connection details.
 - In the **From** field, specify the name of the MediaAgent computer.
 - In the **State** field, select **Restricted**, since the Client can connect to the MediaAgent.
 - Click **OK**.



- 18.
 - Click the **Incoming Ports** tab.
 - Select the **Listen for tunnel connections on port** option and specify the incoming port number on which the firewall will allow connections from the CommServe and the MediaAgent. The client will listen for incoming tunnel connections on this port.
 - **Additional Open Ports:** You can speed up the data transfer by opening additional ports towards the client on the firewall and recording them as open in this screen. Specify the range of ports in the **Additional open ports** area, **From** and **To** fields. Click **Add** to add the ports. To remove a port from the listing, select the port and click **Delete**. The ports must be within the range of 1024 - 65000. Ensure that the ports specified here are not used by other applications.

Review the following recommendations.

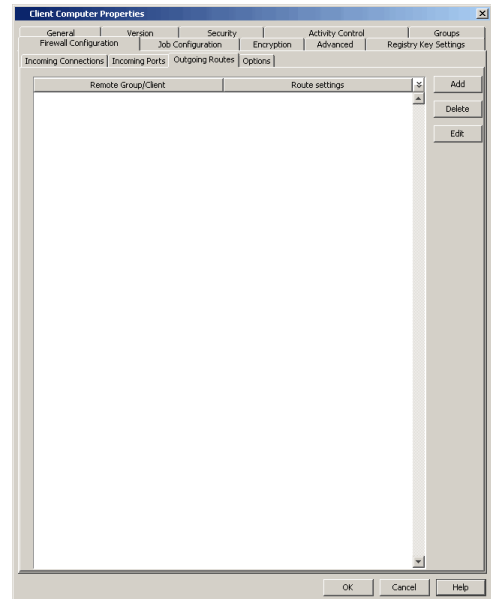
- For backups to MediaAgents with **Optimize for concurrent LAN backups** option unchecked, opening additional incoming ports improves the backup performance. The number of open ports should correspond to the number of simultaneously running backup streams.
- For ContinuousDataReplicator and Workstation Backup destination computers, opening additional incoming ports improves the replication performance.
- Click **OK**.



- 19.
- Click the **Outgoing Routes** tab.
 - Click **Add**.

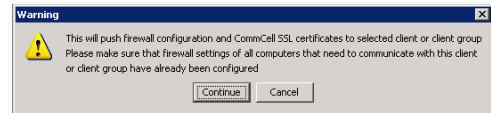
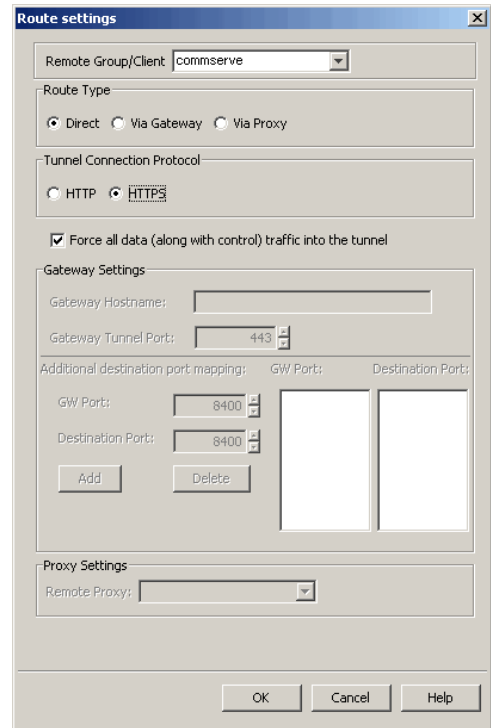
Outgoing routes are automatically created in the direct connectivity setup — manual entry is not required. However, you might want to create an entry if you wish to achieve one of the following.

- Enable HTTPS encryption for the tunnel or data traffic.
- Encrypt the data connections by forcing the connections into the tunnel. However, consider the following before using this option.
 - Direct connections always work faster. Forcing data connections into the tunnel might degrade performance of data protection operations.
 - If you wish to encrypt your backup data, you must rather configure encryption at the client level which offers more control and stores the data in encrypted form on the backup media as well.



- 20.
- Select the CommServe name in **Remote Group/Client**.
 - Select **Direct**.
 - Select **HTTPS** protocol. This will enable authentication and encryption for tunnel connections.
 - **Force all data (along with control) traffic into the tunnel** option is not required as this route is not toward MediaAgent.
 - Click **OK**.

21. From the CommCell Console, right-click the client computer and click **All Tasks | Push Firewall Configuration**. This updates the firewall configuration files on the client computer.
22. Click **Continue**.
The client is configured to communicate with the CommServe and MediaAgent.
Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.
23. From the CommCell Console, right-click the client computer and click **All Tasks | Check Readiness**. The results are displayed in **Client Connectivity** dialog box.
If the client computer is not ready, verify your settings with the above recommendations and revise the settings if required.



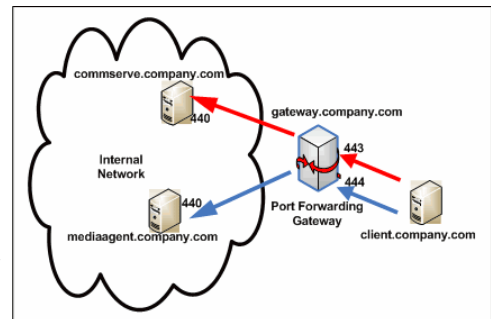
Connectivity between CommServe, MediaAgent, and the client is now established.

OPERATING THROUGH A PORT-FORWARDING GATEWAY

There are cases where direct connectivity setups do not work. Imagine a situation where the CommServe and MediaAgent are located inside a company's internal network, and the entire network is exposed to the outside world through a single IP address. Typically this IP address belongs to a firewall/gateway that works as a NAT device for connections from the internal network to the outside.

In scenarios like this, you can establish a port-forwarding at the gateway to forward incoming connections on specific ports to certain machines on the internal network (on specific ports). You can then configure the client to open a direct connection to the port-forwarder's IP on a specific port to reach a particular internal server. This creates a custom route from client towards the internally running server(s).

Consider the diagram on the right that illustrates the setup. The following sections explain how to configure the software to operate in this setup.



Review the following considerations before you begin.

- Make a note of the port configurations in your setup and substitute them in the following instructions.
- Microsoft Internet Information Services (IIS) uses port number 443 by default. So if you have IIS running on a computer, then you will not be able to use port 443 for firewall configuration on that computer.
- Any additional destination port specified in the outgoing connection routes of the client must also be defined in the incoming port list of the remote client (CommServe or MediaAgent).

CONFIGURE THE PORT-FORWARDING GATEWAY

A port-forwarding gateway sends incoming connections to specific machines on the internal network based on the incoming connection's destination port number. With reference to our illustration above, the following port-forwarding must be configured on the gateway.

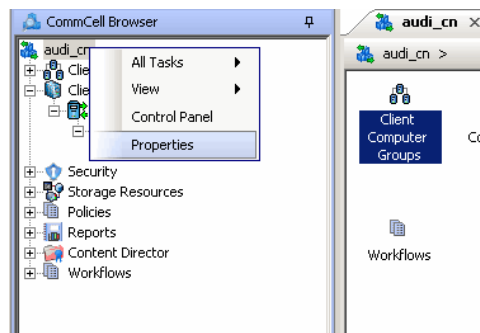
- Connections to gateway.company.com on port 443 must be forwarded to the internally running commserve.company.com on port 440.
- Connections to gateway.company.com on port 444 must be forwarded to the internally running mediaagent.company.com on port 440.

Note that there is no restriction on the internal port numbers. They need not be the same as shown in the illustration. Also, for machines in the internal network, neither the IP addresses nor the names have to be reachable or resolvable from outside.

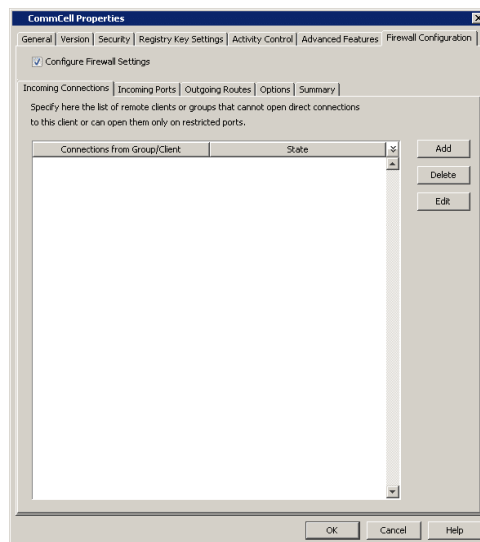
SETUP CONNECTION TO THE COMMSERVE

This procedure assumes that the CommServe is installed and available behind the gateway. The following steps explain the configurations required to connect to the CommServe before installing the client.

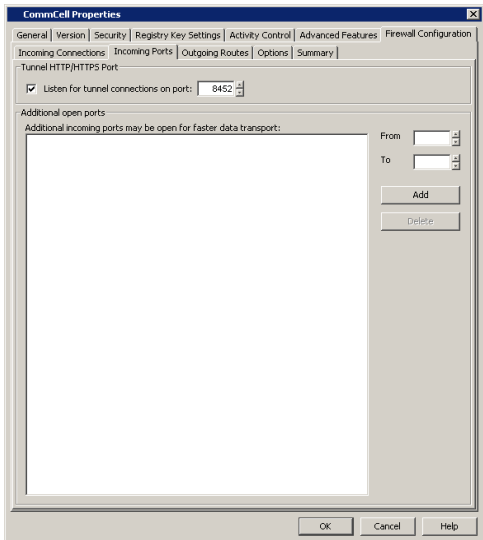
1. From the CommCell Console, right-click the CommServe computer and click **Properties**.



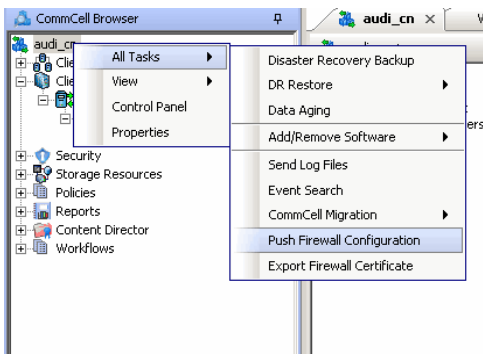
2. Click the **Firewall Configuration** tab.



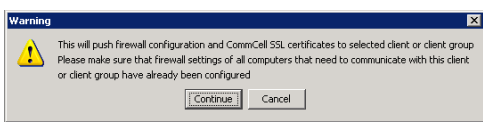
3.
 - Click the **Incoming Ports** tab.
 - Select **Listen for tunnel connections on port** and enter **440** as the port number. The gateway will forward connections to commserve.company.com:440 when the gateway receives them from outside on port 443.
 - Click **OK**.



- From the CommCell Console, right-click the CommServe computer and click **All Tasks | Push Firewall Configuration**.



- Click **Continue**.
The specified configuration is saved.
Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.



INSTALL THE CLIENT

See Installation for step-by-step installation procedures to install the client.

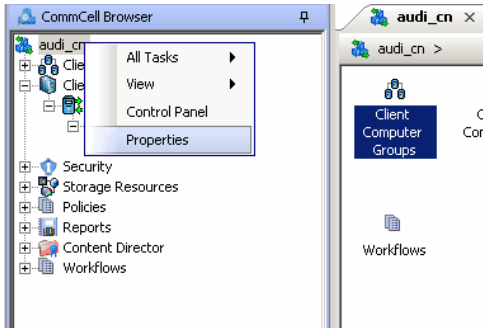
During installation, provide the gateway information through which the CommServe computer can be reached. The install program communicates to the CommServe using this information. Use one of the following firewall configuration sequence.

- CommServe can be Reached through a Port Forwarding Gateway (Windows clients)
- CommServe can be Reached through a Port Forwarding Gateway (Unix clients)

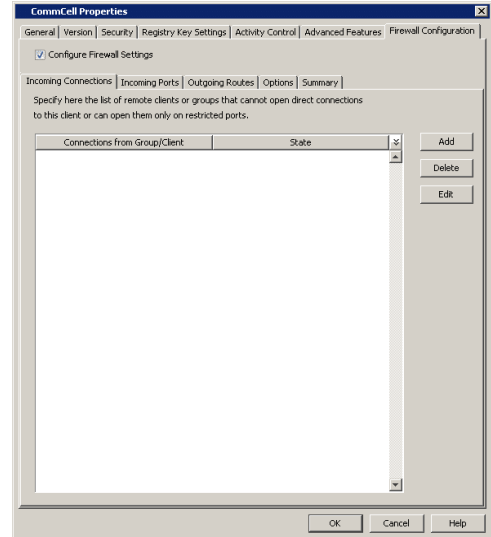
CONFIGURE THE COMMSERVE, MEDIAAGENT AND CLIENT

The previous configurations provided a path to reach the CommServe for installation purposes. To enable data protection operations between the two computers, you will have to establish the communication path between them. Perform the following steps to establish the communication route.

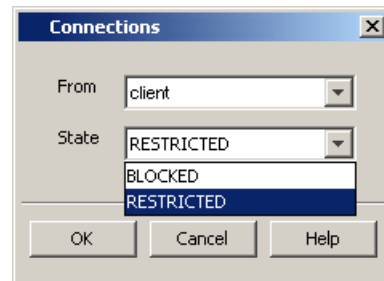
- To configure the CommServe, right-click the CommServe computer from the CommCell Console and click **Properties**.



2. Click the **Firewall Configuration** tab.
3.
 - Click the **Incoming Connections** tab.
 - Click **Add**.



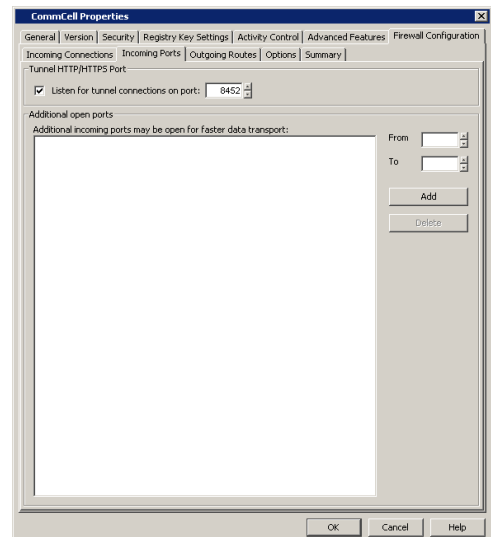
4.
 - In the **From** field, specify the name of the client outside the gateway you just installed.
 - In the **State** field, specify the status of the connection from the client. Since the connection is restricted through a gateway, select **Restricted**.
 - Click **OK**.



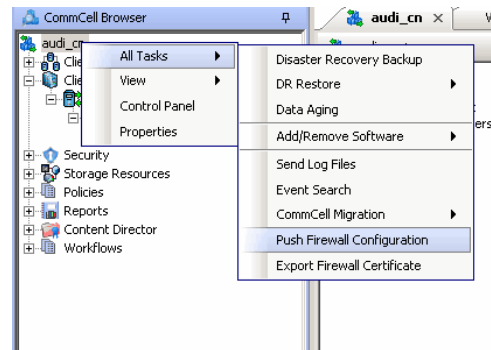
5.
 - Click the **Incoming Ports** tab.

You will see the tunnel port already specified on the CommServe with port number 440.

 - Click **OK**.



6. From the CommCell Console right-click the CommServe computer and click **All Tasks** | **Push Firewall Configuration**.



7. Click **Continue**.
The CommServe is configured to receive communication from the client.
Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.

8. From the CommCell Console, right-click the client computer and click **All Tasks | Check Readiness**. The results are displayed in **Client Connectivity** dialog box.
If the client computer is not ready, verify your settings with the above recommendations and revise the settings if required.

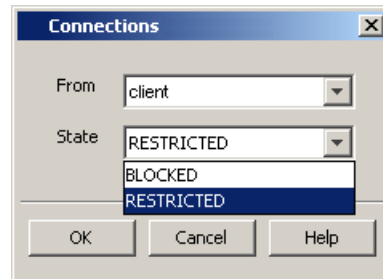
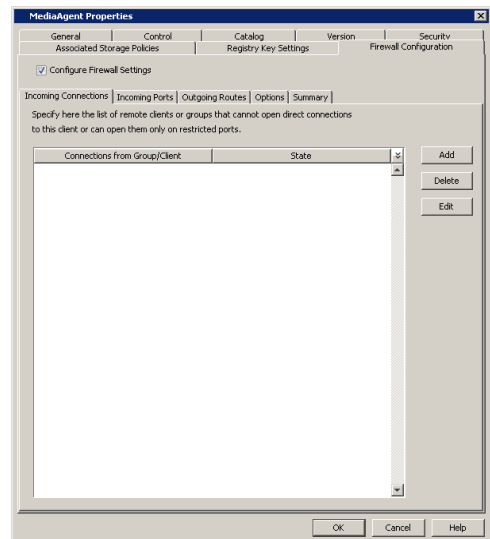
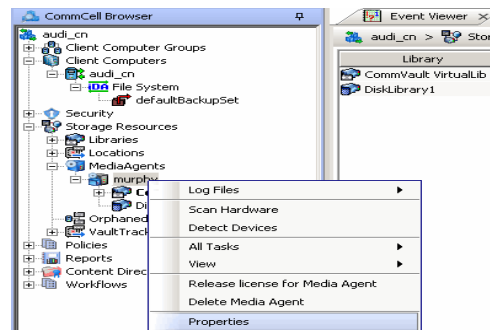
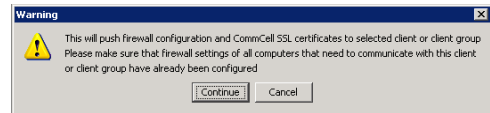
9. To configure the MediaAgent, right-click the MediaAgent computer from the CommCell Console and click **Properties**.

10. Click the **Firewall Configuration** tab.

11. From the **Incoming Connections** tab, click **Add**.

12.
 - In the **From** field, specify the name of the client outside the gateway you just installed.
 - In the **State** field, specify the status of the connection from the client. Since the connection is restricted through a gateway, select **Restricted**.
 - Click **OK**.

13.
 - Click the **Incoming Ports** tab.



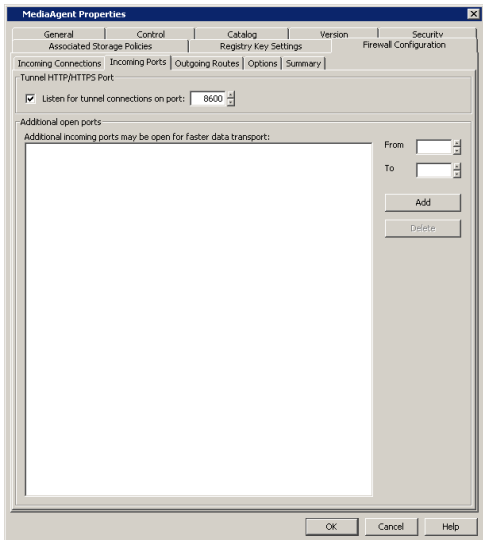
- Select **Listen for tunnel connections on port** and enter **440** as the port number. The gateway will forward connections to **mediaagent.company.com:440** when the gateway receives them from outside on port 444.
- **Additional Open Ports:** For components that handle data transfer (for example, MediaAgent, File System iDataAgent, etc.), you can open and port-forward additional ports on the gateway to speed up the data transport. Note that the additional ports may be the same on the MediaAgent and on the gateway since the gateway has the ability to translate externally visible port numbers to the actual port numbers on the MediaAgent.

In this screen you need to configure the range of ports used for listening to additional incoming connections from the clients. The mapping on how these ports are exported by the gateway must be defined in the outgoing route from the client towards the MediaAgent. (See Step 21) Specify the range of ports in the **Additional open ports** area, **From** and **To** fields. Click **Add** to add the ports. To remove a port from the listing, select the port and click **Delete**. The ports must be within the range of 1024 - 65000. Ensure that the ports specified here are not used by other applications.

Review the following recommendations:

- For MediaAgents involving multi-stream restores, opening additional ports increases the restore performance. The number of open ports should correspond to the number of simultaneously running restore streams.
 - For MediaAgents with **Optimize for concurrent LAN backups** option enabled, opening the incoming port of the Bull Calypso Communications Service improves the backup performance.
 - For MediaAgents performing SnapProtect operations with Data Replicator snap engine, opening additional ports increases the backup performance.
 - For ContinuousDataReplicator and Workstation Backup destination computers, opening additional incoming ports improves the replication performance.
- Click **OK**.

The MediaAgent is now configured to receive communication from the client.

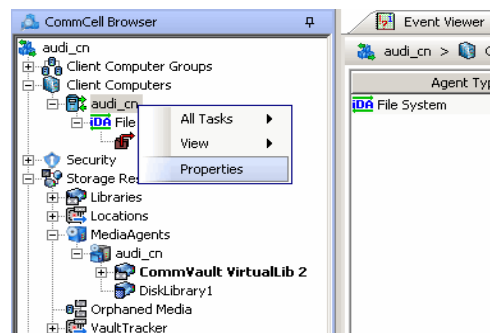


14. From the CommCell Console, right-click the client computer and click **All Tasks | Check Readiness**. The results are displayed in **Client Connectivity** dialog box.

If the client computer is not ready, verify your settings with the above recommendations and revise the settings if required.



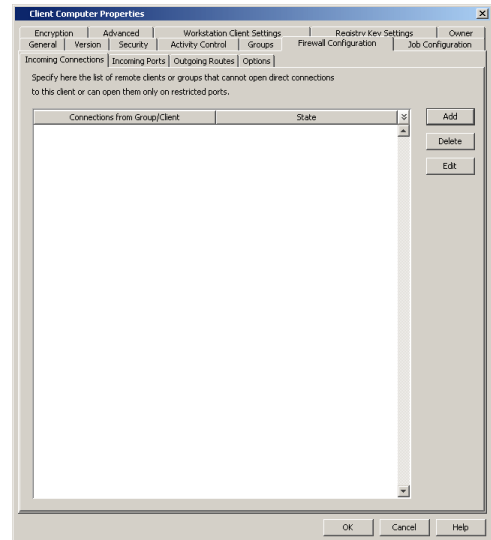
15. To configure the Client, right-click the client computer from the CommCell Console and click **Properties**.



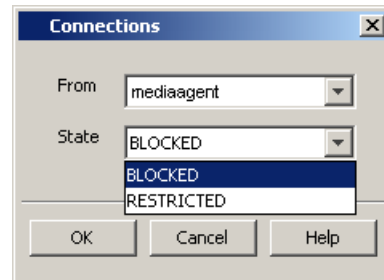
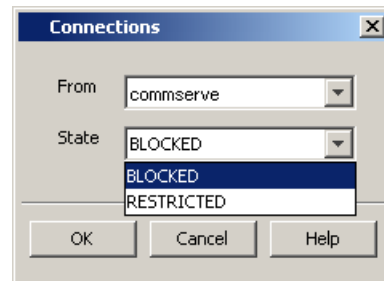
16. Click the **Firewall Configuration** tab.

17. From the **Incoming Connections** tab, click **Add**.

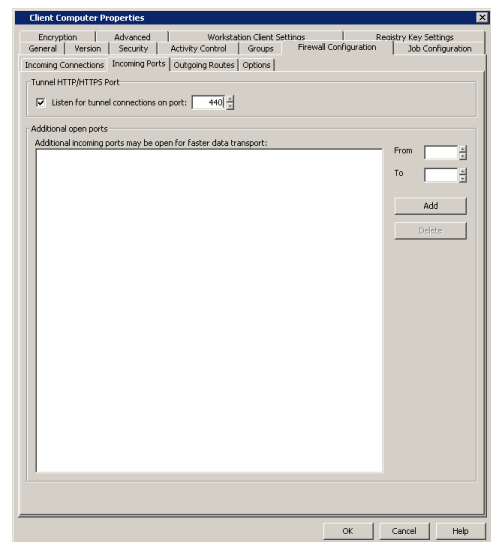
18.
 - In the **From** field, specify the name of the CommServe computer behind the gateway.
 - In the **State** field, specify the status of the connection from the CommServe. Since CommServe does not open connections towards the client, select **Blocked**.
 - Click **OK**.



19.
 - Click **Add** again to specify the MediaAgent connection details.
 - In the **From** field, specify the name of the MediaAgent computer behind the gateway.
 - In the **State** field, specify the status of the connection from the CommServe. Since MediaAgent does not open connections towards the client, select **Blocked**.
 - Click **OK**.

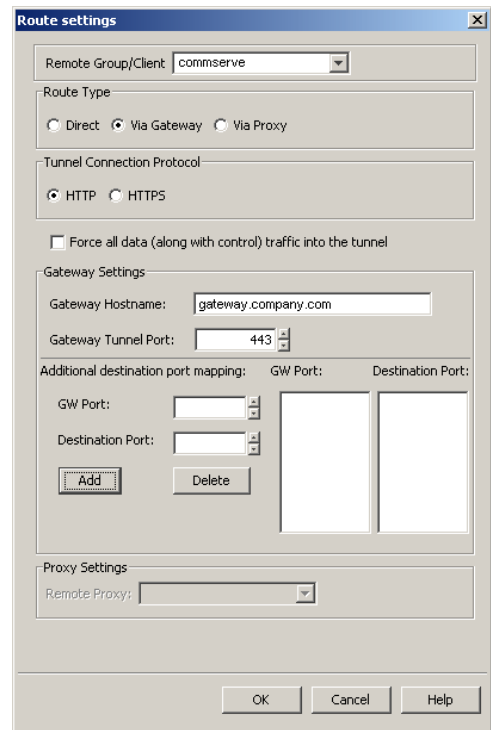
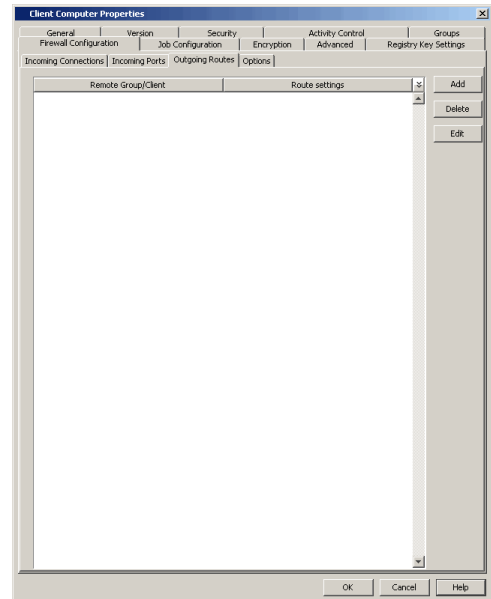


20.
 - Click the **Incoming Ports** tab.
 - As the client does not receive incoming connections from the CommServe or MediaAgent, there is no need to select **Listen for tunnel connections on port**.
 - Click **OK**.



21.
 - Click the **Outgoing Routes** tab.
 - Click **Add** to specify the outgoing connection route from this client towards the CommServe.

- 22.
- Select the CommServe name in **Remote Group/Client**.
 - Select **Via Gateway**.
 - **Force all data (along with control) traffic into the tunnel** option is not required as this route is not toward MediaAgent.
 - Enter the **Gateway Hostname** through which you can reach the CommServe. Referring to our diagram, it is gateway.company.com.
 - Enter the **Gateway Tunnel Port** through which the CommServe can be reached. Referring to the diagram above, this is port number 443.
 - **Additional destination port mapping:** If you want to configure additional destination ports, make sure that these ports are also defined on the CommServe, then you can establish mappings between those ports on the CommServe and the ports on the gateway which the client will connect to.
- To add destination port mapping, specify the incoming gateway port in **GW Port** and the mapping destination port in **Destination Port**. Click **Add** to add the port mapping. To remove a port from the listing, select the port and click **Delete**. The ports must be within the range of 1024 - 65000. Ensure that the ports specified here are not used by other applications.
- Click **OK**.

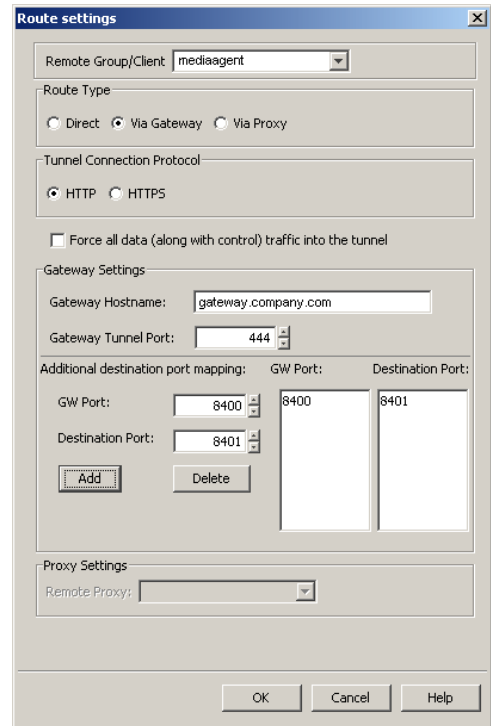


- 23.
- Click **Add** again to specify the outgoing connection route from this client towards the MediaAgent.
 - Select the MediaAgent in **Remote Group/Client**.
 - Select **Via Gateway**.
 - Select **Force all data (along with the control) traffic into the tunnel** to force the data traffic into the control tunnel. This automatically encrypts the data connection.
 - Enter the **Gateway Hostname** through which you can reach the CommServe. Referring to our diagram, it is gateway.company.com.
 - Enter the **Gateway Tunnel Port** through which the MediaAgent can be reached. Referring to the diagram above, this is port number 444.
 - **Additional destination port mapping:** If you want to configure additional destination ports, make sure that these ports are also defined on the MediaAgent (see Step 13), then you can establish mappings between those ports on the MediaAgent and the ports on the gateway which the client will connect to.

To add destination port mapping, specify the incoming gateway port in **GW Port**

and the mapping destination port in **Destination Port**. Click **Add** to add the port mapping. To remove a port from the listing, select the port and click **Delete**. The ports must be within the range of 1024 - 65000. Ensure that the ports specified here are not used by other applications.

- Click **OK**.



24. From the CommCell Console, right-click the client computer and click **All Tasks | Push Firewall Configuration**.

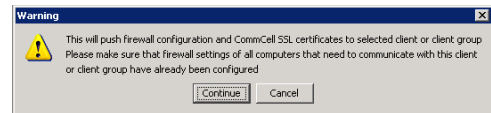
25. Click **Continue**.

The client is configured to communicate with the CommServe and MediaAgent computers behind the gateway.

Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.

26. From the CommCell Console, right-click the client computer and click **All Tasks | Check Readiness**. The results are displayed in **Client Connectivity** dialog box.

If the client computer is not ready, verify your settings with the above recommendations and revise the settings if required.



Connectivity between CommServe, MediaAgent, and the client is now established.

SECURITY CONSIDERATIONS

Since both MediaAgent and CommServe computers are in a way exposed to the outside world through port-forwarded connections, you might want to enable encryption and authentication for the tunnel connections. This can be done in one of the following ways.

- Select **HTTPS** for the **Tunnel Connection Protocol** in the **Outgoing Routes tab** on all outgoing routes.
- Select **Allow only HTTPS** for the **Incoming Tunnel Protocol** in the **Options** tab of the CommServe and MediaAgent. Once HTTPS has been enabled, the client and CommServe/MediaAgent will authenticate each other and set up tunnel encryption in accordance with the HTTPS standard.

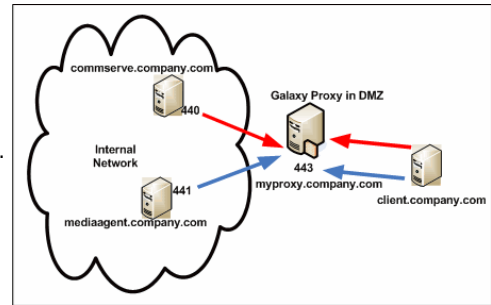
OPERATING THROUGH A DMZ USING CALYPSO PROXY

Calypso proxy is a special proxy configuration where a dedicated *iDataAgent* is placed in a Demilitarized Zone (DMZ) and the firewall(s) is configured to allow connections (from inside and outside networks) into the DMZ. The proxy, which is the agent running in the DMZ, authenticates, encrypts, and proxies accepted tunnel connections to connect the clients operating outside to clients operating inside. In effect, the Calypso proxy acts like a Private

Branch Exchange (PBX) that sets up secure conferences between dial-in client calls. With this setup, firewalls can be configured to disallow straight connections between inside and outside networks.

The diagram on right illustrates this setup where a client from outside communicates to the CommServe and MediaAgent operating in an internal network through the Calypso proxy.

The following sections describe the configuration required to operate the software in this setup.



Review the following considerations before you begin.

- The instructions given below are tailored to the component names and port numbers presented in the illustration. Make a note of the details in your setup and substitute them appropriately.
- Microsoft Internet Information Services (IIS) uses port number 443 by default. So if you have IIS running on a computer, then you will not be able to use port 443 for firewall configuration on that computer.

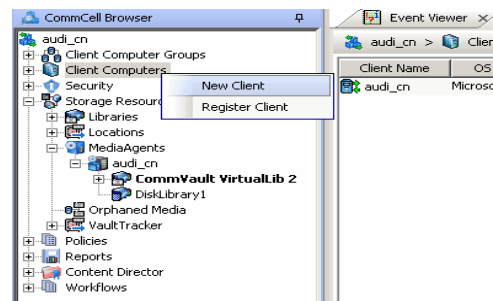
SET UP THE CALYPSO PROXY

The following sections explain the steps involved in creating the Calypso proxy.

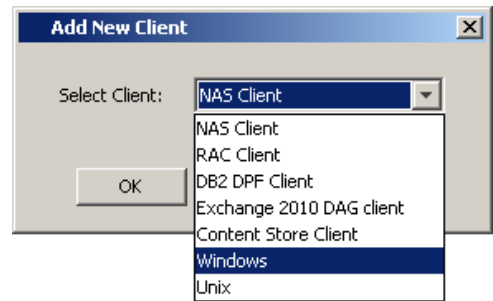
PRECONFIGURE THE CALYPSO PROXY

Follow the steps below to create and configure a placeholder for the Calypso proxy on your CommServe computer before installing it.

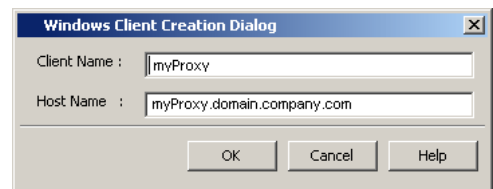
1. From the CommCell Console, right-click on the client computer node, and click **New Client**.



2. Select **Windows** or **Unix** as applicable.

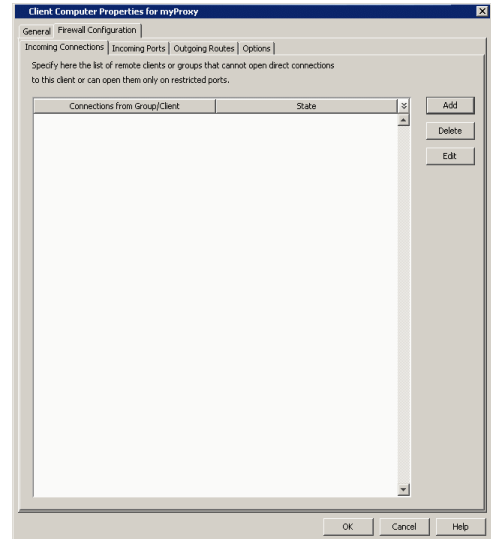
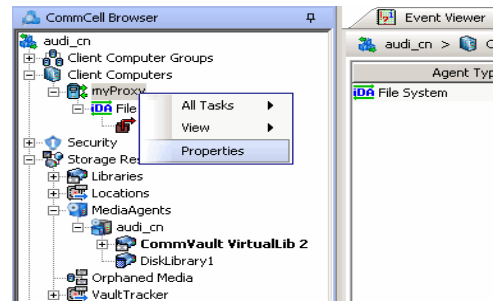


3.
 - Provide the **Client Name** and the **Host Name** you will use during your Calypso proxy installation.
 - Click **OK**.

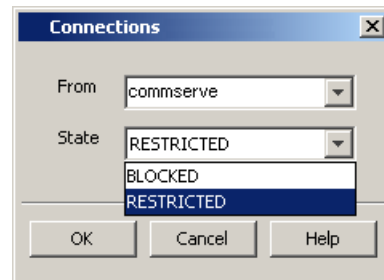


4. From the CommCell Console, right-click the client you just created, and click **Properties**.

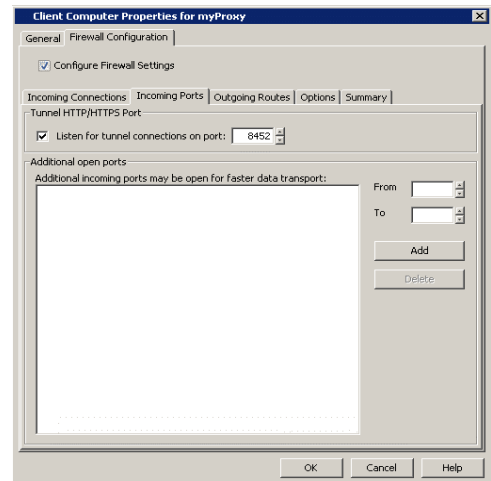
5.
 - Click the **Firewall Configuration** tab.
 - Click **Add**.



6.
 - In the **From** field, select the CommServe name.
 - In the **State** field, select **Restricted**.
 - Click **OK**.
 If you have a MediaAgent, repeat this step providing the MediaAgent computer name.

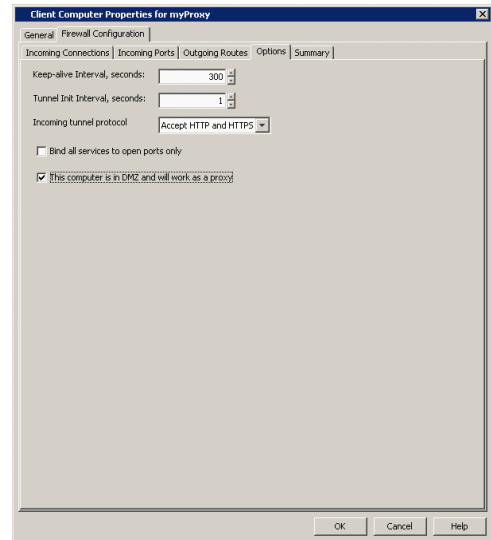


7.
 - Click the **Incoming Ports** tab.
 - Select **Listen for tunnel connections on port** and enter port number on which the Calypso proxy will listen from the CommServe.
 Write down the port number used as it will be needed during the Calypso proxy installation.

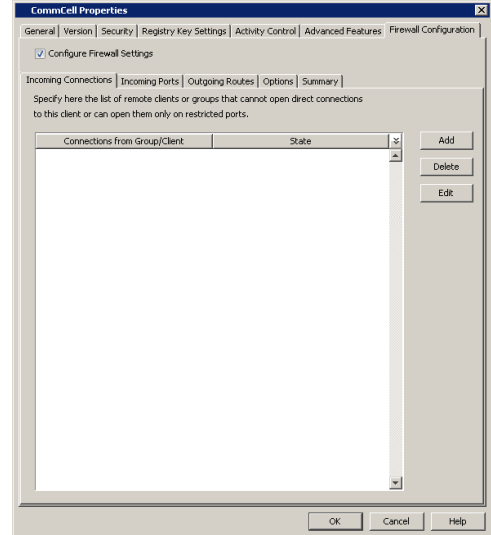
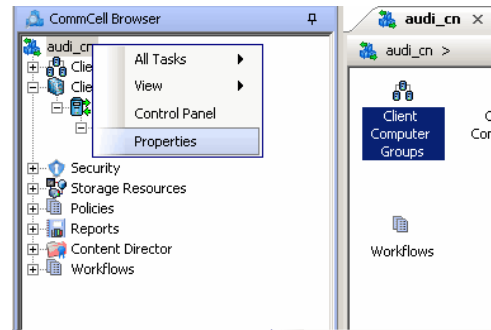


8.
 - Click the **Options** tab.
 - Select **This computer is in DMZ and will work as a proxy**.
 - Click **OK**.

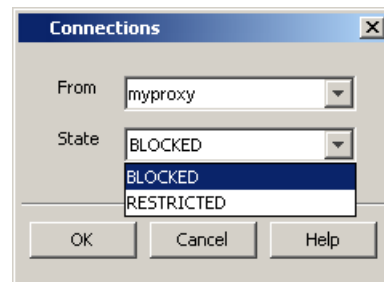
9. From the CommCell Console, right-click the CommServe computer and click **Properties**.



10.
 - Click the **Firewall Configuration** tab.
 - From the **Incoming Connections** tab, click **Add**.

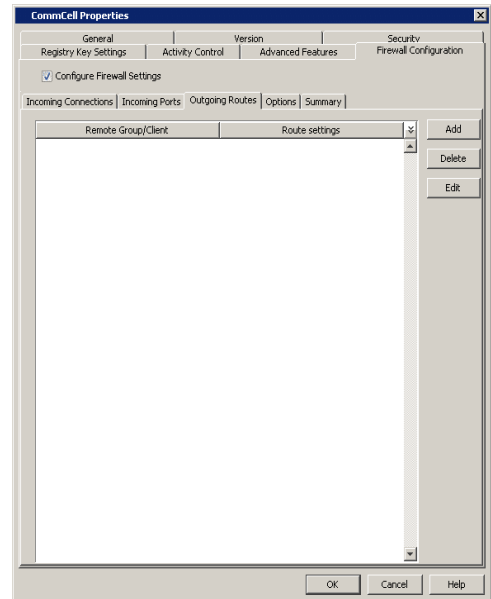


11.
 - In the **From** field, select the Calypso proxy computer.
 - In the **State** field, select **Blocked**.
 - Click **OK**.

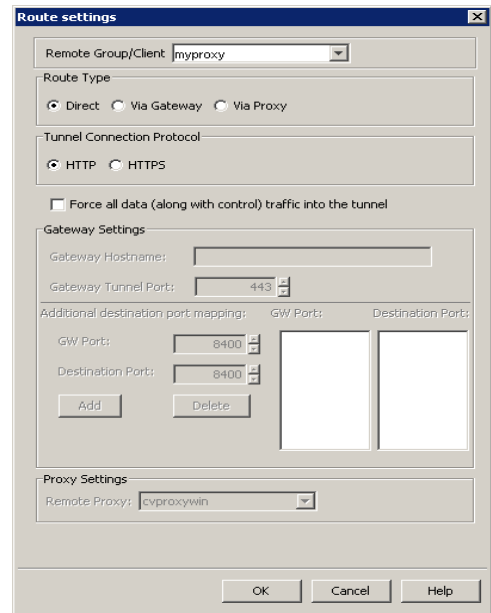


12.
 - Click the **Outgoing Routes** tab.

- Click **Add**.

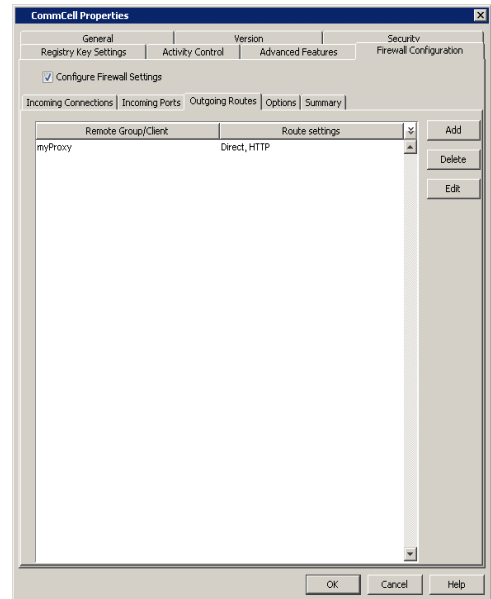


- 13.
- Select the Calypso proxy in **Remote Group/Client**.
 - Select **Direct**.
 - Click **OK**.

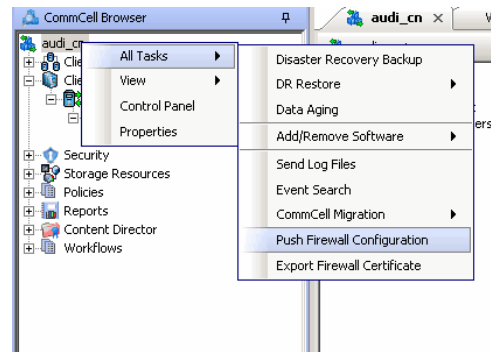


14. Click **OK**.

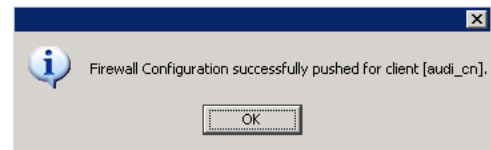
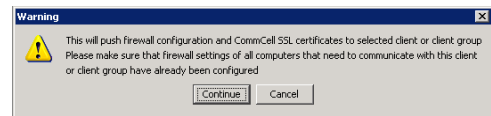
- From the CommCell Console right-click the CommServe computer, click **All Tasks**, and click **Push Firewall Configuration**.



- Click **Continue**.



- Click **OK**.
You are now ready to install the Calypso proxy.
Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.



INSTALL THE CALYPSO PROXY

Install a CommCell client (e.g., File System iDataAgent) in the DMZ. This will operate as the Calypso proxy. Since DMZ always receives connections from outside, the Calypso proxy in DMZ must communicate to the CommServe through tunnel connections initiated by the CommServe.

If firewall is enabled on the computer where the Calypso proxy will be installed, ensure there are open connections for the CommServe and client computers.

During the installation, use one of the following firewall configuration sequences:

- CommServe can reach the Client/MediaAgent (Windows clients)
- CommServe can reach the Client/MediaAgent (Unix clients)

After the installation is completed, open the CommCell Console, right-click the Calypso proxy computer and click **All Tasks | Push Firewall Configuration**.

INSTALL THE CLIENT

To install the client across the Calypso proxy, you will have to specify the path to reach the CommServe computer. The install program communicates to the CommServe using this information.

See Installation for step-by-step installation procedures to install the client. During installation, use one of the following firewall configuration sequences:

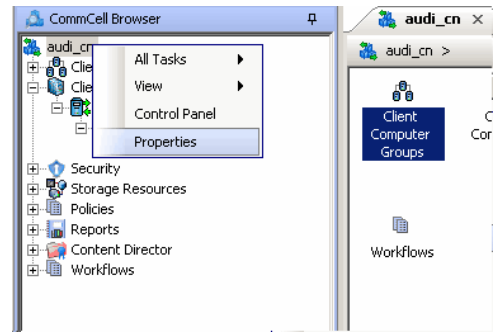
- CommServe can be Reached through a Proxy (Windows clients)

- CommServe can be Reached through a Proxy (Unix clients)

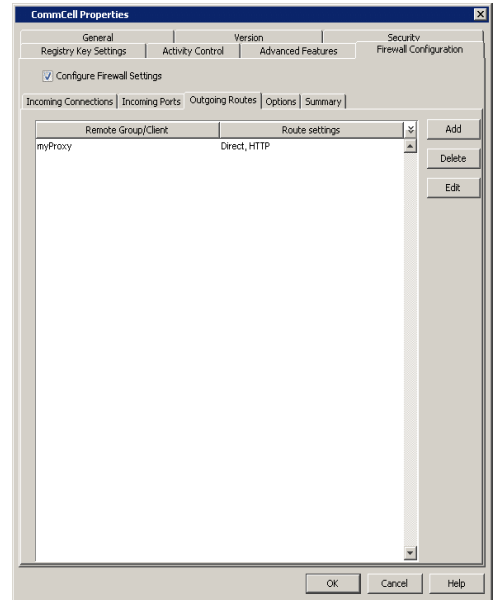
CONFIGURE THE COMMSERVE, MEDIAAGENT AND CLIENT

The following steps explain the actions required to configure routes between CommServe, MediaAgent and the new client through the Calypso proxy.

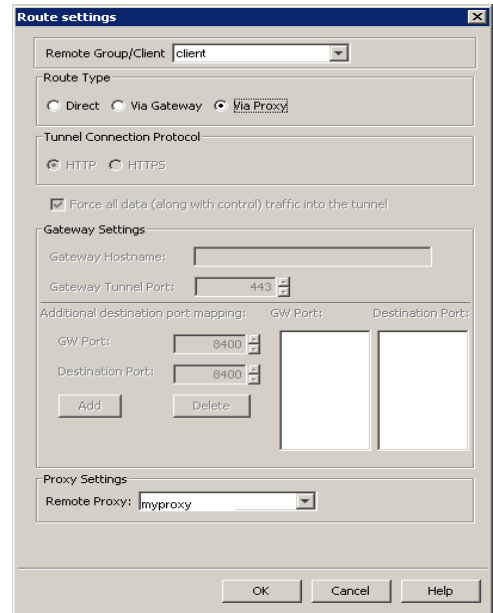
1. To configure the CommServe, right-click the CommServe computer from the CommCell Console and click **Properties**.



2.
 - Click the **Firewall Configuration** tab.
 - Click the **Outgoing Routes** tab.
 - Click **Add** to specify the outgoing connection route from the CommServe to the Client through the Calypso proxy.



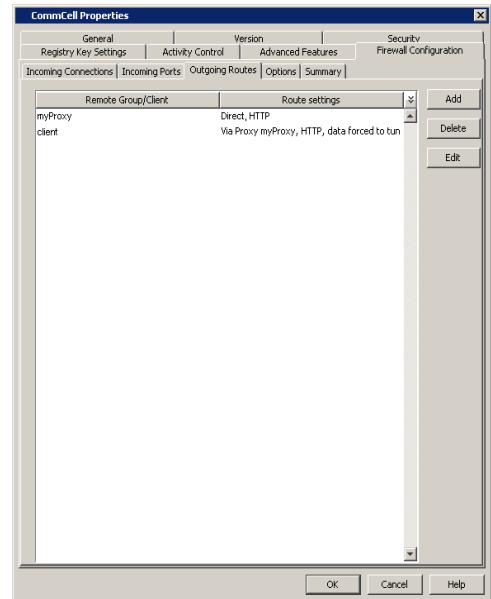
3.
 - Select the client computer in **Remote Group/Client**.
 - Select **Via Proxy**.
 - Select the Calypso proxy in **Remote Proxy**.
 - Click **OK**.



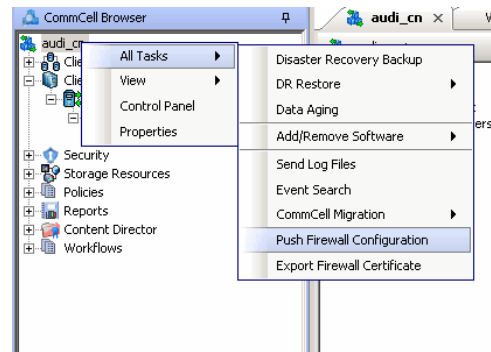
4. Click **OK**.

The **Outgoing Routes** tab should display two routes — the route from CommServe to the proxy and the route from CommServe to the client through the proxy.

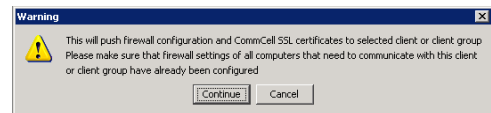
Note that when two computers are communicating with each other through a proxy, two routes need to be configured in each computer's Firewall preferences: one route to describe the connectivity of the computer with the proxy, and another route to describe the connectivity of the computer with the remote computer via proxy.



- From the CommCell Console, right-click the CommServe computer and click **All Tasks | Push Firewall Configuration**.

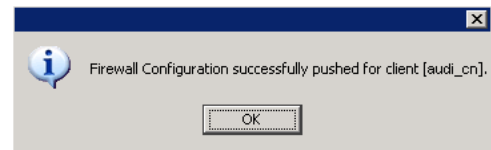


- Click **Continue**.



- Click **OK**.
The CommServe is configured to receive communication from the client through the Calypso proxy.

Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.



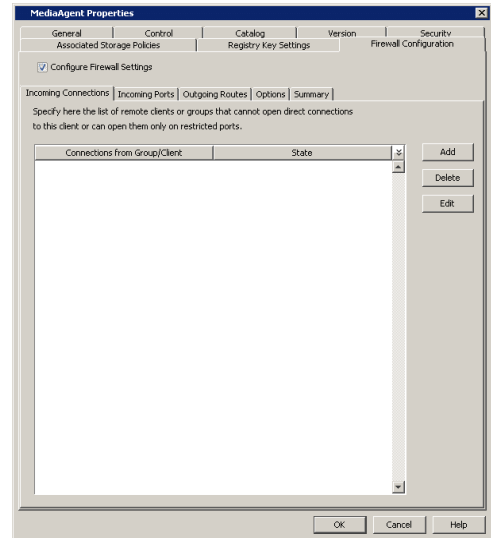
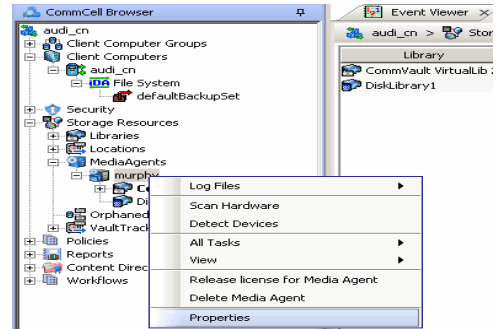
- From the CommCell Console, right-click the client computer and click **All Tasks | Check Readiness**. The results are displayed in **Client Connectivity** dialog box.

If the client computer is not ready, verify your settings with the above recommendations and revise the settings if required.

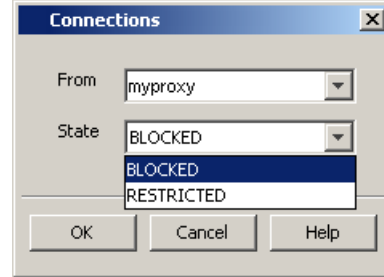


- To configure the MediaAgent, right-click the MediaAgent computer from the CommCell Console and click **Properties**.

10.
 - Click the **Firewall Configuration** tab.
 - From the **Incoming Connections** tab, click **Add**.

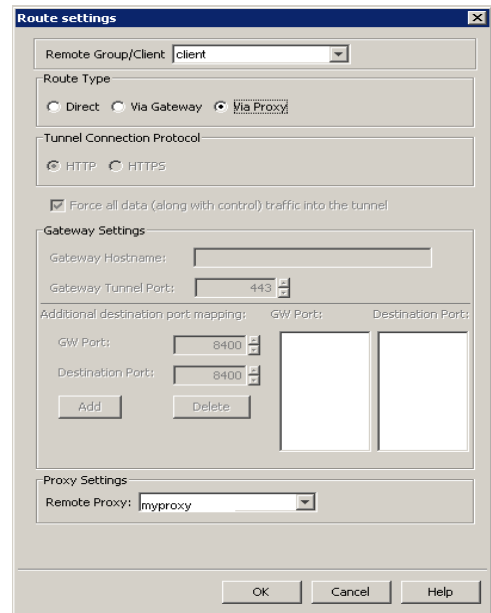
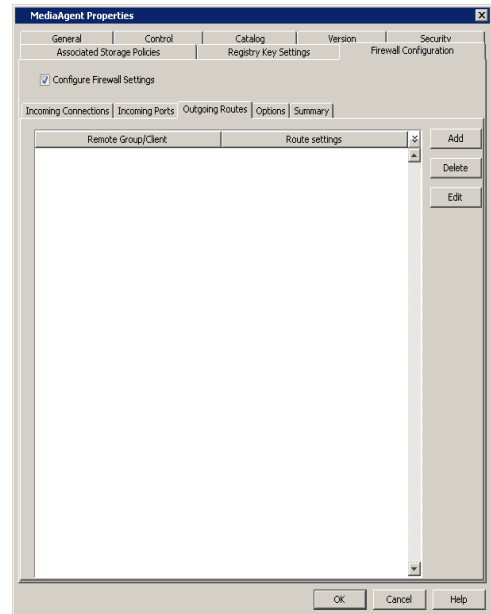


11.
 - In the **From** field, select the Calypso proxy computer.
 - In the **State** field, select **Blocked**.
 - Click **OK**.

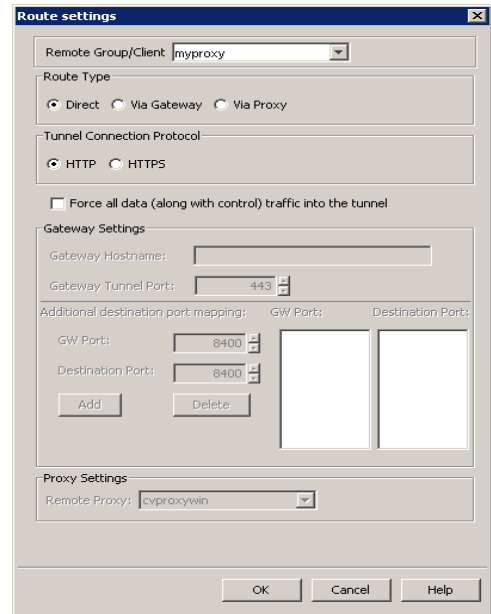


12.
 - Click the **Outgoing Routes** tab.
 - Click **Add** to specify the outgoing connection route from the MediaAgent to the Client through the Calypso proxy.

- 13.
- Select the client computer in **Remote Group/Client**.
 - Select **Via Proxy**.
 - Select the Calypso proxy in **Remote Proxy**.
 - Click **OK**.



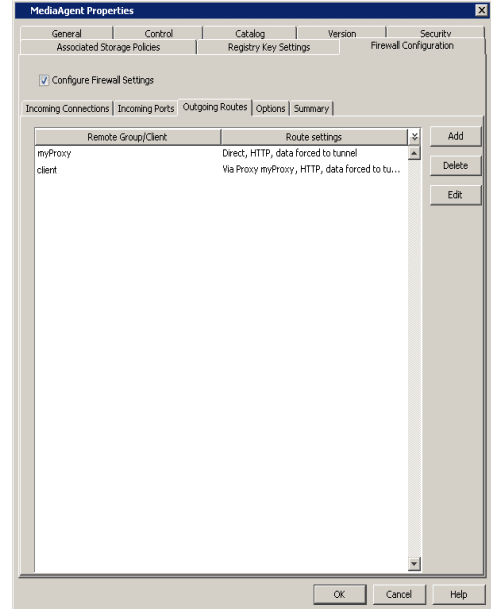
- 14.
- Click **Add** again to specify the route from MediaAgent to the Calypso proxy.
 - Select the name of the CommServe in **Remote Group/Client**.
 - Select **Force all data (along with the control) traffic into the tunnel**.
 - Click **OK**.



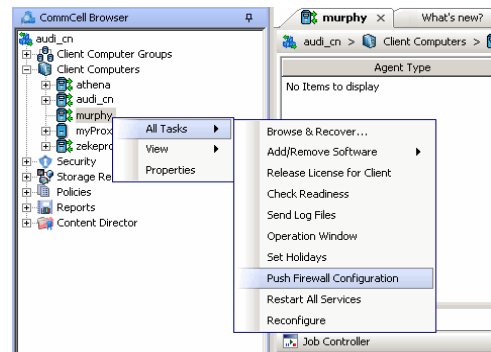
15. Click **OK**.

The **Outgoing Routes** tab must display two routes: the route from MediaAgent to the proxy and the route from MediaAgent to the client through the proxy.

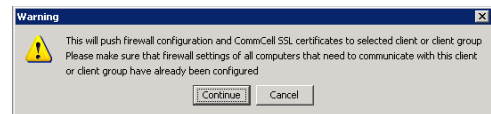
The MediaAgent is configured to receive communication from the client through the Calypso proxy.



16. From the CommCell Console, right-click the MediaAgent computer and click **All Tasks | Push Firewall Configuration**.



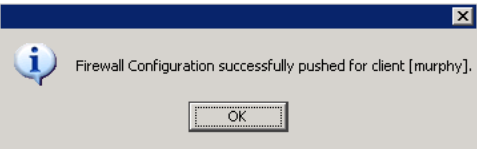
17. Click **Continue**.



18. Click **OK**.

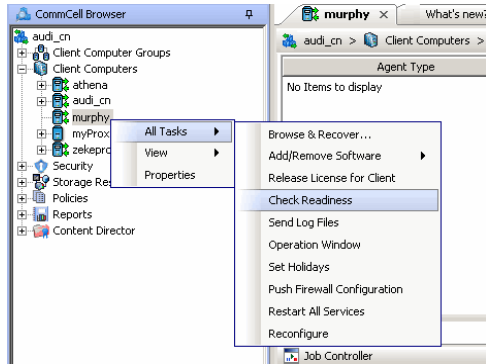
The MediaAgent is configured to receive communication from the client through the Calypso proxy.

Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.

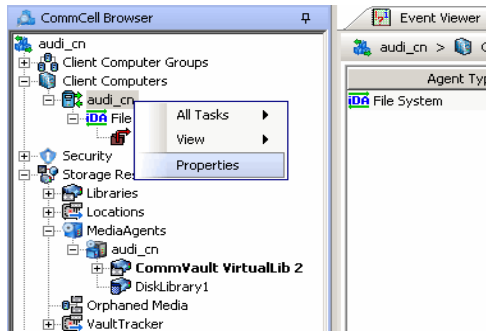


- 19. From the CommCell Console, right-click the MediaAgent computer and click **All Tasks | Check Readiness**. The results are displayed in **Client Connectivity** dialog box.

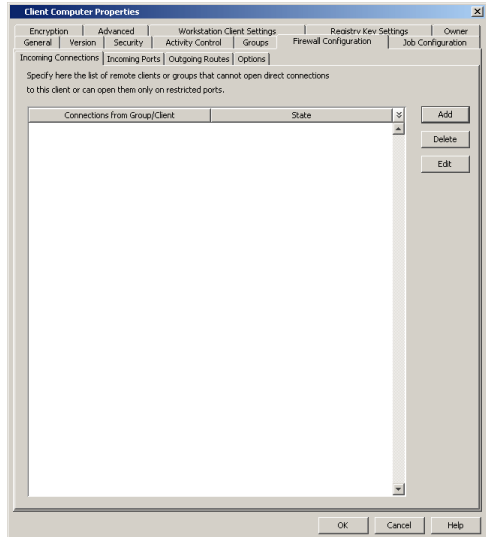
If the MediaAgent computer is not ready, verify your settings with the above recommendations and revise the settings if required.



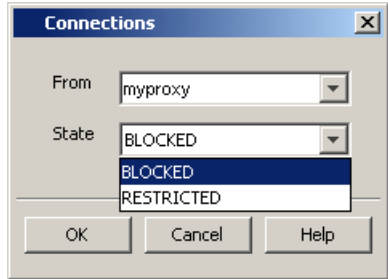
- 20. To configure the Client, right-click the client computer from the CommCell Console and click **Properties**.



- 21.
 - Click the **Firewall Configuration** tab.
 - From the **Incoming Connections** tab, click **Add**.

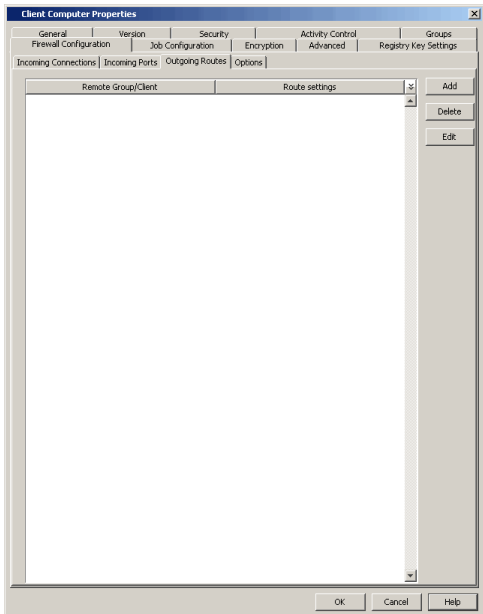


- 22.
 - In the **From** field, select the Calypso proxy computer.
 - In the **State** field, select **Blocked**. Since there are no incoming connections from the proxy to the client, the connection status is **Blocked**.
 - Click **OK**.



- 23.
 - Click the **Outgoing Routes** tab.

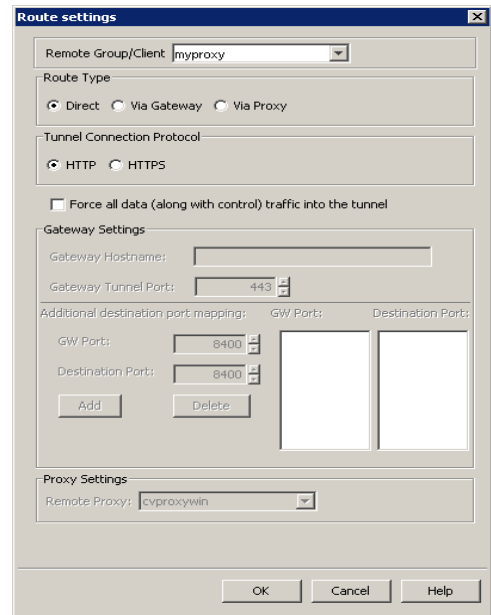
- Click **Add** to specify the route for outgoing connection from the client to the Calypso proxy.



- 24.
- Select the Calypso proxy in **Remote Group/Client**.
 - Select **Direct** for **Route Type**.

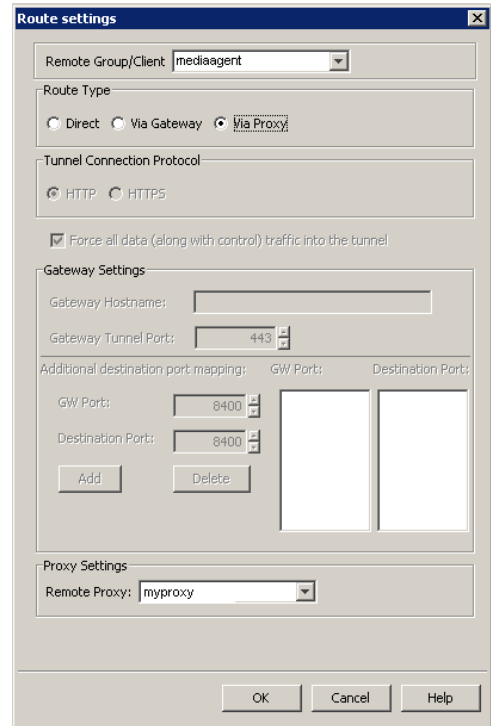
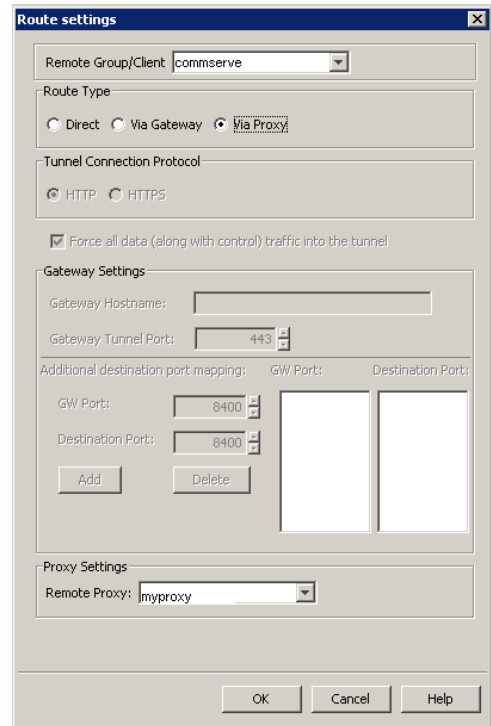
In case there is a port-forwarding gateway between the client and the Proxy, you will have to select **Via Gateway** and configure Gateway Settings.

- Select **Force all data (along with the control) traffic into the tunnel** to force the data traffic into the control tunnel. This automatically encrypts the data connection.
- Click **OK**.



- 25.
- Click **Add** again to specify the route for outgoing connection from the client to the CommServe through the Calypso proxy.
 - Select the name of the CommServe in **Remote Group/Client**.
 - Select **Via Proxy**.
 - Select the Calypso proxy in **Remote Proxy**.
 - Click **OK**.

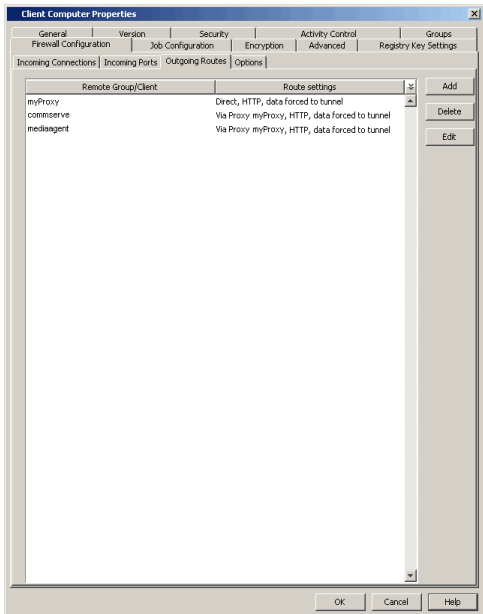
- 26.
- Click **Add** again to specify the route for outgoing connection from the client to the MediaAgent through the Calypso proxy.
 - Select the name of the MediaAgent in **Remote Group/Client**.
 - Select **Via Proxy**.
 - Select the Calypso proxy in **Remote Proxy**.
 - Click **OK**.



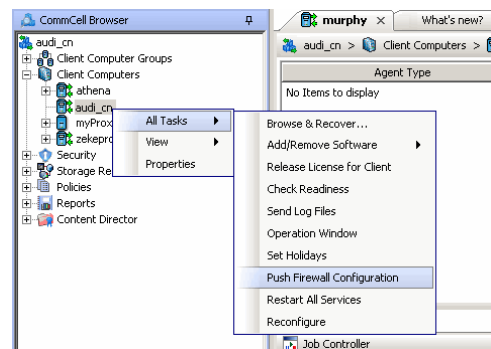
27. Click **OK**.

The **Outgoing Routes** tab should display three routes: the routes from the client to the proxy, client to to the MediaAgent, and client to the CommServe.

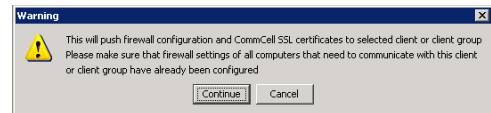
Please note that the image to the right assumes the route between the client and the proxy was configured using a **Direct** route. If you used a port-forwarding gateway, you will see **Via Gateway** as the route setting.



28. From the CommCell Console, right-click the client computer and click **All Tasks | Push Firewall Configuration**.



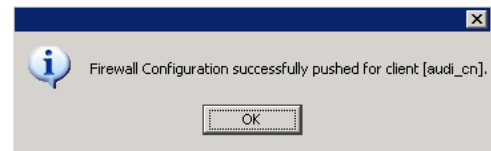
29. Click **Continue**.



30. Click **OK**.

The specified configurations are saved.

Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.



31. From the CommCell Console, right-click the client computer and click **All Tasks | Check Readiness**. The results are displayed in **Client Connectivity** dialog box.

If the client computer is not ready, verify your settings with the above recommendations and revise the settings if required.



Connectivity between the CommServe, MediaAgent, and the client through the Calypso proxy is established.

OPERATING USING PUBLIC WIFI CONNECTIONS

Consider the scenario where you are in a public location like a coffee shop, airport, hotel, or other such remote locations where internet access is using public WiFi through a HTTP proxy. If you are a roaming user who travels frequently, you might operate the software in this scenario. The following sections describe the configuration required to operate the software through HTTP proxy.

INSTALL THE CLIENT

We assume that your computer contains client components only. In most cases, the client software is already installed and ready for backup and recovery operations. You can however, install the software from behind a HTTP proxy. The following sections present the possible firewall scenarios that might protect the CommServe and the installer sequence to reach the CommServe in each scenario. Select the scenario that matches your deployment setup and follow the steps in sequence.

- Firewall Configuration - Windows
- Firewall Configuration - Unix

CONFIGURE THE CLIENT TO OPERATE ACROSS HTTP PROXY

To configure the client to operate across HTTP Proxy:

1. Locate the firewall configuration file `FWConfigLocal.txt` under `<software_installation>/Base` folder. This file contains the firewall configuration options provided during installation. Do not modify the `FWConfig.txt` file.

This file might not be available if the client software was installed within the internal network with no firewall separating the computer and the CommServe. In such case, contact your system administrator for details to create this file.

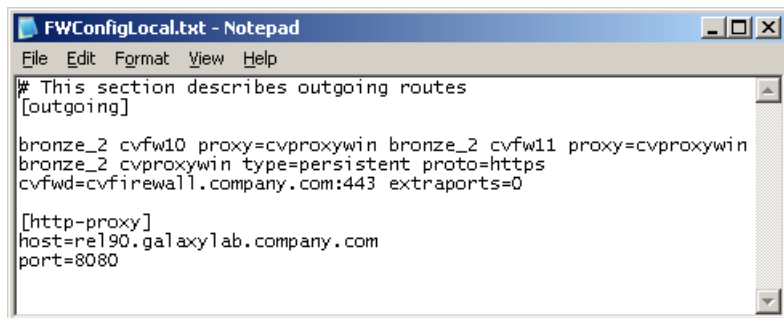
2. Locate the `[http-proxy]` section at the end of the file and remove the comment tag (`#`) from the section and its body. The section and its contents will appear as follows.

```
# [http-proxy]
# host= <host name of the proxy server>
# port= <HTTP proxy port number>
```

3. Provide the correct values for the host name and port number of the HTTP server. The software does not support HTTP proxies that require authentication.

If you are a roaming user frequently operating using public WiFi, you will have entries from your previous access. In such case, update the entries with the `host` and `port` information applicable to the current setup.

The following are sample entries for an outgoing route through HTTP Proxy.



```
FWConfigLocal.txt - Notepad
File Edit Format View Help
# This section describes outgoing routes
[outgoing]
bronze_2 cvfw10 proxy=cvproxywin bronze_2 cvfw11 proxy=cvproxywin
bronze_2 cvproxywin type=persistent proto=https
cvfwd=cvfirewall.company.com:443 extraports=0
[http-proxy]
host=re190.galaxy1ab.company.com
port=8080
```

CONFIGURING WINDOWS FIREWALL TO ALLOW COMMCELL COMMUNICATION

Windows Firewall, the built-in firewall included in Windows Operating Systems, can be configured to allow CommCell communication by adding CommCell programs and services to the Windows Firewall Exception list. Once the CommCell programs are added to the Exception list, the Windows Firewall will allow external network connections to the CommCell Console.

During installation of Windows components, the installer provides an option to add CommCell programs and services to Windows Firewall List. You can use this option to configure Windows Firewall during installation.

After installation, you can later configure Windows Firewall using `AddFWExclusions.bat` program. The `AddFWExclusions.bat` program should be run through the command prompt to prevent adding system32 executables to the firewall exception list as the default system environment variable may be triggered.

To add CommCell programs and services to Windows Firewall Exception List:

1. Open the command prompt.
2. Navigate to the `<Software_Installation_Path>/Base` folder.
3. Run the `AddFWExclusions.bat` file to execute the commands.

- All applicable CommCell communication programs and services are added to Windows Firewall Exception List. Note that this must be done on all CommCell Computers.

If the firewall configuration is reset on a computer for any reason (this can happen, for example, when the computer is moved from a workgroup to a domain), then the firewall exclusions must be added again.

[Back To Top](#)

Firewall

Setup	Advanced	Troubleshooting	Best Practices
-----------------------	--------------------------	---------------------------------	--------------------------------

Overview

Configuring Multiple Clients Simultaneously

Inherit the Firewall Configuration from the Client Group

Configuring Multiple Connection Routes

Configuring a Clustered Environment

Configuring CommCell Components to Use HTTPS

Prerequisite

Method 1: Configure a Component to Accept HTTPS Only

Method 2: Enable HTTPS Between two Components

Configuring Firewall Using Save As Script

Enforcing CommCell Specific Certificates for Authentication

Enabling CommCell Specific Certificates

Installing on a Locked Down CommCell

Setting up Application-Based Firewall

Block Unauthorized CommCell Session Connections

Block External Interface Connections

Block Local Interface Connections

Binding Services to Open Ports

Registering a CommServe to a CommNet Server

Configure the CommServe (CommCell Console)

Configure the CommNet Server (CommCell Console)

Register the CommServe (CommNet Browser)

Removing Firewall Configuration

Upgrade Considerations

CommServe Upgrade

Client/MediaAgent Upgrade

OVERVIEW

Firewall configuration provides additional features and functions that can be used to fine-tune CommCell communication and operations. The following sections explain the additional features and their usage.

CONFIGURING MULTIPLE CLIENTS SIMULTANEOUSLY

If you have multiple clients with the same firewall configuration settings, instead of defining the configuration for each client, you can create a Client Group with clients that have the same firewall configuration and define the configuration at the Client Group level.

Use the following steps to configure firewall settings for multiple clients simultaneously:

- From the CommCell Console, create a Client Computer Group with clients that have the same firewall configuration.
See [Getting Started - Client Computer Groups](#) for step-by-step procedure.
- Right-click the newly-created client group and click **Properties**.
- In the **Firewall Configuration** tab, provide the necessary details in the **Incoming Connections**, **Incoming Routes**, **Outgoing Connections**, and **Options** tabs as discussed in the procedures of the Firewall (Setup) page.
- Right-click the client group, click **All Tasks**, and click **Push Firewall Configuration**. The configuration is now applicable for all the clients. You can verify the new firewall configuration on each client computer.

INHERIT THE FIREWALL CONFIGURATION FROM THE CLIENT GROUP

Use the following steps to configure a client to inherit the firewall settings from the client computer group.

1. From the CommCell Console, right-click the client computer and click **Properties**.
2. In the **Firewall Configuration** tab, ensure the **Configure Firewall Settings** option is not selected.
3. Click **OK**.

Future firewall changes will be applicable at the client group level.

When **Configure Firewall Settings** is selected, the firewall configuration of both the client computer and client group are merged in the client computer.

CONFIGURING MULTIPLE CONNECTION ROUTES

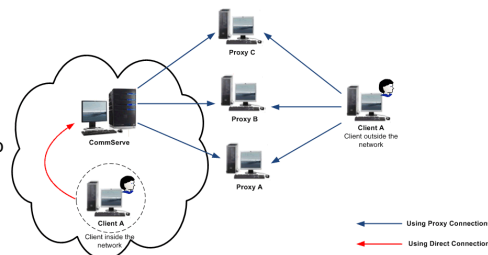
You can define the following routes for a client group or client computer:

- Multiple proxy connections
- A direct connection (where the client connects to the CommServe)

It is recommended to configure proxy and direct routes for a client computer because:

- whenever the client is outside the network, the CommServe will use the proxy connection to access the client.
- if the client is moved inside the network, the client will use the direct connection to access the CommServe.

The diagram on the right depicts this setup.



Follow the steps below to configure multiple connection routes for a client computer:

1. Create a proxy connection as described in Operating through a DMZ using Calypso Proxy. This step can be repeated as needed to add additional proxy connections for the client.
2. Create a direct connection as described in Client Connects to the CommServe.

CONFIGURING A CLUSTERED ENVIRONMENT

When configuring firewall on a clustered environment, virtual nodes of a clustered client computer must be configured with the connection route to reach each other across the firewall. Once configured, the virtual nodes communicate across the firewall for all data management operations.

Use the following steps to configure firewall settings:

1. From the CommCell Console, right-click the virtual node to configure and click **Properties**.
2. In the **Firewall Configuration** tab, provide the necessary details in the **Incoming Connections**, **Incoming Routes**, **Outgoing Connections**, and **Options** tabs as discussed in the procedures of the Firewall (Setup) page.
3. Right-click the physical node, click **All Tasks**, and click **Push Firewall Configuration**. Repeat this step for all physical nodes of the cluster.

The configuration is now applicable for the virtual node.

CONFIGURING COMMCELL COMPONENTS TO USE HTTPS

Communication between CommCell components can be automatically encrypted and authenticated through Secured Socket Layer (SSL), similar to what happens when a web browser opens secure connections with https:// prefix.

CERTIFICATE FOR AUTHENTICATION

The authentication and encryption is done with the help of certificates. The software supports two types of SSL certificates: Built-In certificates and CommCell certificates. Built-In certificates are present on installation media and are used primarily during installation. CommCell certificates are generated during CommServe install or upgrade and are unique to the CommCell.

Typically the software uses the built-in certificate during installation, and as soon as the newly installed client establishes its first connection with the CommServe, it retrieves CommCell certificate and uses it for all future SSL exchange. You can however, refuse connections backed by the built-in certificates and enforce CommCell certificates only by using the CommCell Lockdown feature. See Enforcing CommCell Specific Certificates for Authentication for more information.

PREREQUISITE

This can be configured using firewall configuration settings in the Client Computer Properties.

Your setup would be one of the following:

- CommCell components are separated by firewall.

Configure the firewall settings. Refer to Firewall (Setup) to review supported firewall types. Identify the type of your firewall and configure the components accordingly.

- CommCell components are not separated by firewall.

In this case, you will have to configure firewall settings just to initiate a tunnel connection to enforce HTTPS transport. Configure the components in one of the following ways:

- Operating Using Direct Connections - Client Connects to the CommServe
- Operating Using Direct Connections - CommServe Connects to the Client

To enable HTTPS communication:

METHOD 1: CONFIGURE A COMPONENT TO ACCEPT HTTPS ONLY

Once a component is configured to receive HTTPS connections only, it will force all incoming tunnel connections to HTTPS by authenticating and setting up encryption in accordance with the HTTPS standard.

1. From the CommCell Console, right-click the client computer and click **Properties**.
2. In the **Client Computer Properties** window, click the **Firewall Configuration** tab.
3. Click the **Options** tab, and for **Incoming Tunnel Protocol** select **Allow only HTTPS**.
4. From the CommCell Console, right-click the client computer, and click **All Tasks | Push Firewall Configuration**. The configuration is saved.
5. Repeat the above configuration for all components.

METHOD 2: ENABLE HTTPS BETWEEN TWO COMPONENTS

This is a more granular approach that involves defining the outgoing route from one component towards the other.

1. From the CommCell Console, right-click the client computer and click **Properties**.
2. In the **Client Computer Properties** window, click the **Firewall Configuration** tab.
3. Click the **Outgoing Routes** tab, select the remote client in **Remote Group/Client**, and then click **Edit**.
4. In the **Route Settings** window, for **Tunnel Connection Protocol** select **HTTPS**.
5. From the CommCell Console, right-click the client computer and click **All Tasks | Push Firewall Configuration**. The configuration is saved.
6. Repeat the above configuration for all outgoing routes, on all components.

CONFIGURING FIREWALL USING SAVE AS SCRIPT

When Calypso proxy is in use, you can use Save As Script (.xml) file generated during the push install to configure firewall settings while performing remote installation on a new client. For more information, see Install Software on Client Using Save As Script.

ENFORCING COMMCELL SPECIFIC CERTIFICATES FOR AUTHENTICATION

CommCell environments can be locked down to prevent existing CommCell components from accepting HTTPS tunnel connections backed by a built-in certificate. In this secure Lockdown mode, CommCell components accept/initiate HTTPS connections with CommCell certificates only as opposed to accepting/initiating HTTPS connections with mutually negotiated built-in or CommCell certificates (favoring the later.) The mandatory use of CommCell certificates provides a high level of security that cannot be hacked or compromised by connections from outside the CommCell.

CommCell certificates are created during CommServe install/upgrade and are stored in the CommServe database. These certificates can be delivered to the clients either automatically or manually.

- When new clients are installed on a CommCell that is not operating in the Lockdown mode, the certificates are automatically delivered to the clients upon installation.
- When new clients are installed on a locked down CommCell, the certificates must be manually delivered to the client by exporting the certificates and physically providing it to the new clients.

ENABLING COMMCELL SPECIFIC CERTIFICATES

To enable CommCell specific certificates for authentication:

1. From the CommCell Console, right-click the CommServe computer and click **Properties**.
2. In the **CommCell Properties** window, click the **Firewall Configuration** tab.
3. Click the **Options** tab and select **Lock down CommCell**.
4. Click **OK** to save the changes.
5. Repeat the process for other CommCell components such as MediaAgents and other clients.

INSTALLING ON A LOCKED DOWN COMMCELL

When you install a client on a locked down CommCell, you need CommCell certificates to authenticate the installation. The certificates can be exported from the CommServe and delivered to the client.

EXPORT THE COMMCELL CERTIFICATE

To export the CommCell certificate:

1. From the CommCell Console, right-click the CommServe computer and click **All Tasks | Export Firewall Certificate**.
2. In the **Export Location** window, specify the location to store the certificate.
3. Click **OK** to export the certificate.

You can use a portable drive to store the certificates and physically deliver the drive to the new client, or transfer the data electronically.

PROVIDE THE CERTIFICATE DURING INSTALLATION

When you install to a locked down CommServe, during installation in the **Firewall Configuration** sequence, the installer asks for the CommCell Certificate. In the **CommCell Certificate** screen, provide the location of the certificates folder. The installer uses this certificate to authenticate the connection to the CommServe during installation. Once the installation is complete, the certificate folder is available at `<software_installation_path/base>` folder for further authentication and access.

SETTING UP APPLICATION-BASED FIREWALL

You can create an application-based firewall to block any rogue sessions from other CommCell Components. You can also block any undesired connections from other local and remote computers.

BLOCK UNAUTHORIZED COMMCELL SESSION CONNECTIONS

When a remote client is force deleted from the CommServe, the Services for the client would remain active. Such clients would still be able to initiate sessions connections to other CommCell components. Communications from such unauthorized clients would affect the performance of the software, especially if they grow more in number. CommCell Clients can be configured to blacklist and block any such connections using Session Blacklisting.

The session blacklisting works as follows. CommCell validates every incoming connection, and if an unauthorized connection is identified, then the IP address of the client initiating the session is added to a session blacklist. Any subsequent connection from the blacklisted client is immediately denied without verification. This list is dynamically created on each client. Optionally you can also record the list of such blacklisted clients in a log file for later reference; this list can be used to review the list of client that are denied connection using this feature. The log file can be located at `<Software_Installation_Path>/Log Files/blacklist.log`.

To block unauthorized CommCell session connections:

1. To enable blacklisting, create the `nEnableSessionBlacklist` registry key and set the value to '1'. When this registry key is set to '1', unauthorized CommCell session are identified and blocked.
To disable session blacklisting, set the registry key value to '0'.
2. To maintain a log file containing the list of blacklisted clients, create the `nEnableSessionBlacklistLogging` registry key and set the value to '1'.
To disable logging, set the registry key value to '0'.

BLOCK EXTERNAL INTERFACE CONNECTIONS

You can protect your computer from undesired remote connections. For each client, create the file `InterfaceBlacklist.txt` under `<Software_Installation_Path>/Base` folder and specify the IP addresses of external interface connections that must be blacklisted. When a new connection is initiated, the software consults the Interface Blacklist and drops the connection if it is initiated from a blacklisted external address.

This file can be modified at any time; you must recycle the services for the changes to take effect. The feature is not enabled if this file is not present, or empty.

To block external interface connections:

1. Stop all services on the computer.
2. In the `<Software_Installation_Path>/Base` folder, create a text file `InterfaceBlacklist.txt`.
3. Add the IP addresses of the external computers from which you wish to block connections, one IP address per line. Note that wild characters are not supported. For example, an entry like `172.19.*.*` cannot be resolved.
To allow connections from a computer, remove the corresponding IP address from `InterfaceBlacklist.txt`.
4. Connections from IP addresses listed in the `InterfaceBlacklist.txt` file are blocked.

BLOCK LOCAL INTERFACE CONNECTIONS

You can also protect your computer from undesired connections to local interfaces. For each client, create the file `LocalInterfaceBlacklist.txt` under `<Software_Installation_Path>/Base` folder and specify the list IP addresses or hostnames of local interfaces to which connections must be blocked. When there is a new incoming connection, the local interface to which the connection arrived is checked against this list and if found, the connection is dropped immediately without any further processing.

This file can be modified at any time; you must recycle the services for the changes to take effect. The feature is not enabled if this file is not present, or empty.

To block a local interface connection:

1. Stop all services on the computer.
2. In the `<Software_Installation_Path>/Base` folder, create a text file `LocalInterfaceBlacklist.txt`.
3. Add the IP addresses (or host names) to which connections must be blocked, one IP address (or hostname) per line. Note that wild characters are not supported. For example, an entry like `172.19.*.*` cannot be resolved.

To allow connections from a computer, remove the corresponding IP address from `LocalInterfaceBlacklist.txt`.

4. Connections from IP addresses listed in the `LocalInterfaceBlacklist.txt` file are blocked.

BINDING SERVICES TO OPEN PORTS

When TCP/IP filtering is enabled on Windows computers, even same-machine connections can be restricted unless they are made on specifically open ports. In situations like this, you can force Calypso to bind all of its services to ports from the list of incoming ports configurable for the client.

To bind all services of a client to open ports:

1. From the CommCell Console, right-click the client/MediaAgent/CommServe and click **Properties**.
2. In the **Client Computer Properties** window, select the **Firewall Configuration** tab.
3. In the **Options** tab, select **Bind all Services to open ports only**.
4. Click **OK** to save the changes.

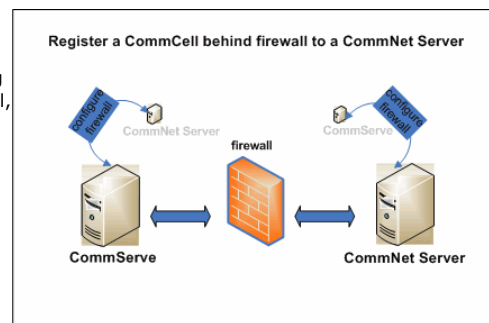
REGISTERING A COMMSERVE TO A COMMNET SERVER

You can register a CommServe that is operating behind a firewall to a CommNet Server.

When two CommCell components operate across firewall, the firewall specifications are provided on the client properties of the components from the CommCell Console. In registering a CommServe to CommNet Server, since the CommServe is not present in the same CommCell, you will have to create a placeholder client to represent the components for firewall configuration.

The diagram on the right depicts this setup and solution.

The following sections describe the required configuration.



To register a CommServe Operating Behind Firewall to the CommNet Server:

CONFIGURE THE COMMSERVE (COMMCELL CONSOLE)

On the CommCell containing the CommServe, create a placeholder client for the CommNet Server, provide firewall configuration for CommNet Server and CommServe, and save the configuration for CommServe.

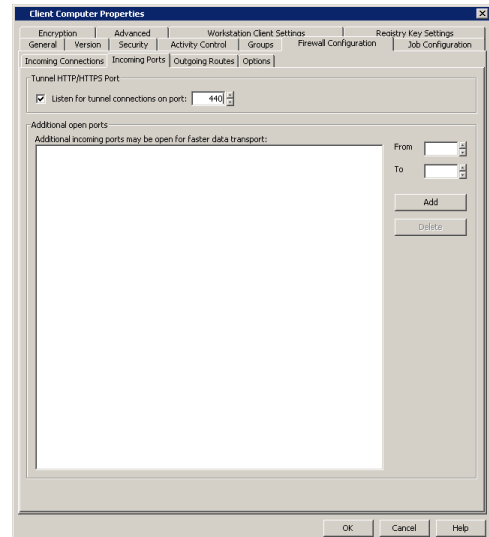
1. From the CommCell Console, right-click on the client computer node, and click **New Client**.
2. In the **Add New Client** window, select **Windows** and click OK.
3.
 - In the **Windows Client Creation** window, enter the **Client Name** and the **Host Name** of the CommNet Server computer on the other side of the firewall. Ensure to provide the correct client name as the firewall program uses the client name to establish connection to the CommCell.
 - Click **OK**.

A placeholder client for CommNet Server is created in the CommServe.

4. Right-click the newly created CommNet Server, and then click **Properties**.

5.
 - In the **Firewall Configuration** tab, provide details in the **Incoming Connections, Incoming Ports, Outgoing Routes, and Options** tabs. Verify the details in the **Summary** tab.
 - Click **OK**.

The options you provide in the firewall configuration tabs are based on the firewall setup that separates the two computers.



6. Right-click the CommServe computer, and then click **Properties**.
7.
 - In the **Firewall Configuration** tab, provide details in the **Incoming Connections, Incoming Ports, Outgoing Routes, and Options** tabs. Verify the details in the **Summary** tab.
 - Click **OK**.
8. Right-click the CommServe computer, click **All Tasks**, and then click **Push Firewall Configuration**.

The firewall configuration between the two computers is saved.

CONFIGURE THE COMMNET SERVER (COMMCELL CONSOLE)

On the CommCell containing the CommNet Server, create a placeholder client for CommServe, provide firewall configuration for CommServe and CommNet Server, and save the configuration for CommNet Server.

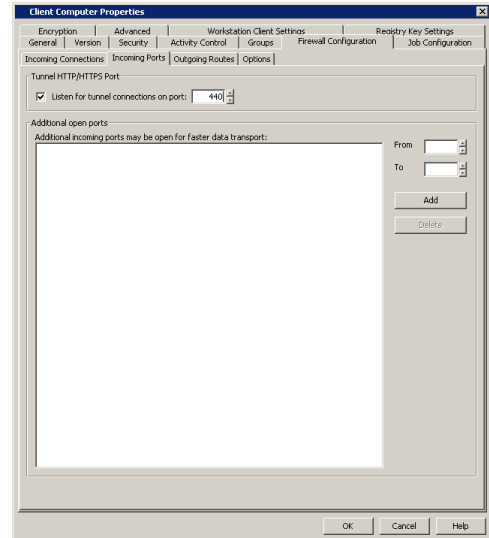
9. From the CommCell Console, right-click the client computer node, and click **New Client**.
10. In the **Add New Client** window, select **Windows** and click **OK**.
11.
 - In the **Windows Client Creation** window, enter the **Client Name** and the **Host Name** of the CommServe computer on the other side of the firewall.

Ensure to provide the correct client name as the firewall program uses the client name to establish connection to the CommCell.

 - Click **OK**.

A placeholder client for CommNet Server is created in the CommServe.
12. Right-click on the newly created CommServe, and then click **Properties**.
13.
 - In the **Firewall Configuration** tab, provide details in the **Incoming Connections, Incoming Ports, Outgoing Routes, and Options** tabs. Verify the details in the **Summary** tab.
 - Click **OK**.

The options you provide in the firewall configuration tabs are based on the firewall setup that separates the two computers.



14. Right-click the CommNet Server computer, and then click **Properties**.
15.
 - In the **Firewall Configuration** tab, provide details in the **Incoming Connections**, **Incoming Ports**, **Outgoing Routes**, and **Options** tabs. Verify the details in the **Summary** tab.
 - Click **OK**.
16. Right-click the CommNet Server computer, click **All Tasks**, and then click **Push Firewall Configuration**.
The firewall configuration between the two computers is saved.

REGISTER THE COMMSERVE (COMMNET BROWSER)

From the CommNet Browser, register the CommServe to the CommNet Server.

17. If the CommNet Browser is installed as a stand-alone application on a computer that operates across firewall(s) from the CommNet Server and has no other CommServe component installed, specify port number 8403 to allow connection through the firewall.
18. From the CommNet Browser, click on the **Setup** menu, and click **Cell Registration**.
19. In the **Cell Registration** window, click **Add CommCell**.
20. In the **Register CommCell** window, specify the **CommCell Client name** of the CommServe computer. This is also the name of placeholder client for CommServe you created earlier.
21. Click **OK** to complete the registration.
The software connects to the newly registered CommCell through the firewall configuration defined earlier in the procedure.

REMOVING FIREWALL CONFIGURATION

Use the following steps to remove the firewall settings for a client computer:

1. From the CommCell Browser, right-click the client and click **Properties**.
2. Click the **Firewall Configuration** tab.
3. Verify if the client computer has any incoming connection from other clients or client groups. If found, write down the name of the client.
4. Clear the **Configure Firewall Settings** option and click **OK**.
5. Right-click the client and then click **All Tasks** | **Push Firewall Configuration**.
6. If incoming connections were found, navigate to the client(s) found in **Step 3** and do the following for each of them:
 - Right-click the client/client group and click **Properties**.
 - Click the **Firewall Configuration** tab.
 - Select the client whose firewall settings were removed and click **Delete**. Click **Yes** from the **Delete** dialog box.
 - Click **OK**.

- o Right-click the client/client group and then click **All Tasks | Push Firewall Configuration**.

UPGRADE CONSIDERATIONS

On upgraded CommCells with firewall configuration settings from previous releases, you have the option to continue with the existing settings. Firewall configuration files of clients with software version 7.0 and 8.0 are supported on a CommServe with software version 9.0.

However, we strongly recommend that you revise your settings with configuration options available in this release to take advantage of the additional firewall configuration capabilities. Configuration options available in this release support a wide range of standard and customized firewall scenarios.

COMMSERVE UPGRADE

When upgrading at the CommServe level, the old firewall files of the CommServe computer will be automatically upgraded to the new configuration available in this release if the following two conditions are met.

1. The IP address or hostname defined in the `FwHosts.txt` and `FwPeers.txt` firewall files literally matches the host name of the client computer as recorded in the CommServe database.
2. The IP address or hostname defined in the `FwHosts.txt` and `FwPeers.txt` firewall files resolves to the same IP address as the one in the existing Data Interface Pairs (DIP).

If the old firewall files fail to get upgraded, mainly due to hostname wildcards present in the `FwPeers.txt` firewall file, follow the steps below to perform a manual upgrade of your firewall files.

1. Upgrade the CommServe computer. See Upgrade the CommServe for more information.
2. Configure the firewall settings by following the procedures explained in the Firewall (Setup) page.
3. Restart the services on the CommServe.
4. Run the `FirewallConfigDeprecated.exe` tool located in the `<software installation path>/Base/` folder on the CommServe and remove the old firewall configuration files.

The firewall configuration files for the CommServe computer are upgraded.

CLIENT/MEDIAAGENT UPGRADE

The old firewall files of a client/MediaAgent computer will be automatically upgraded to the new configuration available in this release if the following two conditions are met.

1. The IP address or hostname defined in the `FwHosts.txt` and `FwPeers.txt` firewall files literally matches the host name of the client computer as recorded in the CommServe database.
2. The IP address or hostname defined in the `FwHosts.txt` and `FwPeers.txt` firewall files resolves to the same IP address as the one in the existing Data Interface Pairs (DIP).

If the old firewall files fail to get upgraded, mainly due to hostname wildcards present in the `FwPeers.txt` firewall file, follow the steps below to perform a manual upgrade of your firewall files.

1. Upgrade the client/MediaAgent computer. See Upgrade software on clients for more information.
2. Configure firewall settings for the CommServe, MediaAgent and client computers by following the procedures explained in the Firewall (Setup) page. If you need to configure multiple client computers, see Configuring Multiple Clients Simultaneously.
3. Restart the services on the client/MediaAgent.
4. Run the `FirewallConfigDeprecated.exe` tool located in the `<software installation path>/Base/` folder on the CommServe and MediaAgent computers, and remove the client computer's name from the old firewall configuration files.

For Unix machines, run the `config_fw_deprecated` command in the `opt/<software installation path>/Base/` directory.

You should not delete the `FwHosts.txt`, `FwPorts.txt` and `FwPeers.txt` firewall files on the CommServe and MediaAgent computers until all client computers have been upgraded with the new firewall configuration.

The firewall configuration files for the client/MediaAgent computer are upgraded.

[Back To Top](#)

Robust Network Layer

[Topics](#) | [How To](#) | [Support](#) | [Related Topics](#)

Overview

[How the Robust Network Layer Feature Works](#)

[Customize Robust Network Layer Feature](#)

[Important Considerations](#)

OVERVIEW

The CommServe coordinates all the activities within the CommCell. This includes starting and managing data protection jobs, receiving updates from them and also recording their final as well as intermediate job status conditions. Each data protection job consists of several phases, each of which is initiated and managed by the CommServe computer. The CommServe also checks for the liveliness and continued operation of each of the phases.

Such a centralized architecture allows for ease of administration, reporting and monitoring. Given the scalability and flexibility of the software's architecture, a CommServe located at a one location can manage a CommCell that spans a wide variety of networks and geographic locations. The actual data in the CommCell flows from the Client computer to the MediaAgent. Often, these two computers are located at the same site connected by a Local Area Network (LAN); however, their connectivity to the CommServe is via a Wide Area Network (WAN) or Virtual Private Network (VPN), which are more prone to glitches and temporary outages.

When a data protection activity is in progress, there is a significant time and resource investment in transferring and saving the data to the target media. If this data protection operation were disrupted due to a WAN glitch, the investment would be at risk. Some of the database backups (e.g., Exchange, Oracle) need to be restarted from the beginning, which can be costly in addition to time consuming.

The purpose of the Robust Network Layer feature is to protect this investment of time and resources when these network glitches occur. It allows the connections between a CommServe, MediaAgent, and client to be retried at set intervals, if there is any loss of connectivity.

HOW THE ROBUST NETWORK LAYER FEATURE WORKS

During the data transfer phase of a backup operation, which runs on a MediaAgent and client, the Job Manager will periodically need to communicate directives to the CommServe (via a WAN or VPN). If during this time, a loss of network connectivity is detected, the Robust Network Layer feature enables the Job Manager to keep the job in a **Running (Cannot be verified)** job state, visible in the Job Controller, for up to 20 minutes while continuously checking for network connectivity at set intervals, e.g., every 30 seconds. Though the default amount of time the system will hold a job in a running state when there is loss of connectivity is up to 20 minutes, users can edit the Robust Network Layer default configuration, refer to [Customize Robust Network Layer Feature](#).

CUSTOMIZE ROBUST NETWORK LAYER FEATURE

During an installation of a CommServe, a Client or an Agent, the Robust Network Layer feature is automatically enabled by default. To disable the feature, refer to [Enable/Disable the Robust Network Layer](#). To change the intervals at which the network connectivity will be checked as well as the number of times for each retry, refer to [Change the Robust Network Layer Configuration](#).

IMPORTANT CONSIDERATIONS

Installation

During an installation of a CommServe, a Client or an Agent, the Robust Network Layer feature is enabled by default.

Upgrade

Windows Platforms

During an upgrade of a CommServe, Client or Agent, the Robust Network Layer settings remain unchanged from the previous version. To enable the Robust Network Layer feature on an upgraded Windows computer, see [Enable/Disable the Robust Network Layer](#).

UNIX Platforms

During an upgrade of a CommServe, Client or Agent, the Robust Network Layer registry key settings remain unchanged from the previous version. To enable the Robust Network Layer feature on an upgraded UNIX computer, see [Enable/Disable the Robust Network Layer](#).

[Back to Top](#)

Robust Network Layer - How To

[Topics](#) | [How To](#) | [Support](#) | [Related Topics](#)

[Enable/Disable Robust Network Layer](#)

[Change Robust Network Layer Configuration](#)

ENABLE/DISABLE ROBUST NETWORK LAYER

Required Capability: Capabilities and Permitted Actions

▶ To enable or disable the Robust Network Layer feature:

1. From the CommCell Console, right click on a client, and select **Properties** from the pop-up menu. Select the Client Computer Properties (Advanced) tab.
Alternatively, right click on a MediaAgent and select **Properties** from the pop-up menu. Select the MediaAgent Properties (Control) tab.
 2. Select the **Enable retry on network errors** option to enable the feature. Deselect it to disable the feature.
 3. Click **OK**.
-

CHANGE ROBUST NETWORK LAYER CONFIGURATION

Required Capability: Capabilities and Permitted Actions

▶ To change the Robust Network Layer configuration:

1. From the CommCell Console, right click on a client, and select **Properties** from the pop-up menu. Select the Client Computer Properties (Advanced) tab.
Alternatively, right click on a MediaAgent and select **Properties** from the pop-up menu. Select the MediaAgent Properties (Control) tab.
 2. Select the **Enable retry on network errors** option to enable the feature. Deselect it to disable the feature. If enabled, you may configure the following:
 - **Retry Frequency (seconds):** The interval (in seconds) at which the Job Manager will continuously check for network connectivity. Default is set at 30 seconds.
 - **Retry Count:** The number of times the Job Manager will check for network connectivity. Default is set at 40.
 3. Click **OK**.
-

[Back To Top](#)

Client

Topics | How To | Related Topics

Overview

- DB2 DPF Pseudo-Client
- RAC Pseudo-Client
- NAS NDMP Clients
- CommNet Client
- SRM Oracle Agent
- SRM NAS Agent
- SRM NetWare Proxy Agent
- Clustered Environments
- Decoupled Installs

Configurable Properties

- Activity Control
- Configuring the CDR Log File Location
- Configuring the Proxy for Exchange
- Configuring the Search Server URLs
- Data Collection
- Data Encryption
- Job Configuration
- Name Management
- User Security
- Associate or Disassociate Clients
- Version
- Data Interface pairs
- Firewall Configuration
- Configuring Deduplication Options
- Content Indexing

Using UNC Paths for Job Results Directory

- User Impersonation for Accessing the Job Results Directory

Client Connectivity

- CommNet Client Connectivity

Client Configuration Considerations

Operation Window

Audit Trail

OVERVIEW

A client is a logical grouping of the agents installed on a computer. A client level is created in the CommCell Browser the first time an agent is installed on a computer.

You can perform client operations as long as the client is available and has agents installed on that computer. Operations performed on clients are applicable to all the agents that are installed on that client.

DB2 DPF PSEUDO-CLIENT

For the DB2 DPF *i*DataAgent, the DB2 DPF pseudo-client and its corresponding instance serve as a logical grouping of DB2 DPF database partitions that are housed on various clients. See Overview - DB2 DPF *i*DataAgent for more information. The pseudo-client is not automatically created in the CommCell Browser by the software; you must create and configure it using the Create a DB2 DPF Client procedure.

RAC PSEUDO-CLIENT

For the Oracle RAC *iDataAgent*, the RAC pseudo-client serves as a logical grouping of one or more Oracle *iDataAgent* instances within a RAC pseudo-client instance. See Overview - Oracle RAC *iDataAgent* for more information. The pseudo-client is not automatically created in the CommCell Browser by the software; you must create and configure it using the Create a RAC Client procedure.

NAS NDMP CLIENTS

The software for the NAS NDMP *iDataAgents* is installed automatically as part of the MediaAgent installation. Additional software components must also be installed and configured as part of NAS NDMP *iDataAgent* Deployment; however, the client is not automatically created in the CommCell Browser. To add the client to the CommCell, refer to the following procedure:

- Add a Client for NAS NDMP *iDataAgents*

COMMNET CLIENT

A CommNet client is created on the CommCell if the CommServe is associated with a CommNet Server; during the installation of the CommNet Server software, you must specify the CommCell with which the CommNet Server will be associated. This does not register the CommCell with the CommNet Server for reporting, nor does it merge the user interfaces; however, this enables the CommNet Server to act as a client computer in the CommCell, which allows for the CommNet Server computer to support the automatic updates and license administration from the CommCell License Administration utility.

SRM ORACLE AGENT

For the SRM Oracle Agent, the agent software is installed on a proxy client. Once the installation is complete, the agent and the Oracle database information must be configured from the client level in the CommCell Console. For step-by-step instructions, see Add Oracle Database.

SRM NAS AGENT

For the SRM NAS Agent, the agent software is installed on a proxy client. Once the installation is complete, the agent and the NAS file server must be configured from the client level in the CommCell Console. For step-by-step instructions, see Add NAS Filer.

SRM NETWARE PROXY AGENT

For the SRM NetWare proxy Agent, the agent software is installed on a proxy client. Once the installation is complete, the agent and the NetWare server information must be configured from the client level in the CommCell Console. For step-by-step instructions, see Add NetWare Server.

CLUSTERED ENVIRONMENTS

Information on whether the client is a physical or virtual client is displayed in the Client Properties.

DECOUPLED INSTALLS

Agent and/or MediaAgent software can be installed on a computer that is not part of a CommCell. For more information, see Decoupled Install.

A client or MediaAgent can be pre-configured on the CommServe, and it can be subsequently connected to a computer with client and/or MediaAgent software already installed. A Product License(s) will be consumed when you perform this procedure.

The two parts involved in a Decoupled Install can be performed in any order, but must both be performed before the client and/or MediaAgent are functional in the CommCell.

CONFIGURABLE PROPERTIES

Once installed, the client computer is configured and is therefore able to manage the data or volumes. You can change the following aspects of the configuration:

ACTIVITY CONTROL

You can enable or disable all operations for this CommCell object and all objects below it. For more information, see Activity Control.

MediaAgents and data protection and recovery operations for clients can be enabled or disabled in bulk with the EnableDisableComputers command line utility in the Resource Pack. The tool can be applied to all MediaAgents and clients, or for a select targeted group.

CONFIGURING THE CDR LOG FILE LOCATION

ContinuousDataReplicator (CDR) performs replication by logging all activities in the source computer and replaying the log in the destination. On the source computer CDR logs all file write activities - new files and changes to existing files - both in the directories and volumes specified in the source paths of all the Replication Pair(s). These replication logs are transferred to the destination computer and replayed, ensuring that the destination remains a *nearly* real-time

replica of the source.

You can specify the location of these log files and how often the logs must be replayed. For more information, see Replication Logs.

CONFIGURING THE PROXY FOR EXCHANGE

When 32-bit Exchange agents are installed in non-standard configurations, such as off-host proxy or 32-bit on 64-bit, this property must be configured on the client hosting the Exchange Server to establish communications between the 32-bit Exchange agents and the Exchange Server in order to support Outlook Add-In and/or OWA functionality. The proper setting for this property depends on the type of installation configuration, as discussed below:

- When Exchange 2007 agents are installed in a 32-bit on 64-bit configuration, set this value to the client name of the 32-bit instance.
- When Exchange 2003/2007 agents are installed in an off-host proxy configuration, set this value to the client name of the off-host proxy computer.

This field should be configured after installing the Exchange agents and the OWA Proxy Enabler; it can be configured either before or after the installation of the Outlook Add-In (if applicable), but it must be configured before using Outlook Add-In and/or OWA in the configurations mentioned above. For step-by-step instructions, see Configure the Proxy for Exchange.

CONFIGURING THE SEARCH SERVER URLS

When the client is configured as a Web Search Client to support content index and search capabilities from the Search Console, options are provided that allow you to view or change the URLs used to access the Search Console and User Administration page.

You can also view the name and URL of the Web Search Server associated with the Web Search Client. Note that, the Web Search Server association cannot be changed without re-installing the Web Search Client. Also note that, the Web Search Server URL specified in the **Client Properties (Search Server URLs)** tab is not directly accessible by the user from any Web browsers.

When the client is an Exchange Server, an option is provided that allows you to associate a Web Server to the client for searching.

For step-by-step instructions, see Configure the Search Server URLs.

DATA COLLECTION

You can configure Data Collection for a Client Group or for a Client. For more information, see Data Collection.

DATA ENCRYPTION

You can enable or disable the encryption of data for transmission over unsecure networks and for storage on media. For more information, see Data Encryption.

JOB CONFIGURATION

You can set the following job configuration options:

- The Job Priority of a client.
- The time period and disk capacity after which job results are pruned.
- The directory path of the client where the job results files are located. See Using UNC Paths for Job Results Directory for more information.
- The amount of time the job results for a client should be retained.
- The low-space threshold of the job results directory, which is used to configure an alert. See Alerts and Monitoring for more information.
 - Change the name of the computer in the operating system.
 - Make sure that the computer is available in the network with the new name. (DNS lookup or other name resolution facilities are appropriately configured to resolve the new name of the computer.)
 - Ensure that all applications running on the computer, such as SQL server, Exchange, Server, Oracle database, etc., function with the new name.

TIP

Use **ping** (or other such network connectivity utilities) to verify whether the computer that has a new name is accessible. Also, ensure that the other computers in the network are accessible to the computer with the new name.

NAME MANAGEMENT

You can change the name of the Client/MediaAgent computer if the Host name is changed. See Name Management for more information.

Do not use spaces when specifying a new name for the Client.

USER SECURITY

You can perform the following functions:

- Identify the user groups to which this CommCell object is associated.

- Associate this object with a user group.
- Disassociate this object from a user group.

For more information, see User Administration and Security.

ASSOCIATE OR DISASSOCIATE CLIENTS

You can associate or disassociate clients to or from a client computer group.

VERSION

The **Version** tab displays the software version and post-release service packs and updates installed for the component. See Version for an overview.

DATA INTERFACE PAIRS

You can add, delete, and view data interface pairs between the client and other CommCell computers. The **Advanced** tab of the client's **Properties** dialog box contains options to configure new data interface pairs and view and delete any existing data interface pairs. For more information on data interface pairs, see Data Interface Pairs.

FIREWALL CONFIGURATION

You can define the connection details required to operate this client or client group across firewalls. Details of the connection passage for incoming and outgoing connections between this and other clients behind a firewall must be defined. For complete configuration details, see Firewalls.

CONFIGURING DEDUPLICATION OPTIONS

You can configure client-side deduplication options for the client. The **Client Side Deduplication** tab of the client's **Properties** dialog box consists of the following configuration options for client-side deduplication.

- Enable deduplication at the client side.
- Enable signature cache at the client side.
- Enable intelligent block alignment for deduplication operations.

See Configure Deduplication Options for the Client for step-by-step instructions.

For information, see Source Deduplication.

CONTENT INDEXING

You can enable/disable offline content indexing for the client from the **Content Indexing** tab in the **Client Properties** dialog. Moreover, for clients installed with Microsoft Windows File System, Microsoft Exchange agents, or Microsoft SharePoint Server agents, you can also enable decryption of RMS (Rights Management Service) protected documents/emails to facilitate offline content indexing. For detailed information on content indexing RMS protected documents/emails, see Content Indexing RMS Protected Files.

USING UNC PATHS FOR JOB RESULTS DIRECTORY

UNC paths are supported for job results directory by the Exchange Database *iDataAgent* 2007 and above when configured in Cluster Continuous Replicator environment. The Windows File System *iDataAgent* is also supported when configured in this environment.

When assigning UNC paths, the designated directory must be ONE level below the directory which is shared for this purpose. Examples:

`\\machine1\<share_name>\job_results\` is shared. Then specify `\\machine1\<share_name>\job_results\job_results_1` as the job results directory.

`\\machine1\<share_name>\job_results\` is shared. Then specifying `\\machine1\<share_name>\job_results` as the job results directory is not supported.

USER IMPERSONATION FOR ACCESSING THE JOB RESULTS DIRECTORY

On a Windows client, you need to specify a Windows User Account with the appropriate privileges to access the job results directory.

User impersonation requires that the specified user have write permissions to the product installation folders; otherwise, the user impersonation account may not take effect. This is especially true if the associated computer is not part of a domain and if the user is not a domain user. Additionally, users will need full permissions (registry rights) to the following registry key: `\\HKEY_LOCAL_MACHINE\SOFTWARE\CommVault Systems`.

In addition, if UNC paths are used for job results and subclient contents are specified as UNC paths, the user impersonation account used for the job results directory must have access to both paths.

For the File System *iDataAgent*, the user impersonation occurs only once; therefore, the user impersonation account specified for the job results directory will take precedence and will be used to back up the contents of the UNC path included in the subclient content.

For the Virtual Server *iDataAgent*, the user impersonation account specified for the job results directory will take precedence and will be used to backup and

restore data from a virtual machine. This may result into file access related issues during the backup. Therefore, it is recommended to use a local folder on the client computer as the job results directory.

For the Exchange iDataAgent, the account must have the following:

- The account must have the Remote Access rights to the UNC path.

Remote Access can be granted by right-clicking **My Computer | Properties | Remote | Select Remote Users | Add** and then specifying the domain\user in the **Select User** dialog box in the computer hosting the UNC path.

- In addition, the Exchange Administrator account specified in the Agent Properties dialog box must have write access permissions to the share used for job results.

For step-by-step instructions, see [Change the User Account for Accessing the Job Results Directory](#).

CLIENT CONNECTIVITY

You can check whether or not a client is accessible in the CommCell by using the **Check Readiness** option in the CommCell Console.

When selected, this option will display a message indicating whether or not the client is accessible. If the client is not accessible, you can check the Service Control Manager to ensure the client's services are running.

For step-by-step instructions, see [Check Client Connectivity](#).

COMMNET CLIENT CONNECTIVITY

If the CommCell is registered to a CommNet Server, the client readiness check is automatically run every 24 hours from 1:00 PM to 2:00 PM. If necessary you can change these values using the following registry keys:

- To change the frequency use the ClientCheckInterval registry key. As the client readiness check can be expensive, especially in a CommCell with a number of clients, exercise caution while changing the value.
- To change the time range use the ClientCheckWindowStartHour and ClientCheckWindowEndHour registry keys.

Client readiness checks cannot occur when services are down. The initial client readiness check is triggered 30 minutes after services are restarted. Once triggered, the values set in the registry keys are honored.

CLIENT CONFIGURATION CONSIDERATIONS

Consider the following when configuring your clients:

- The volume containing the job results directory must have sufficient free space for the collect file. Bear this in mind when backing up large file systems, such as those residing on a SAN. Each subclient in each backup set will consume disk space for the collect file. Change the Job Results Path of the Client if there is insufficient room for collect file growth during large backups.

The **Collect File** records the path and name of each scanned file that is to be backed up; therefore, the collect file size is determined by the number of files to be backed up and the length of the file path and file name. If you are working with very deep directory structures, the file paths will be longer, and this impacts the collect file size. When performing full backups of large file systems with a mix of short and long file paths, plan on collect file growth of approximately 50MB for every 1 Million files. Plan on 100MB-200MB per one million files if most of the files in your backup operation have very long file paths (200 + characters in length). Incremental and Differential backups tend to back up fewer files than full backups, and so create smaller collect files.

- If you change the path of the URLs in the Client Properties (Search Server URLs) tab, which are used for accessing the end-user or compliance user Search Console and/or the User Administration page, then you must manually update the corresponding virtual directory path in the IIS Server. Likewise, if you change the path of the URLs in the IIS Server that are used for accessing the end-user or compliance user Search Console and/or the User Administration page, then you must manually update the corresponding paths in the Client Properties (Search Server URLs) tab.

OPERATION WINDOW

You can configure operation rules at this level using the Operation Window. See [Operation Window](#) for an overview.

AUDIT TRAIL

Operations performed with this feature are recorded in the Audit Trail. See [Audit Trail](#) for more information.

[Back to Top](#)

Client - How To

Topics | [How To](#) | [Related Topics](#)

[Enable or Disable Operations](#)

[Browse the Latest Data](#)

[Check Client Connectivity](#)

[Configure Data Interface Pairs](#)

[Configure the Client for Data Encryption](#)

[Configure the Proxy for Exchange](#)

[Configure the Search Server URLs](#)

[Configure Deduplication Options for the Client](#)

[Release License for a Client](#)

[Suspend Use of a Client Computer Temporarily](#)

[Change the Job Results Path of a Client](#)

[Change the User Account for Accessing the Job Results Directory](#)

[Change the Retention of the Job Results of a Client Computer](#)

[Set the Job Priority of a Client](#)

[Specify CDR Log File Location on Source and Destination Computers](#)

[View Data Interface Pairs Configured for the Client](#)

[View the Data Recovery Job History of a Client](#)

[View the Data Protection Job History of a Client](#)

[View the Log Files of a CommServe, SRM Server, MediaAgent, or Client Computer](#)

[Delete a Client Computer](#)

[Delete a Pseudo-Client](#)

[Delete Data Interface Pairs](#)

[Create a DB2 DPF Client](#)

[Add a NAS Client](#)

[View the Software Install Folder](#)

For remote clients:

- [Store Automatic Update Packages Locally before Installation](#)

[Associate or Disassociate a User Group to a Client](#)

[Associate or Disassociate a Client to a Client Group](#)

[Enable/Disable Robust Network Layer](#)

[Change Robust Network Layer Configuration](#)

[View the Software Version \(For CommServe, MediaAgent, Client and/or Agent\)](#)

ENABLE OR DISABLE OPERATIONS

Required Capability: See Capabilities and Permitted Actions

Level	Capability
CommCell	Administrative Management with CommCell level association
Client Computer Group	Administrative Management with Client Computer Group level association
Client	Agent Management with Client level association
Agent	Agent Management with Agent level association
Subclient	Agent Management with Subclient level association

▶ To enable or disable activity control at the CommCell, client computer group, client, agent, or subclient levels:

1. From the CommCell Browser, right-click the CommServe, client computer group, client computer, agent, or subclient, and then click **Properties** from the short-cut menu.
2. From the Activity Control tab of the associated Properties dialog box, select or clear option(s), as desired.
3. Click **OK**.



Disabled data management and/or data recovery operations are displayed with client and/or agent icon changes in the CommCell Browser. For a comprehensive list of all icons in the CommCell Console, see CommCell Console Icons.

BROWSE THE LATEST DATA

The following procedure can be used to browse data from the client, agent, instance, backup set, replication set, or subclient level, depending on the functionality of a given agent.

Required Capability: See Capabilities and Permitted Actions

▶ To browse the latest data:

1. From the CommCell Browser, right-click the level whose data you want to browse, click **All Tasks**, and then click the **Browse/Browse Backup Data** option from that level.
2. From the Browse Options dialog box, click **OK** to execute the browse using the **Browse the Latest Data** option.

CHECK CLIENT CONNECTIVITY

Required Capability: None.

▶ To check client connectivity:

1. From the CommCell Browser, right-click the icon of the client computer whose connectivity you want to check.
2. Click **All Tasks**, and then click **Check Readiness**.
3. A message will be displayed indicating whether or not the client is accessible in the CommCell.
4. Click **Ok**.

CONFIGURE DATA INTERFACE PAIRS

Before You Begin

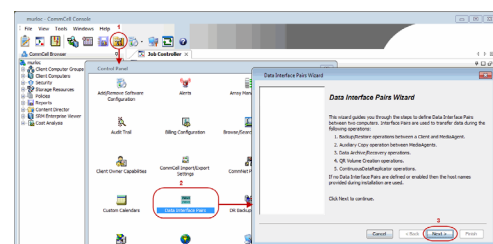
- When you create a data interface between two computers, you must ensure that there is a network path between the two computers. If there is no network path between the two computers all operations will fail. If necessary, check with your network administrator to determine whether a given interface pair is valid.

Required Capability: Capabilities and Permitted Actions

▶ To configure data interface pairs:

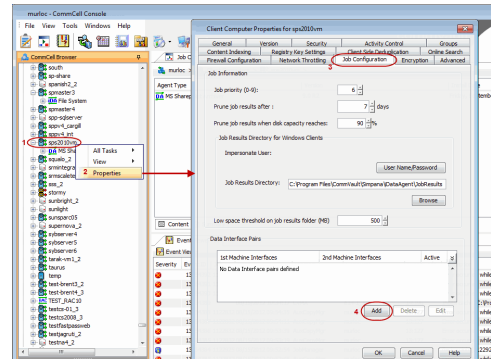
1. From the **Tools** menu in the CommCell Console, click **Control Panel** and then double-click **Data Interface Pairs**.

The **Data Interface Pairs Wizard** guides you through the process of creating Data Interface Pairs between any two computers. Click **Next** to continue.



Alternatively, you can also configure data interface pairs from the client computer:

- From the CommCell Browser, right-click the **<Client>** for which you wish to configure data interface pair, and click **Properties**.
- Click the **Job Configuration** tab.
- Under the **Data Interface Pairs** section, click the **Add** button.



2. Select the names of computers for which you want to define the Data Interface Pairs and then click **Next**.
3. Click **Add**.
4. Select the network interface name that you want to use for each client, and then click **Next**. This will become the interface pair for communication between the two clients.
 - If you do not find an specific network interface in the list, you can type the name or IP address of the NIC card.
 - In the case of remote computers, it is important to specify a network interface that is visible to the other computer.
5. The interface names between the two computers are displayed. Click **Next** to continue.

No more than one data interface pair should be created between two computers. If you want to establish a new interface pair, delete the existing one and configure the interface you want to use.
6. Click **Finish** to create the new data interface pair.

CONFIGURE THE CLIENT FOR DATA ENCRYPTION

To encrypt data during data protection and recovery operations using the CommCell Console, you must configure encryption at the client level first and then at the subclient level.

To encrypt data during third-party Command Line operations, you must configure encryption at the client level first and then at the instance level.

See Data Encryption - Support for a list of supported products.

Before You Begin

This procedure configures data encryption for all supported agents that reside on this client, however, no content at any level (instance or subclient) will be encrypted until the respective level's encryption property is enabled.

Required Capability: Capabilities and Permitted Actions

▶ To configure the client for data encryption:

1. From the CommCell Console, right-click the Client and click **Properties**.
2. From the client's Client Properties (Encryption) tab, select the **Encrypt Data** check box to enable options.
3. Select options based on the criteria described in the Encryption tab help.
4. Configure data encryption for Restore Access and Direct Media Access.

If you configure data encryption with **With a Pass-Phrase** and do not elect to export the pass-phrase to destination servers:

- o You will be required to enter the pass-phrase during immediate data recovery operations.
- o You will not be able to run scheduled data recovery operations.

If you do not require this level of security, consider using **Regular** encryption instead or Export an Encryption Pass-Phrase. The following requires you to export the pass-phrase:

- o Scheduled data recovery operations
- o Stub data recovery operations (initiated from Migration Archiver Agents)
- o Third-party Command Line data recovery operations

Note, if you selected pass-phrase security you must enter a pass-phrase in the dialog box that appears.

5. Click **OK** to save your settings and close client properties.
-

CONFIGURE THE PROXY FOR EXCHANGE

Before You Begin

- Review Configuring the Proxy for Exchange.

Required Capability: Capabilities and Permitted Actions

▶ To configure the Proxy for Exchange client:

1. From the CommCell Browser, right-click the icon of the client computer hosting the Exchange Server whose proxy client needs to be configured, and then click **Properties**.
2. From the Advanced tab of the **Client Computer Properties** dialog box, select the name of the proxy client from the **Proxy for Exchange** list.

NOTES

- For 32-bit on 64-bit configurations, select the client name of the instance containing the 32-bit Exchange agents.
 - For off-host proxy configurations, select the client name of the off-host proxy computer.
3. Click **OK** to save your changes.
-

CONFIGURE THE SEARCH SERVER URLS

Before You Begin

- Review Configuring the Search Server URLs.
- When editing the Search Server URLs, keep in mind that any changes must be synchronized with the associated Virtual Directory name on the IIS Server.

Required Capability: Capabilities and Permitted Actions

▶ To configure Search Server URLs for the client:

1. From the CommCell Browser, right-click the icon of the client computer for which you would like to configure the Web Server URLs, and then click **Properties**.
 2. From the Search Server URLs tab of the **Client Computer Properties** dialog box, enter the desired changes.
 3. Click **OK** to save your changes.
-

CONFIGURE DEDUPLICATION OPTIONS FOR THE CLIENT

Required Capability: Capabilities and Permitted Actions

Before You Begin

Review Source Deduplication.

▶ To configure deduplication options for the client:

1. From the CommCell Browser, right-click the client computer for which you wish to configure deduplication options, and then click **Properties**.
 2. From the Client Side Deduplication tab of the **Client Computer Properties** dialog box, provide the following options.
 3. If you wish to deduplicate the client's backup data on the client side before transferring the data to the MediaAgent, select **Perform client side Deduplication**.
 4. If you wish to maintain a signature cache at the client for local lookups, select **Enable Client Side Disk Cache**.
 5. Click **OK** to save your changes.
-

RELEASE LICENSE FOR CLIENT, MEDIAAGENT, AGENT, OR ENABLER

Required Capabilities: Capabilities and Permitted Actions

Administrative Management capability cannot be used to release the license from the MediaAgent level.

Before you Begin:

- To release license for MediaAgent, ensure that all the storage policies or copies associated with the configured libraries (or drive pools) in the MediaAgent are deleted or re-associated to another MediaAgent.

▶ To release license for client, MediaAgent, agent, or enabler:

1. In the CommCell Browser, right-click the name of the client, MediaAgent, agent, or enabler you want to release license, click **All Tasks** (if displayed), and select **Release License**.
2. A popup warning message appears.
Click **OK** to continue.
3. Another popup message then appears.
Click **Yes** to continue with the deconfiguration or **No** to abort.
4. If releasing a license is unsuccessful, a number of popup messages appears. In some cases, the message requests that you take some corrective action. For example, the message might advise you to ensure that there are no jobs running on the agent. In such a case, click **OK** and take the appropriate action. Then repeat the process.

If releasing a license is successful, the tree element is dimmed and available for deletion.

SUSPEND USE OF A CLIENT COMPUTER TEMPORARILY

Required Capability: Capabilities and Permitted Actions

▶ To suspend use of a client computer temporarily:

1. Create a New Scratch Pool that does not contain any media, and name it `No_Media`. Note that a scratch pool with no media associations does not harm any existing configurations, nor does it misuse media.
2. Create a Storage Policy (standard), name it `No_Backups`, and point it to the `No_Media` scratch pool.
3. Disable Operations for the client that you are temporarily disabling.
4. Verify that the Queue Jobs if Activity Control is Disabled option is disabled. This will reduce the number of queued jobs in the Job Controller.
5. Re-point all the client's subclients to the `No_Backups` storage policy. When a user changes the storage policy association of a subclient, retention cycles are set to zero (0), therefore, only the retention days must be exceeded for data to be aged. In this case, the data in the storage policy to which the client's subclients were originally pointing to will age accordingly. Note that if the client computer's activity is re-enabled, you can point the subclients back to their original storage policy.
6. To resume client activity: Enable Operations for the client, and point the subclients back to their original storage policy.

NOTES

- This feature does not require a user to uninstall client software; therefore, no licenses are released during this process.
- Any scheduled jobs associated with the suspended client will cause job failures when initiated. This is normal behavior. Once client activity is re-enabled, these scheduled jobs will no longer cause job failures.

CHANGE THE JOB RESULTS PATH OF A CLIENT**Before You Begin**

Review Using UNC Paths for Job Results Directory

Required Capability: Capabilities and Permitted Actions

▶ To change the job results path of a client:

1. From the CommCell Browser, right-click the icon of the client computer whose job results path you want to change, and then click **Properties**.
2. From the Job Configuration tab of the **Client Computer Properties** dialog box, if necessary or desired, click **User Name/Password** to establish or change the Impersonate User account to access the Job Results Directory. If you do this, click **OK** once you have administered the account.
3. From the Job Configuration tab, type a new job results path in the **Job results path** field.
You can also click **Browse** to browse to a new job results path from the **Browse for Job Result Path** dialog box. Click **OK**.
4. Click **OK** to save your changes.

CHANGE THE USER ACCOUNT FOR ACCESSING THE JOB RESULTS DIRECTORY

Required Capability: Capabilities and Permitted Actions

▶ To change the user account for accessing the Job Results Directory for the client:

1. From the CommCell Browser, right-click the icon of the client computer whose job results path user account you want to change, and then click **Properties**.
 2. From the Job Configuration tab of the **Client Computer Properties** dialog box, click **User Name/Password**.
 3. In the Change User Account dialog box, enter the appropriate User Impersonation account information.
 4. Click **OK** to save your changes.
-

CHANGE THE RETENTION OF THE JOB RESULTS OF A CLIENT COMPUTER

Required Capability: Capabilities and Permitted Actions

▶ To change the retention of the job results of a client computer:

1. From the CommCell Browser, right-click the icon of the client computer whose job results retention criteria you want to change, and then click **Properties**.
 2. From the Job Configuration tab of the **Client Computer Properties** dialog box, select the number of days job results should be pruned from the **Prune job results after** field.
 3. Select a disk capacity after which job results should be pruned from the **Prune job results when disk capacity reaches** field.
 4. Click **OK** to save your changes.
-

VIEW DATA INTERFACE PAIRS CONFIGURED FOR THE CLIENT

Required Capability: Capabilities and Permitted Actions

▶ To view data interface pairs:

1. In the CommCell Browser, right-click the Client computer for which you wish to view the data interface pair, and select **Properties**. In the client's properties dialog box, select the **Advanced** tab.
 2. The list of data interface pairs configured for the client is displayed in the **Data Interface pairs** area.
 3. Click **OK** to exit the screen.
-

SET THE JOB PRIORITY OF A CLIENT

Required Capability: Capabilities and Permitted Actions

▶ To set the priority of a client:

1. From the CommCell Browser, right-click the client computer icon, and then click **Properties** from the short-cut menu.
 2. From the Job Configuration tab of the Client Computer Properties dialog box, click in the Job Priority (0-9) field and enter a new client priority value. Remember that the lower the value, the higher the priority.
 3. Click **OK** to save your changes.
-

SPECIFY CDR LOG FILE LOCATION ON SOURCE AND DESTINATION COMPUTERS

Before You Begin

- On Windows, this procedure can be performed on both the source and destination computer(s); On UNIX, this procedure only applies to a source computer.

Required Capability: Capabilities and Permitted Actions

▶ To specify a location for the CDR log files:

1. In the CommCell Browser, right-click the Client on either a source or destination computer, and select **Properties**.
2. In the **Advanced** tab of the Client Computer Properties screen, type or browse to path for **CDR Log File Location**.
3. Click **OK** to save your changes.

VIEW THE DATA RECOVERY JOB HISTORY OF A CLIENT

▶ To view the history of data recovery operations:

1. From the CommCell Browser, right-click a client computer whose data recovery history you want to view, click **View**, then click to view a job history.
2. From the Job History Filter dialog box, select **Restore, QR Volume Recovery, Recovery/Retrieve** and/or **Stub Recall** from the Data Recovery Operations pane, then click **OK**.
 - If you want to view more advanced options for restores, from the Job History Filter, select **Restore**, then click **Advanced**.
 - From the Data Recovery History Advanced Filter select the destination client computer of the restores you would like to view, then click **OK**.
3. The system displays the results of the options you selected in the Data Recovery Job History window.

If you selected **Stub Recall** as a job history filter option, the system displays the results of the options you selected in the **Data Recovery Job History** window's Stub Recall Jobs tab.

4. Click **OK**.
-

VIEW THE DATA PROTECTION JOB HISTORY OF A CLIENT

▶ To view the data protection job history of a client:

1. From the CommCell Browser, right-click a client computer whose data protection history you want to view, click **View**, then click **View Job History**.
 2. From the Job History Filter, select **Backup, QR Volume Creation**, and/or **Archive/Compliance Archive** from the Data Protection Operations pane, then click **OK**.
 3. If you want to view more advanced options, from the Job History Filter window, select **Backup** and/or **QR Volume Creation**, then click **Advanced**.
 4. From the Data Protection History Advanced Filter, select the type of backup you would like to view, as well as the type of QR Volume Creation operation. Click **OK**.
 5. The system displays the options you selected in the Data Protection Job History window.
 6. Click **OK**.
-

VIEW THE LOG FILES OF A COMMSERVE, SRM SERVER, MEDIAAGENT, OR CLIENT COMPUTER

Required Capability: See Capabilities and Permitted Actions

▶ To view the log files of a CommServe, MediaAgent, or client computer.

1. From the CommCell Browser, right-click a CommServe, MediaAgent, or client computer, click **View**, and then click **Log Files**. The **Select the Log File to Open** window displays.
 2. To see a specific log file, either select the log file name from the list or type the name of the log file in the field provided. (In the **Files of type** field, **Log Files (*.log)** is displayed by default.) Click **Open**. The contents of the log file are displayed.
-

DELETE A CLIENT COMPUTER

Before You Begin

- Before deleting the client computer for most agents, remove the base client software.
- In order to remove the base client software, there must be no agents installed on the client computer.

Required Capability: Capabilities and Permitted Actions

▶ To delete a client computer:

1. From the CommCell Browser, right-click the icon of the client computer that you want to delete, click **All Tasks** and then click **Delete** from the short-cut menu.

If the **Delete** command is not available, then you have not successfully deleted the base client software (if relevant) from the client computer.

2. A confirmation message appears. Click **Yes** to delete the client computer or click **No** to cancel the deletion.

If you click **Yes**, the backup data that corresponds to the selected client computer is deleted. Consequently, you will not be able to browse or restore this data. If you click **Yes**, the client computer icon is removed from the view.

DELETE A PSEUDO-CLIENT

Before You Begin

- For NAS clients, the client must first be deconfigured before you can delete it. For more information, see Deconfiguring Agents.

Required Capability: Capabilities and Permitted Actions

▶ To delete a pseudo-client:

1. From the CommCell Browser, right-click the icon of the pseudo-client that you want to delete, click **All Tasks** and then click **Delete** from the short-cut menu.

For a NAS client, if the **Delete** command is not shown, you have not deconfigured the client, and the **Deconfigure** command will be shown instead; refer to Deconfiguring Agents. (There is no base client software for a NAS Client.)

2. A confirmation message is displayed. Click **OK**, type the supplied phrase in the **Enter Confirmation Text** dialog box, and click **OK**. The pseudo-client icon should be removed from the view.

DELETE DATA INTERFACE PAIRS

Required Capability: Capabilities and Permitted Actions

▶ To delete data interface pairs:

1. From the **Tools** menu in the CommCell console, click **Control Panel**, and then double-click **Data Interface Pairs**. Select the names of computers of which you wish to delete the Data Interface Pairs and then click **Next**.
2. The **Data Interface Pairs Wizard** displays the list of data interface pairs available.
3. Select the data interface pair you wish to delete, and then click the Delete button.
4. Select **Next** to review the details and click **Finish** to delete the selected data interface pair.

CREATE A DB2 DPF CLIENT

When you create a DB2 DPF pseudo-client, you also create a DB2 DPF partition instance at the same time. Each pseudo-client can include only this one partition instance; you cannot create additional instances for any one pseudo-client. To create additional partition instances, you must create additional pseudo-clients.

Before You Begin

Review the following to avoid common problems:

- You should have administrative privileges.
- Ensure that the user group to which the user belongs has agent management capability on the DB2 DPF clients that will be added to the DB2 DPF pseudo-client.
- You have the appropriate licenses available.

Add Client Checklist

For each DB2 DPF pseudo-client/instance that you want to create, collect the following information in the first block before creating the pseudo-client. Also collect the information in the second block. (Use the spaces provided to record the information. Retain this information in your Disaster Recovery binder.)

1. Name of the DB2 DPF pseudo-client: _____
 Instance path for which the DB2 DPF pseudo-client is being created: _____

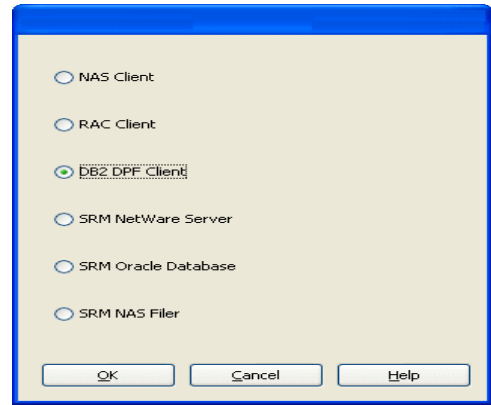
 User account information (Windows only, optionally): _____
 Names of DB2 DPF database partitions and corresponding clients for the DB2 DPF instance

2. Storage policy to be used by the default subclient for data: _____
 Storage policies to be used by the instance for user command backups and archive log backups: _____

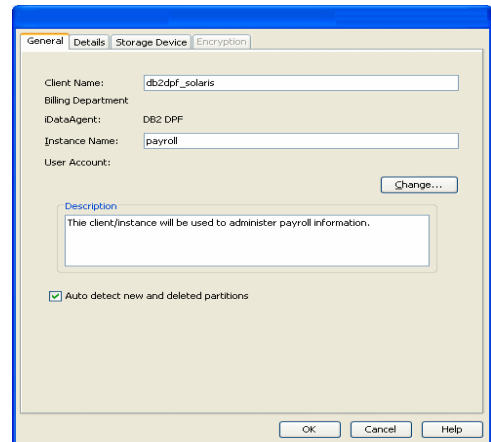
To create a DB2 DPF Client

1. From the CommCell Console, right-click **Client Computers** and click **New Client**.
2. From the Add New Client dialog box, click **DB2 DPF Client** and then click **OK**.

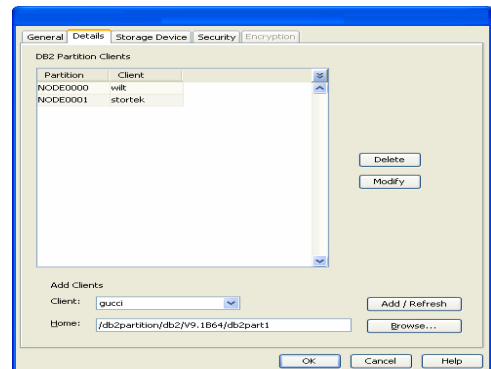
3. In the Create DPF Client (General) dialog box, type or select values for the fields as appropriate. To change the Windows user account, click **Change User Account**, type the DB2 DPF user name and password credentials, and click **OK**. Ensure that Auto detect new and deleted partitions is enabled. Then click **Details**.



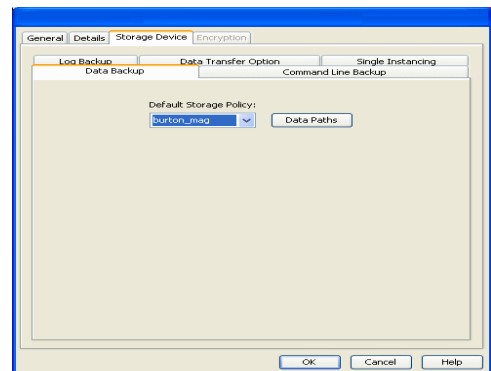
4. In the Create DPF Client (Details) dialog box, use the Clients list and click **Add/Refresh** to include the appropriate database partitions in the instance. Selected database partitions and their corresponding clients will be displayed in the DB2 Partition Clients space.



5. From the Data Backup tab in the Create DPF Client (Storage Device) dialog box, click the default data storage policy from the list.

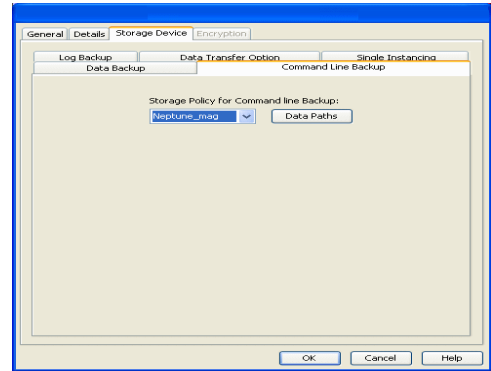
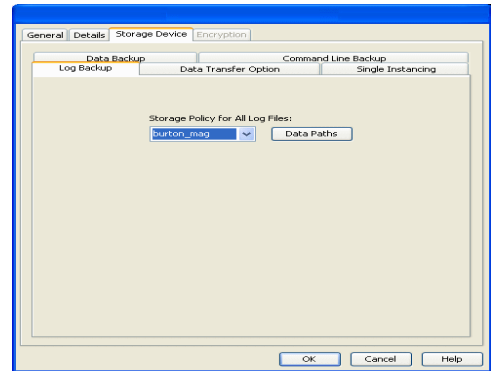


6. From the Log Backup tab in the Create DPF Client (Storage Device) dialog box, click the storage policy for all log files from the list.



- From the Command Line Backup tab in the Create DPF Client (Storage Device) dialog box, click the storage policy for command line backups from the list.

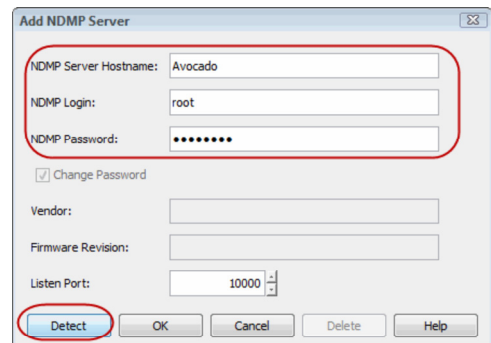
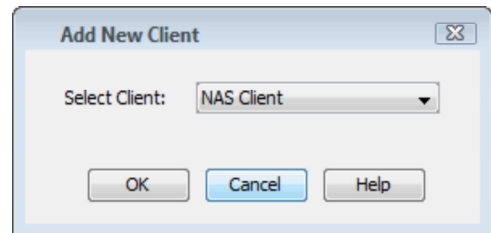
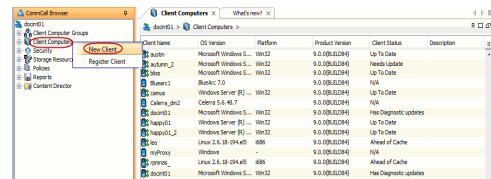
Also, configure items in the Data Transfer Option and De-Duplication tabs as appropriate.



- Click **OK**.
This task is now complete.

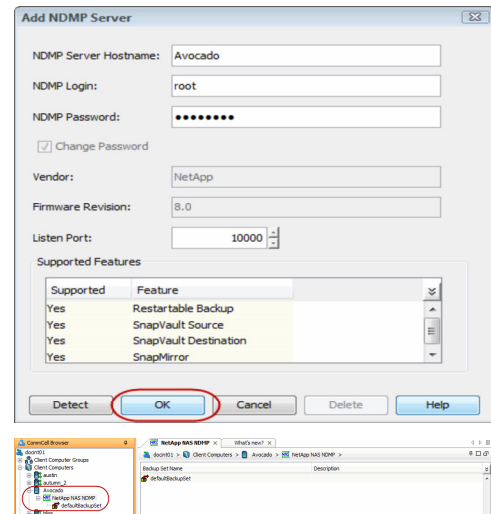
ADD A NAS CLIENT

- From the CommCell Browser, right-click **Client Computers**.
 - Select **New Client**.
- Select **NAS Client** from the list.
 - Click **OK**.
- Enter the NAS file server in the **NDMP Server Hostname** field.
 - Enter the user account used to access the storage device in the **NDMP Login** field.
 - For NetApp, type **root**.
 - For EMC Celerra, type **ndmp**.
 - For all other file servers, use any valid login.
 - In the **NDMP Password** field, enter the password for the login account.
 - Click **Detect**. The system automatically populates the **Vendor**, **Hardware OS Revision**, and **Listen Port** information.



- Click **OK**.
Depending on the File Server you are using, your screen may look different from the example shown.

- In the CommCell Browser, confirm that the NAS client was added under **Client Computers**.



VIEW THE SOFTWARE INSTALL FOLDER

▶ To view the Software Install folder:

- From the CommCell Browser, click the **CommServe, Client, Agent or MediaAgent** for which you wish to view the version, and then click **Properties**.
- Click the Version tab.

The **Software Install Directory** displays the software installation folder on the local computer.

STORE AUTOMATIC UPDATE PACKAGES LOCALLY BEFORE INSTALLATION

▶ To Store Update Packages Locally before Installation:

- From the CommCell Browser, click the **Client or MediaAgent** for which you wish to configure the Update installation, and then click **Properties**.
- Click the Version tab.
- To store update packages locally before installation, specify a local folder in the **Store Updates Locally** field in which the updates must be stored. This serves as a temporary cache area. Note that you cannot specify a different folder to serve as the temporary cache area for NetWare clients; this field is disabled.
- Click **OK** to save the information.

ASSOCIATE OR DISASSOCIATE A USER GROUP TO A COMMCELL OBJECT

Required Capability: See Capabilities and Permitted Actions

▶ To associate or disassociate a user group to a CommCell entity:

- From the CommCell Browser, click the CommServe, client computer group, client computer, agent, MediaAgent, Library, Storage Policy, backup set, subclient, or Shelf media, and then select **Properties**.
- From the **Security** tab, select the appropriate user groups to which you want to associate to the CommCell object from the **Available Groups** pane, and then move the user group to the **Associated Groups** pane.
- Click **OK**.

ASSOCIATE OR DISASSOCIATE A CLIENT TO A CLIENT GROUP

Required Capability: Capabilities and Permitted Actions

▶ To associate or disassociate a client to a client group:

- From the CommCell Browser, right-click the icon of the client computer for which you would like to configure the Web Server URLs, and then click **Properties**.
- From the Groups tab of the **Client Computer Properties** dialog box, associate a client to a client group or remove the association from a group.

3. Click **OK** to save your changes.
-

ENABLE/DISABLE ROBUST NETWORK LAYER

Required Capability: Capabilities and Permitted Actions

▶ To enable or disable the Robust Network Layer feature:

1. From the CommCell Console, right click on a client, and select **Properties** from the pop-up menu. Select the Client Computer Properties (Advanced) tab.
Alternatively, right click on a MediaAgent and select **Properties** from the pop-up menu. Select the MediaAgent Properties (Control) tab.
 2. Select the **Enable retry on network errors** option to enable the feature. Deselect it to disable the feature.
 3. Click **OK**.
-

CHANGE ROBUST NETWORK LAYER CONFIGURATION

Required Capability: Capabilities and Permitted Actions

▶ To change the Robust Network Layer configuration:

1. From the CommCell Console, right click on a client, and select **Properties** from the pop-up menu. Select the Client Computer Properties (Advanced) tab.
Alternatively, right click on a MediaAgent and select **Properties** from the pop-up menu. Select the MediaAgent Properties (Control) tab.
 2. Select the **Enable retry on network errors** option to enable the feature. Deselect it to disable the feature. If enabled, you may configure the following:
 - **Retry Frequency (seconds):** The interval (in seconds) at which the Job Manager will continuously check for network connectivity. Default is set at 30 seconds.
 - **Retry Count:** The number of times the Job Manager will check for network connectivity. Default is set at 40.
 3. Click **OK**.
-

VIEW THE SOFTWARE VERSION

▶ To view the Software Version:

1. From the CommCell Browser, click the **CommServe, Client, Agent, MediaAgent, or Enabler** for which you wish to view the version, and then click **Properties**.
 2. Click the Version tab.
The component version and post release service pack, additional updates and missing updates are displayed.
-

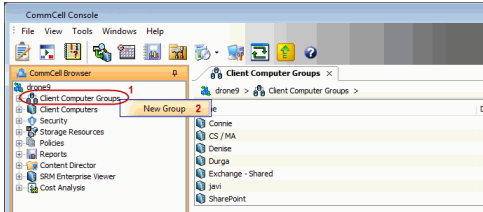
Client Computer Groups

Getting Started | **Advanced**

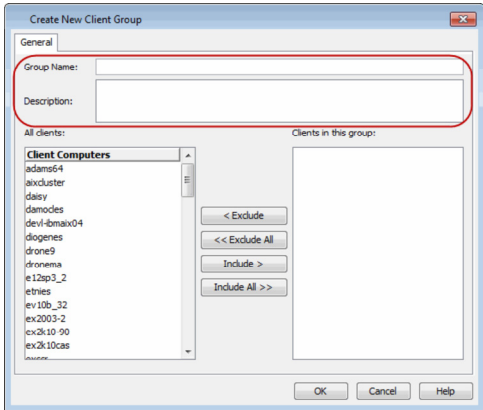
A client computer group is a logical grouping of client computers. Client Computer Group definition help to define options to the entire group instead of the individual clients.

Use the following steps to create a client computer group and to move client computers into computer group manually.

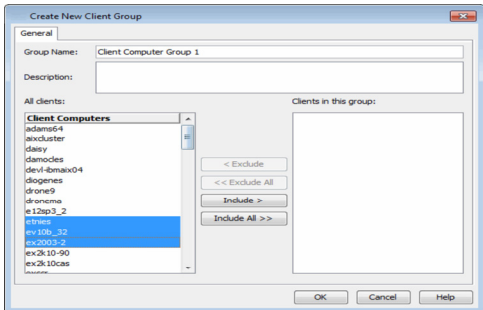
- From the CommCell Browser, right-click **Client Computer Groups** and then click **New Group**.



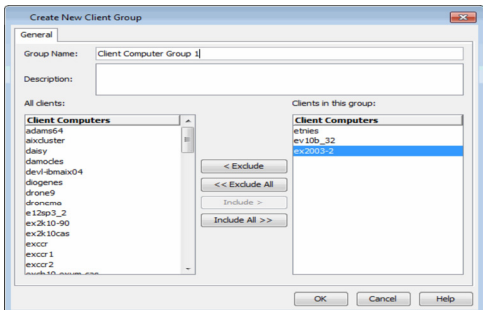
- In the **Group Name** box, type a name for your new computer group.
In the **Description** box, type the purpose of the new computer group.



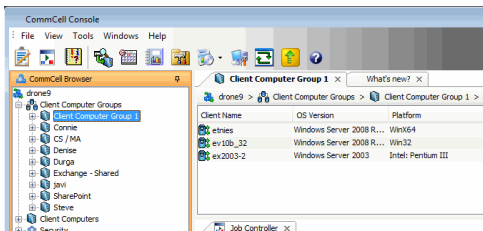
- In the list of **Client Computers**, press **Ctrl** key and select the clients that you want to move.
Click **Include >** button to move the selected clients Group to the **Clients in this group**.



- The selected clients will appear in the **Clients in this group** list.
Click **OK**.



- You can view the newly created client group under **Client Computer Groups**.



Client Computer Groups

Getting Started | **Advanced**

TABLE OF CONTENTS

Overview

Managing Computer Groups

- Enabling/Disabling Activity Control
- Associating/Disassociating Clients
- Associating/Disassociating User Groups
- Changing the Client Computer Group Name
- Configuring Firewall Settings
- Configuring Network Throttling

Configuring User Accounts for SQL Server iDataAgent Backups

Scheduling Automatic Updates

Configuring Operation Window

Viewing Job History

Deleting a Client Computer Group

OVERVIEW

A client computer group is a logical grouping of client computers. Client Computer Group definition help to define options to the entire group instead of the individual clients.

Once created, client computer groups can be used to perform the following tasks for all the members in the client group:

- Create Schedule Policies
- Set Firewall Settings
- Associate User Groups with specific security
- Install Updates
- Generate Reports
- View job history details
- Set the activity control for backup/restore operations
- Set up operation window

MANAGING COMPUTER GROUPS

Once a client computer group is created, you can configure/modify the following options:

ENABLING/DISABLING ACTIVITY CONTROL

Activity Control allows you to enable or disable all the data management, data recovery and/or online content indexing operations on all client computers that are members of a client computer group.

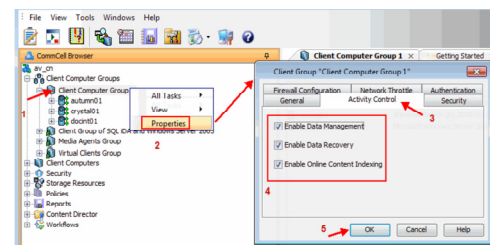
Use the following steps to enable or disable the activity control.

1. From the CommCell Browser, expand **Client Computer Groups**.
2. Right-click the **<Client Computer Group>** and then click **Properties**.
3. Click the **Activity Control** tab.
4. By default, **Enable Data Management**, **Enable Data Recovery** and **Enable Online Content Indexing** options are enabled.

To disable, clear the **Enable Data Management**, **Enable Data Recovery** and **Enable Online Content Indexing** check boxes.

5. Click **OK**.

If the data management and/or data recovery operations are disabled, client group icon changes in the CommCell Browser.



ASSOCIATING/DISASSOCIATING CLIENTS

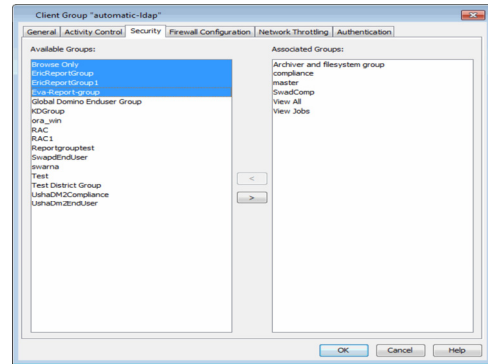
You can associate or disassociate clients to or from a client computer group.

<userGroupName>usergroup1</userGroupName>

- o **associatedUserGroupsOperationType** - Indicate one of the following operation types:

ADD - This will associate the User Group to a Client Computer Group
DELETE - This will disassociate the User Group to a Client Computer Group
OVERWRITE - To associate the user group mentioned above and disassociate all the user group available on the client computer group. For example:

If usergroup2 and usergroup3 are already associated on clientgroup1, and you wish to overwrite the available user groups with usergroup4. This operation associates usergroup4 to the clientgroup1 and disassociates usergroup2 and usergroup3.

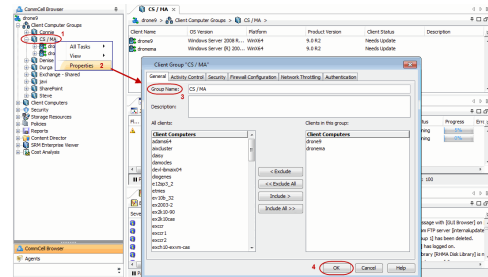


3. Save the file as **input.xml**.
4. From Command prompt, navigate to <Software_Installation_Directory>/Base and then run the following command:
 - o Login to the CommServe using the qllogin command and commcell credentials.
 For example, to log on to CommServe server1 with username user1:
 C:\>qllogin -cs server1 -u user1
 - o Run the XML using the qoperation command.
 For example, to run **input.xml**
 C:\>qoperation execute -af input.xml
5. You can verify the user group associated to client from **Associated Groups**.
 - o From the CommCell Browser, right-click the **<Client_Computer_Group>** and then click **Properties**.
 - o Click **Security** tab.
 - o The **User Group** specified above will be listed in the **Associated Groups**.

CHANGE THE CLIENT COMPUTER GROUP NAME

Use the following steps to change the name of a client computer group.

1. From the CommCell Browser, expand **Client Computer Groups**.
2. Right-click the **<Client Computer Group>** that you wish to change the name and then click **Properties**.
3. In the **Group Name**, type the new name of the computer group.
4. Click **OK**.



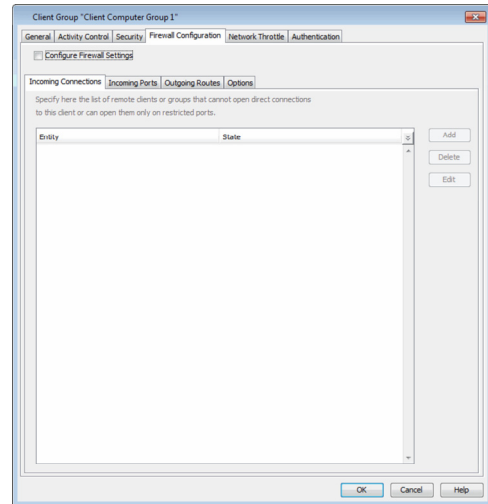
CONFIGURING FIREWALL SETTINGS

You can define the connection details for incoming and outgoing connections required to operate the client group across the firewall by configure firewall settings.

Use the following steps to configure firewall settings for client computer group:

1. From the CommCell Browser, expand **Client Computer Groups**.
2. Right-click the **<Client Computer Group>** and then click **Properties**.
3. Click the **Firewall Configuration** tab.
4. In the **Firewall Configuration** tab, provide the necessary options.
 The options depends on your firewall settings. See Firewall for more information.
5. Right-click the **<Client Computer Group>**, point **All Tasks**, and then click **Push Firewall Configuration**.

The configuration is now applicable for all the clients. You can verify the new firewall configuration on each client computer.



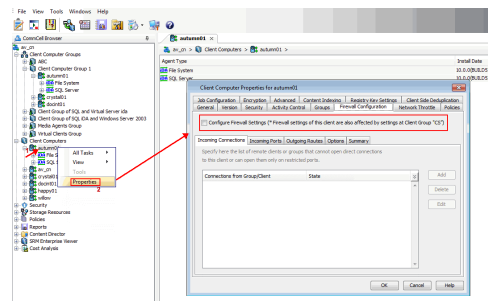
INHERIT THE FIREWALL CONFIGURATION FROM THE CLIENT GROUP

Use the following steps to configure a client to inherit the firewall settings from the client computer group.

1. From the CommCell Browser, expand **Client Computers**.
2. Right-click the **<Client Computer>** and then click **Properties**.
3. Click the **Firewall Configuration** tab.
4. In the **Firewall Configuration** tab, ensure the **Configure Firewall Settings** option is not selected.
5. Click **OK**.

Future firewall changes will be applicable at the client group level.

When **Configure Firewall Settings** is selected, the firewall configuration of both the client computer and client group are merged in the client computer.



CONFIGURING NETWORK THROTTLING

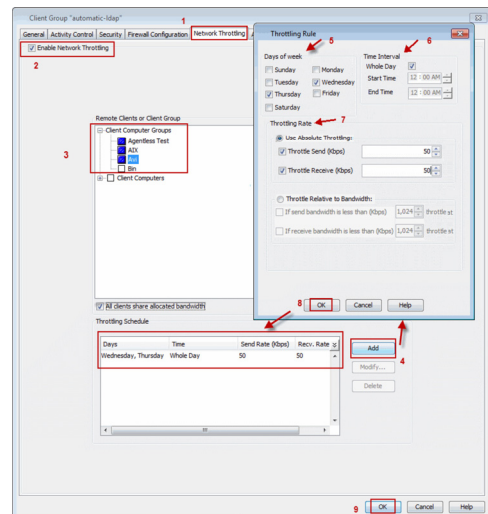
The network traffic for Clients and MediaAgents can be throttled based on the network bandwidth in your environment. This is useful if you want to limit the network bandwidth usage.

By default, network throttling is disabled. You can enable the throttling options on a client group for multiple clients. Once configured, the throttling options are applied to all data transfer and control message operations, such as Data Protection operations including Laptop Backups, Copy operations including DASH copy, Data Recovery Operations, etc.

1. From the CommCell Browser, expand **Client Computers**.
2. Right-click the **<Client Computer Group>** and then click **Properties**.
3. Click the **Network Throttling** tab.
4. Select **Enable Network Throttling** check box.
5. Under **Client Computer Groups**, select client computer groups to setup throttling.
6. By default, **All clients share allocated bandwidth** check box is selected to share the throttling settings among all selected clients cumulatively.
If this check box is cleared, each client will throttle at the configured rate instead of a combined and shared rate.
7. Click **Add** to setup throttling rules. For example:
 - o **Days of Week** - select a day or multiple days for the schedule to run.
 - o **Time Interval** - select Whole day or a specific time interval for the schedule to run.

You can select one of the following to specify a throttling rate:

- o **Use Absolute Throttling**
Select **Throttle Send** and **Throttle Receive** rate and enter values for each.
- o **Throttle Relative to Bandwidth**



Select **If send bandwidth is less than (Kbps)** to specify a minimum bandwidth required for send throttling to take affect and then specify the percentage rate to throttle the network bandwidth when the minimum bandwidth is available.

Select **If receive bandwidth is less than (Kbps)** to specify a minimum bandwidth required for receive throttling to take affect and then specify the percentage rate to throttle the network bandwidth when the minimum bandwidth is available.

If the throttle bandwidth is higher than the amount specified in Kbps, then the job will run without throttling.

Click **OK**.

The newly added throttling rules will be displayed in Throttling Schedule.

8. Click **OK**.
9. From the CommCell Browser, navigate to **Client Computer Groups** | **<Client Computer Group>** | **All Tasks** and click **Push Firewall Configuration**.
10. Click **Continue**.

CONFIGURING USER ACCOUNTS FOR SQL SERVER IDATAAGENT BACKUPS

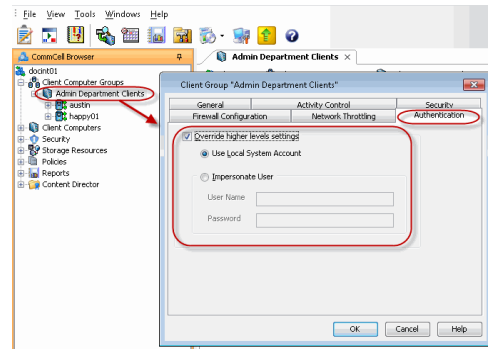
This user account will be used for all computers within a Client Computer Group. Configure the user account at this level if different users will be conducting backup and restore operations for each Client Computer Group in your organization. This user account will override the user account configured at the CommCell level.

1. Verify that all the SQL Server clients for which you wish to configure the user account are included in the Client Computer Groups.
2. Navigate to **Client Computer Groups**, right-click the **<Client Computer Group>** and click **Properties**.
3. Enable the **Override higher levels settings** check box.
4. Select the following:

Use Local System Account if the computer's Administrator account contains the required privileges.

Impersonate User if you want to use a different account that contains the required privileges. Enter the **User Name** and **Password** for this account in the space provided.

5. Click **OK**.



SCHEDULING AUTOMATIC UPDATES

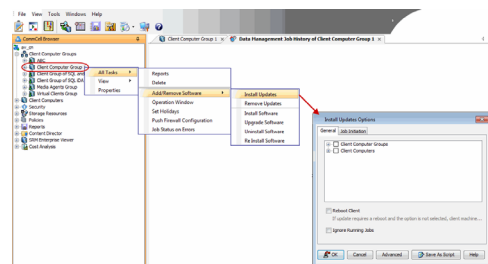
Use the following steps to schedule automatic updates to the members in the client computer group.

1. From the CommCell Browser, expand **Client Computers**.
2. Right-click the **<Client Computer>**, point to **All Tasks** | **Add/Remove Software** and then click **Install Updates**.
3. From the **Install Updates Options** dialog box, expand **Client Computer Groups** and select **<Client Computer Group>** you wish to schedule the updates job.
4. Select **Reboot Client** to have the system automatically reboot the client and/or MediaAgent computers if a reboot is required.
5. Click the **Job Initiation** tab.
6. Click **Schedule** to schedule the updates for a specific time.
7. Click **Configure** button to set the schedule for the updates job. The **Schedule Details** dialog displays.
8. Select the appropriate scheduling options. For example:

Type a name for the schedule in the **Schedule Name** box.

- o Click **Weekly**.
- o Check the days you want to run the updates job.
- o Change the **Start Time** to 9:00 PM.
- o Click **OK** to close the **Schedule Details** dialog box.
- o Click **OK** to close the **Backup Options** dialog box.

The Updates job will be executed as per scheduled.



CONFIGURING OPERATION WINDOW

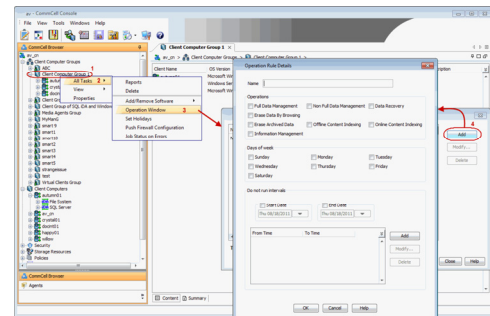
By default, all operations in the CommCell will run for 24 hours without restriction. However, it may be necessary to prevent operations from running during certain time periods of the day, e.g., during the day time when the resources are busy. To accomplish this, you can define operation rules which will enable certain operations to be run during idle periods, thereby not consuming resources such as network bandwidth, data, or storage resources during busy hours. For more information, see Operation Window.

Use the following steps to configure operation rules.

1. From the CommCell Browser, expand **Client Computer Groups**.
2. Right-click the **<Client Computer Group>**, point **All Tasks** and then click **Operation Window**.
3. From the **Operation Windows** dialog box, click **Add**.
4. In the **Operation Rule Details** dialog box, specify the following:
 - o In the **Name** box, type a name.
 - o From the **Operation**, select either an administration, data protection (either full or non-full), and/or a data recovery operations.
 - o From the **Days of week**, select the day(s) of the week to exclude the operation.
 - o From the **Do not run intervals** pane, click **Add** to add a date interval that will prevent the selected operation(s) from running.

From the **Time Intervals** dialog box, select a start and end time to exclude the operation(s) from running, then click **Add**. Click **OK** to close the **Time Intervals**.

5. Click **OK**.



VIEWING THE JOB HISTORY

Use the following steps to view the job history of a client computer group:

1. From the CommCell Browser, expand **Client Computer Groups**.
2. Right-click the **<Client Computer Group>**, and then click **View | Job History**.
3. Perform one of the following:

To view Data Protection Operations:

- o By default, **Backup, Quick Recovery Agent Volume Creation, Archive/Compliance Archive** and **Recovery Point Creation/CDR Data Verification** options are selected.
- o For advanced options, click **Advanced** button.

From the **Data Protection History Advanced Filter** dialog box, select the type of backup you would like to view, as well as the type of QR Volume Creation operation.

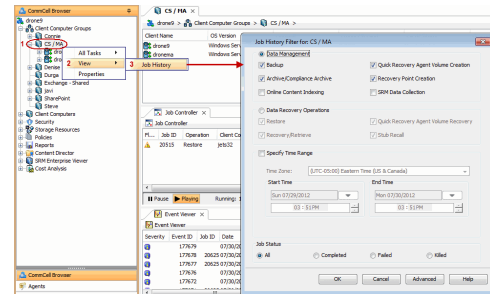
- o Click **OK**.

The system displays the options you selected in the **Data Protection Job History** dialog box.

To view Data Recovery Operations:

- o Select **Data Recovery Operations**. All restore operation types are selected by default.
- o If you want to view more advanced options for restores, click **Advanced**.
- o From the **Data Recovery History Advanced Filter** select the destination client computer of the restores you would like to view, then click **OK**.
- o Click **OK**.

The system displays the options you selected in the **Data Recovery Job History** dialog box.

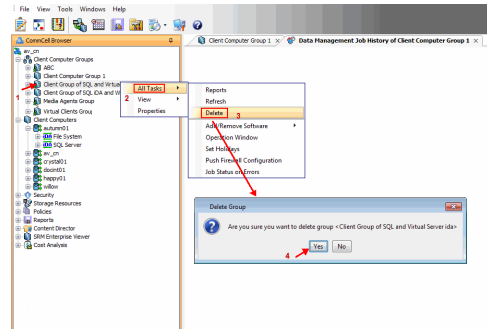


DELETING A CLIENT COMPUTER GROUP

Use the following steps to delete the client computer group.

1. From the CommCell Browser, expand **Client Computer Groups**.
2. Right-click the **<Client Computer Group>** that you want to delete, point to **All Tasks** and then click **Delete**.
3. From the **Delete Group** dialog box, click **Yes**.

The client computer group is now deleted. However, the clients of the group are still available.



Fault Tolerance

Fault tolerance for data protection operations is supported with use of the following:

Alternate Data Paths (GridStor) - Alternate data paths provide the facility to automatically switch over to an alternate data path, when one of the components in the default data path is not available. In addition to ensuring the successful completion of data protection jobs, alternate data paths utilize available libraries and drives in the event of failure or non-availability of these resources.

Clustering Support - Clustering is a way of organizing your hardware and software in order to provide added measures of performance, reliability and fault tolerance. The CommServe, MediaAgent, and certain Agents take advantage of the failover protection afforded to virtual servers within the clustering environment. If an active node fails, the software will still be able to function from the node that has not failed. Regardless of the hosting node, the software will continue to be able to perform data protection operations. Because the binaries are installed on every physical node, the software is protected from corruption; if the binaries are corrupted on one physical node, the cluster resources can fail over to another physical node, which has its own set of binaries, affording the same performance, reliability and fault tolerance as power, hardware, or application failure. In addition, this configuration allows you to apply Updates and Service Packs in a rolling fashion, to one physical node at a time.

Robust Network Layer - Robust Network Layer prevents data protection operations from restarting when network glitches or CommServe services are temporarily interrupted. It allows the connections between a CommServe, MediaAgent, and client to be retried at set intervals, if there is any temporary loss of network connectivity or outage in CommServe services. When this feature is enabled, data protection jobs do not enter a pending state; they will continue, without interruption, when the network or services become available.

Alerts and Monitoring

Topics | How To | Example | Support | Related Topics

Overview

- Alert Locale

Available Alerts and Alert Descriptions

- Application Management
- Automatic Updates
- Configuration
- Job Management
- Media Management

Alert Administration

Notification Types

- Email/Pager
- SNMP Traps
- System Event Viewer
- Run Command
- Save to Disk
- RSS Feeds

Alert Tokens

OVERVIEW

Alerts can inform you of conditions occurring within a CommCell that you may have otherwise not been aware of. These conditions can range from minor occurrences that do not require intervention to severe occurrences that need immediate intervention. The system detects conditions within two minutes of the occurrence.

Alerts can be configured globally or they can be job-based. Alerts that are configured globally are done so through the CommCell Console Control Panel and can be configured for all existing operations, where Job-Based alerts give users the ability to configure an alert while submitting an immediate job, scheduled job, configuring a schedule policy, or for a running job.

- To configure an alert globally, see [Configure Alerts](#).
- To configure an alert while submitting a job, see [Configure Job-Based Alerts](#).

Alerts can be sent to their intended recipients by e-mail/pager, to a Windows System Event Viewer, by SNMP Trap(s), or by running a command script. If the mail server is down, the system will attempt to send alert e-mail notification for the next four hours. If after four hours, the mail server is still down, these alerts will be removed from the system, and will not be sent to the recipient. Additionally, individual alert notifications can now be generated when users select the **Send Individual Notification for This Alert** option while configuring alerts rather than multiple alerts being generated within a single alert notification.

You can also obtain information about conditions within the CommCell from the Event Viewer or Log Files.

The Microsoft Operations Manager (MOM) 2005, NetIQ and SNMP Trap Receiver applications can be used to monitor Alerts.

Users can opt to escalate some alert notifications, by selecting the desired options in the Escalation Notification section of the alert configuration, if available.

ALERT LOCALE

By default, alert notification messages are sent in the same language as the CommCell Console used to configure the alerts. However, they can be displayed in a language other than that of the CommCell Console. You can change the locale while configuring the alert, see:

- [Configure Alerts](#)
- [Configure Job-Based Alerts](#)
 - An alert can be configured to send e-mail notifications to user groups created from within the CommCell Console as well as external domain user groups. However, individual external domain users will not receive the alert notification e-mail if they have not previously logged on to the CommCell Console. Users (from the user groups created from within the CommCell Console) will receive the alert e-mail notification regardless of their login status.
 - Disabled users and/or user groups cannot create or receive scheduled reports or alerts.

- Instance-level alerts for Oracle `rman_util` restore jobs do not work.

AVAILABLE ALERTS AND ALERT DESCRIPTIONS

The alerts available are grouped into six categories:

- Application Management
- Automatic Updates
- Configuration
- Job Management
- Media Management

The following tables identify the types of available alerts within each category, the user capabilities needed for each alert, the entities the alert can be associated with, the types of criteria available, and a description.

APPLICATION MANAGEMENT

Alert Type	User Capabilities Needed for Each Alert type	Entities that can be Associated with the Alert	Criteria	Description
ContinuousDataReplicator	Agent Management or Alert Management capability with association at the object associated with the alert.	Clients Client Groups	Log File Volume Reached Low Watermark	One of the following has occurred: <ul style="list-style-type: none"> • A destination computer has imposed throttling on the source computer, based on the percentage of allocated log space remaining on the destination computer. • A destination computer has stopped the source computer from sending logs, based on the percentage of allocated log space remaining on the destination computer. • A source computer has run out of log space, and CDR has stopped monitoring the source paths for all the Replication Pairs, put the pairs in an aborted state, and deleted all log files. The free disk space thresholds are configurable in the ContinuousDataReplicator Properties (Operational Parameters) window.
			No transfer activity	There has been no data replicated from the source to the destination. The CommServe automatically checks for transfer activity every 15 minutes.
			Failed Replication	A Replication Pair's job has failed, been aborted by a user, or aborted by the system.
Exchange	Agent Management or Alert Management capability with association at the object associated with the alert.	Clients Client Groups	Journal Mailbox Threshold Exceeded	The journal mailbox exceeded its limit. (The mailbox threshold is set by the user in the CommCell console.) <p>NOTES</p> <ul style="list-style-type: none"> • See <i>Configure the Agent for a Journal Mailbox Threshold Alert</i> in Books Online for step-by-step instructions for setting the threshold limit on the agent. • If you would like to change the interval at which the threshold limit is checked or the time-out for the monitoring process, you can set these through the <code>nArcMonitorIntervalInMins</code> and <code>nArcMonitorTimeOutInMins</code> registry keys.
SharePoint	Agent Management or Alert Management capability with association at the object associated with the alert.	Clients Client Groups	New Virtual Servers Were Found. Restart IIS Services.	New virtual servers were found on the SharePoint server after an archive operation, which requires the Internet Information Services (IIS) to be restarted.
			SharePoint version is upgraded. Restart IIS.	The SharePoint server has been upgraded, which requires the Internet Information Services (IIS) to be restarted.

AUTOMATIC UPDATES

Alert Type	User Capabilities Needed for Each Alert type	Entities that can be Associated with the Alert	Criteria	Description
Download Updates	Administrative Management or Alert Management capability with CommCell association.		Job Failed	Updates failed to be downloaded.
			Job Succeeded	Updates were downloaded successfully.
			Job Succeeded with Errors	A download updates operation completed with errors.
Install Updates	Administrative Management or Alert	Machines	Job Failed	An update installation failed.
			Job Succeeded	An update installation completed successfully.

	Management capability with CommCell association.	Client Groups	Job Succeeded with Errors	An update installation operation completed with errors.
			Job Initiated	An update installation was initiated.
Updates Available to Download	Administrative Management or Alert Management capability with CommCell association.		Updates Available to Download	An update is available to be downloaded for installation. The frequency interval at which these updates are detected is configurable in the registry key.
Upgrades and Service Packs	Administrative Management or Alert Management capability with CommCell association.	Machines Client Groups	Release Upgrade Required	A new release software upgrade is required. (If configured, this alert occurs when a Client and/or MediaAgent software version is lower than that of the CommServe.) The frequency interval at which these updates are detected is configurable in the registry key.
			Service Pack Required	A software update is required. (If configured, this alert occurs when a Client and/or MediaAgent service pack version is lower than that of the CommServe.) The frequency interval at which these updates are detected is configurable in the registry key.

CONFIGURATION

Alert Type	User Capabilities Needed for Each Alert type	Entities that can be Associated with the Alert	Criteria	Description
Clients	Agent Management or Alert Management capability with association at the object associated with the alert.	Clients	Properties Modified	The properties of a client were modified, or there was an unauthorized attempt to alter properties.
		Client Groups	Disk Space Low	The minimum thresholds have been reached for the client software installation and system directories, which include the Job Results. The threshold for Job Results directory is configurable in the CommCell Console's Client Computers Properties window. The thresholds for the software installation and system directories and the frequency interval at which the directories are monitored are configurable in the registry key. If Data Classification Enabler is installed, this alert, if configured, will be sent if 85 percent or more of the volume's disk space is consumed. For computers where QSnap and either the Quick Recovery Agent or ContinuousDataReplicator are installed, this alert, if configured, will be sent if 80 percent or more of a volume's disk space is consumed, for all of the client computer's volumes. If Content Indexing Engine is installed, this alert, if configured will be sent for the following: <ul style="list-style-type: none"> • If 80 percent or more of the volume's disk space is consumed. • If the minimum free space falls below 10 GB.
		Agents	Properties Modified	The properties of an agent were modified, new content was added (for the Oracle agent only), or there was an unauthorized attempt to alter properties. This alert is also generated if the content, pre-post commands, or storage policy of a subclient were modified.
CommCell	Administrative Management or Alert Management capability with CommCell association		Alert every <i>n</i> failed login attempts	There were <i>n</i> failed attempts made to login to the CommCell.
			Alert CommServe License Expires With <i>n</i> Days	The CommServe license will expire in <i>n</i> days.
			Alert when License Consumed reaches <i>n</i> %	The CommServe license has reached <i>n</i> %. License Capacity Usage details get updated every 24 hours. It may also be updated if a Data Aging Job is run or if CommServe services are restarted.
			Properties Modified	The properties of the CommServe were modified, or there was an unauthorized attempt to alter properties.
			Alert Modified	A user was added or removed to an alert, an alert was modified, or there was an unauthorized attempt to modify the properties of an alert.
			Force De-configured	A user failed or successfully forced de-configured an Agent,

				Client, or MediaAgent.
			Disk Space Low	<p>The minimum thresholds have been reached for the CommServe software installation and system directories or there is insufficient disk space for the CommServe database to grow.</p> <p>The threshold for the software installation and system directories and the frequency interval at which the directories are monitored are configurable in the registry key.</p> <p>The threshold for CommServe database directory, and the frequency interval at which the database directory is monitored, are configurable in the CommCell Console's Control Panel - System window (Database space check interval and Database Space Check Thresholds).</p>
Library	Library Management or Alert Management capability with library association	Libraries	Properties Modified	The properties of a library were modified, an overwrite media option was selected for the library, or there was an unauthorized attempt to alter properties of a library.
MediaAgents	Media Management or Alert Management capability with MediaAgent association	MediaAgents	Properties Modified	The properties of a MediaAgent were modified, or there was an unauthorized attempt to alter the properties of a MediaAgent.
			Disk Space Low	<p>The minimum thresholds have been reached for the MediaAgent software installation and system directories, which include the Index Cache.</p> <p>The threshold for MediaAgents Index Cache directory is configurable in the CommCell Console's MediaAgents Properties window.</p> <p>The threshold for the software installation and system directories and the frequency interval at which the directories are monitored are configurable in the registry key.</p>
			DDB Store got corrupted	Deduplication Store of a MediaAgent is corrupted.
			MediaAgent went Offline	A MediaAgent was switched on/offline.
			Notify only if Condition persists for	Notify only if the condition persists for certain length of time.
Repeat notification every	Repeat the notification for every <i>n</i> hours and <i>m</i> minutes. (<i>n</i> and <i>m</i> are set by the user at the time of configuration.)			
Schedules	Alert Management capability with CommCell association		Scheduler Changes	A schedule was added, deleted, or modified, a job failed to be scheduled, a user added, removed, or modified a holiday.
Storage Policy	Storage Policy Management or Alert Management capability with storage policy association	Storage Policies	Properties Modified	The properties of a storage policy were modified, or there was an unauthorized attempt to alter the properties of a storage policy.

JOB MANAGEMENT

Alert Type	User Capabilities Needed for Each Alert type	Entities that can be Associated with the Alert	Criteria	Description
Auxiliary Copy	Administrative Management or Alert Management capability with CommCell association	Storage Policies Storage Policy Copies	Job Succeeded	An auxiliary copy operation completed successfully.
			Job Succeeded with Errors	An auxiliary copy operation completed with errors.
			Job Skipped	A scheduled auxiliary copy operation ran late, was skipped, or was skipped due to a holiday.
			Job Failed	An auxiliary copy operation failed, failed to start, or the operation was aborted by the system.
			Job Activity	An auxiliary copy operation was killed, resumed, or suspended by a user.
			Auxiliary Copy fallen behind alert	<p>The following criteria have been met for the selected storage policy:</p> <ul style="list-style-type: none"> data to be copied is more than <i>n</i> GB jobs have not been copied in more than <i>n</i> days <p>(<i>n</i> is set by the user in the Storage Policy Properties (Advanced) window.)</p> <p>The interval at which the storage policy is checked for this criteria can be configured in the Media Management Configuration (Auxiliary Copy Configuration) window; the default Interval (Hours) between Auxiliary Copy Fallen Behind alerts is 24 hours.</p>
			Delayed by <i>n</i> Hrs	An auxiliary copy operation was in a waiting state for <i>n</i> hours. (<i>n</i> is set by the user at time of configuration.)

			Alert every <i>n</i> attempt (Phase failures)	There were <i>n</i> attempts made to resume the auxiliary copy operation after a phase failure.
			Alert every <i>n</i> attempt (Network failures)	There were <i>n</i> attempts made to resume the auxiliary copy operation after a network failure.
Backup Copy Workflow	Administrative Management or Alert Management capability with CommCell association	Storage Policies	Job Succeeded	A backup copy operation completed successfully
			Job Succeeded with Errors	A backup copy operation completed with errors.
			Job Skipped	A scheduled backup copy operation ran late, was skipped, or was skipped due to a holiday.
			Job Failed	A backup copy operation failed, failed to start, or the operation was aborted by the system.
			Job Activity	A backup copy operation was killed, resumed, or suspended by a user.
			Job Started	A backup copy operation was started by a user.
Continuous Data Replication	Data Protection Operations or Alert Management capability at each associated entity.	Clients Agents Replication Sets	Job Succeeded	A Recovery Point creation, Consistent Recovery Point creation, or CopyBack operation completed successfully.
			Job Succeeded with Errors	A Recovery Point creation, Consistent Recovery Point creation, or CopyBack operation completed with errors.
			Job Skipped	A scheduled Recovery Point creation, Consistent Recovery Point creation, or CopyBack operation ran late, was skipped, or was skipped due to a holiday.
			Job Failed	A Recovery Point creation, Consistent Recovery Point creation, or CopyBack operation failed, failed to start, or the operation was aborted by the system.
			Job Activity	A Recovery Point creation, Consistent Recovery Point creation, or CopyBack operation was killed, resumed, or suspended by a user.
			Delayed by <i>n</i> Hrs	A Recovery Point creation, Consistent Recovery Point creation, or CopyBack operation was in a waiting state for <i>n</i> hours. (<i>n</i> is set by the user at time of configuration.)
			Alert every <i>n</i> attempt (Phase failures)	There were <i>n</i> attempts made to resume the Recovery Point Creation or CopyBack operation after a phase failure.
			Alert every <i>n</i> attempt (Network failures)	There were <i>n</i> attempts made to resume the Recovery Point Creation or CopyBack operation after a network failure.
Data Aging	Administrative Management or Alert Management capability with CommCell association		Job Succeeded	A data aging operation completed successfully.
			Job Succeeded with Errors	A data aging operation completed with errors.
			Job Skipped	A scheduled data aging operation ran late, was skipped, or was skipped due to a holiday.
			Job Failed	A data aging operation failed, failed to start, or the operation was aborted by the system.
			Job Activity	A data aging operation was killed by a user.
Data Classification	Alert Management capability	Clients Client Groups	Classification Failed	A data classification operation failed to write to the database.
Data Protection	Data Protection Operations or Alert Management capability at each associated entity.	Clients Client Groups Agents Backup Sets Instance/Partition All Subclients** Subclients	Job Succeeded	A data protection operation completed successfully.
			Job Succeeded with Errors	A data protection operation completed with errors.
			Job Skipped	A scheduled data protection operation ran late, was skipped, or was skipped due to a holiday.
			Job Failed	A data protection operation failed, failed to start, or was aborted by the system.
			Job Activity	A data protection operation was killed, resumed, or suspended by a user.
			No Data Protection	A data protection operation failed to start.
			Delayed by <i>n</i> Hrs	A data protection operation was in a waiting state for <i>n</i> hours. (<i>n</i> is set by the user at time of configuration.)
			No Backup for last <i>n</i> Days	A data protection operation did not complete successfully for the last <i>n</i> days. (<i>n</i> is set by the user at the time of configuration in the alert wizard.)
			Job exceeded running time of <i>n</i> Hrs	A data protection operation was in a suspended, running or in a pending state for more than <i>n</i> hours. (<i>n</i> is set by the user at the time of configuration in the alert wizard.)
			Alert every <i>n</i> attempt (Phase failures)	There were <i>n</i> attempts made to resume the data protection operation after a phase failure.
			Alert every <i>n</i> attempt (Network failures)	There were <i>n</i> attempts made to resume the data protection operation after a network failure.
			Increase in Data Size by <i>n</i> %	A data protection job is at least <i>n</i> % larger in data size than the previous data protection job of the same type (full, incremental, differential or synthetic full). Default is set at 10%. (<i>n</i> is the percentage of increase in data size, at which if

				met, will trigger the alert. The actual data size increase may be larger than the $n\%$.)
			Decrease in Data Size by $n\%$	A data protection job is at least $n\%$ smaller in data size than the previous data protection job of the same type (full, incremental, differential or synthetic full). Default is set at 10%. (n is the percentage of decrease in data size, at which if met, will trigger the alert. The actual data size decrease may be larger than the $n\%$.)
			Notify only when jobs qualify for extension retention	The data protection job is set for extended retention.
			Notify only when job contains failed objects	The data protection job contains one or more failed objects.
Data Recovery	Browse and In Place Recover or Browse and Out of Place Recover or Alert Management capability at each associated entity.	Clients Client Groups Agents Backup Sets Instance/Partition	Job Succeeded	A data recovery operation completed successfully.
			Job Succeeded with Errors	A data recovery operation completed with errors.
			Job Skipped	A scheduled data recovery operation ran late, was skipped, or was skipped due to a holiday.
			Job Failed	A data recovery operation failed, failed to start, or the operation was aborted by the system.
			Job Activity	A data recovery operation was killed, resumed, or suspended by a user.
			Job Started	A data recovery operation was started by a user.
			List Media	A user requested a list of media used for the original data protection operation.
Data Verification	Administrative Management or Alert Management capability	Storage Policies Storage Policy Copies	Job Succeeded	A data verification operation completed successfully.
			Job Succeeded with Errors	A data verification operation completed with errors.
			Job Skipped	A scheduled data verification operation ran late, was skipped, or was skipped due to a holiday.
			Job Failed	A data verification operation failed, failed to start, or the operation was aborted by the system.
			Job Activity	A data verification operation was killed, resumed, or suspended by a user.
			Delayed by n Hrs	A data verification operation was in a waiting state for n hours. (n is set by the user at time of configuration.)
Disaster Recovery Backup	Administration Management or Alert Management capability with CommCell association.		Job Succeeded	A disaster recovery backup completed successfully, a backup set was pruned during the operation (default = 5 backup sets).
			Job Succeeded with Errors	A disaster recovery backup operation completed with errors/warnings.
			Job Skipped	A scheduled disaster recovery backup ran late, was skipped, or was skipped due to a holiday.
			Job Failed	A disaster recovery backup failed, failed to start, the operation was aborted by the system, or no storage policy was defined for the operation.
			Job Activity	A disaster recovery backup operation was killed by a user.
			Delayed by n Hrs	A disaster recovery backup operation was in a waiting state for n hours. (n is set by the user at time of configuration.)
Erase Data	Administration Management or Alert Management capability with CommCell association.	Clients Agents Backup Set Subclients	Job Succeeded	An erase data operation completed successfully..
			Job Succeeded with Errors	An erase data operation completed with errors/warnings.
			Job Skipped	A scheduled erase data operation ran late, was skipped, or was skipped due to a holiday.
			Job Failed	An erase data operation failed, failed to start, was killed by a user, was aborted by the system.
			Job Activity	An erase data operation was killed, resumed, or suspended by a user.
Media Erase	Library Management or Alert Management capability with library association	Libraries	Job Succeeded	A media erase operation completed successfully.
			Job Succeeded with Errors	A media erase operation completed with errors/warnings.
			Job Failed	A media erase operation failed, failed to start, or was killed by a user.
			Job Activity	A media erase operation was killed, resumed, or suspended by a user.
Media Inventory	Library Management or Alert Management capability with library association	Libraries	Job Succeeded	An inventory operation completed successfully.
			Job Succeeded with Errors	An inventory operation completed with errors.
			Job Failed	An inventory operation failed, failed to start, or was killed by a user.
Media Refreshing	Administrative Management or Alert Management capability with CommCell association	Storage Policies Storage Policy Copies	Alert every n attempt (Phase failures)	There were n attempts made to resume the data protection operation after a phase failure.
			Alert every n attempt (Network failures)	There were n attempts made to resume the data protection operation after a network failure.
			Delayed by n Hrs	An offline content indexing operation was in a waiting state for

				<i>n</i> hours. (<i>n</i> is set by the user at time of configuration.)
			Job Succeeded	An offline content indexing operation completed successfully.
			Job Succeeded with Errors	An offline content indexing operation completed with errors.
			Job Skipped	An offline content indexing operation ran late, was skipped, or was skipped due to a holiday.
			Job Failed	An offline content indexing operation failed, failed to start, the operation was aborted by the system.
			Job Activity	An offline content indexing operation was killed by a user.
Offline Content Indexing	Administrative Management or Alert Management capability with CommCell association	Storage Policies	Job Succeeded	An offline content indexing operation completed successfully.
			Job Succeeded with Errors	An offline content indexing operation completed with errors.
		Storage Policy Copies	Job Skipped	An offline content indexing operation ran late, was skipped, or was skipped due to a holiday.
			Job Failed	An offline content indexing operation failed, failed to start, the operation was aborted by the system.
			Job Activity	An offline content indexing operation was killed by a user.
		Delayed by <i>n</i> Hrs	An offline content indexing operation was in a waiting state for <i>n</i> hours. (<i>n</i> is set by the user at time of configuration.)	
		Information Management	Administrative Management or Alert Management capability with CommCell association	
	Job Skipped			An information management operation ran late, was skipped, or was skipped due to a holiday.
	Job Succeeded with Errors			An information management operation completed with errors.
	Job Failed			An information management operation failed, failed to start, the operation was aborted by the system.
	Job Activity			An information management operation was killed by a user.
	Delayed by <i>n</i> Hrs			An information management operation was in a waiting state for <i>n</i> hours. (<i>n</i> is set by the user at time of configuration.)
Report	Administration Management capability with CommCell association.		Job Activity	A report operation was killed by a user.
			Job Failed	A report operation failed, failed to start, the operation was aborted by the system, or a report failed to be saved.
			Job Skipped	A report operation ran late, was skipped, or was skipped due to a holiday.
			Job Succeeded	A report operation completed successfully.
			Job Succeeded with Errors	A report operation completed with errors.
SRM Data Collection	Administration Management capability with CommCell association.	Clients	Alert every <i>n</i> attempt (Phase failures)	There were <i>n</i> attempts made to resume the data collection operation after a phase failure.
			Alert every <i>n</i> attempt (Network failures)	There were <i>n</i> attempts made to resume the data collection operation after a network failure.
		Client Groups	Job Activity	A data collection operation was killed by a user.
			Job Failed	A data collection operation failed, failed to start, the operation was aborted by the system.
			Job Skipped	A data collection operation ran late, was skipped, or was skipped due to a holiday.
			Job Succeeded	A data collection operation completed successfully.
			Job Succeeded with Errors	A data collection operation completed with errors.
			No Data Protection	A data collection operation failed to start.

**DataArchiver agents only

MEDIA MANAGEMENT

Alert Type	User Capabilities Needed for Each Alert type	Entities that can be Associated with the Alert	Criteria	Description
Device Status	Library Management or Alert Management capability with CommCell association	Libraries	Drive went Offline	A drive in a library switched offline.
			Library went Offline	A library switched offline.
			Mount Path went Offline	A mount path went offline.
Library Management	Library Management or Alert Management capability with library association.	Libraries	Insufficient Storage	The number of spare media inside the library for a scratch pool and cleaning pool fell below the low water mark defined or there is no spare media inside the library. For a disk library, the free disk space fell below the low water mark or there is insufficient disk space.
			Maintenance Occurred	A drive cleaning operation completed successfully or failed.
			Maintenance Required	The library or drive has exceeded its threshold, a drive requires cleaning, or the mount path has exceeded its fragmentation threshold.

				The percentage threshold at which the mount path is deemed fragmented can be configured in the Media Management Configuration (Service Configuration) window, Mount Path Fragmentation Threshold Percentage option.
			Media Handling Errors	The system found a duplicate barcode/label in the library, or the system detected a media in the wrong library.
			Media Handling Required	A media is not in the library, or a media in a drive needs changing because the system detected wrong or no media in the drive.
			Media Mount and Usage Errors	A media is marked read only, bad or depreciated, or a mount or an unmount error has occurred.
			User Overwrite of Media	The media was overwritten due to an option selected by the user.
			Media Ready in Mail Slot	Media in mail slot is ready to be picked up by the user. NOTES <ul style="list-style-type: none"> This criterion is applicable to a VaultTracker media export (to mail slot) only, which requires a VaultTracker license. For more information, see License Administration in Books Online. It is recommended that the <MEDIA LIST> and <MORE MEDIA Y/N> tokens be added to the notification message when configuring this alert. For more information, see Alert Tokens in Books Online.
			Media Recalled	The media has been retrieved from an export location for a specific operation. For more information, see Recall Media in Books Online.
VaultTracker	Library Management or Alert Management capability with Library association.	Tracking Policies	Job Succeeded	A pending media movement completed successfully.
			Job Succeeded with Errors	A pending media movement completed with errors.
			Job Failed	A pending media movement failed.
			Job Initiated	A pending media movement was created.
			Media Handling Required	A media is moved to a virtual mail slot, or a media needs import.
			Media Picked Up	Media was picked up.
			Media Reached Destination	A media has reached the required destination.
			Media Returned to Source	A media was returned to the source.
			Rolled Back	A media movement was rolled back.

ALERT ADMINISTRATION

MODIFY ALERTS

The options of a configured alert can be modified from the `Alerts` dialog box.

DELETE ALERTS

An alert can be deleted from the `Alerts` dialog box.

DISABLED/ENABLED

An alert can be disabled/enabled from the `Alerts` dialog box.

VIEW CONFIGURED ALERTS

The `Alerts` dialog box displays the configured alert, the alert category and alert type, and the CommCell user that created the alert. The `Alert Summary` provides the alert options in more detail.

TEST ALERTS

An alert can be tested to verify the e-mail server is configured correctly so that all intended recipients of the alert are receiving the notification messages. For more information, see `Test a Configured Alert`.

The `TestSendMail` utility in the Resource Pack can also be used from the command line to test the mail connection for sending alerts.

REPORTS

The CommCell Configuration report provides the option to include information on configured alerts. See CommCell Configuration Report for an overview.

NOTIFICATION TYPES

Alerts can be sent to the intended recipients by the following means:

- E-mail/Pager
- SNMP Trap(s)
- System Event Viewer
- Run Command
- Save to Disk
- RSS Feeds.

E-MAIL/PAGER

Alerts can be sent in the form of an e-mail to selected recipients, providing the recipient has a valid SMTP mail server, a valid e-mail/pager address, and is enabled as a valid CommCell user. E-mail/pager messages can be customized by adding tokens to the body of the e-mail. An e-mail notification can contain up to 100 alerts.

Before sending an email, you must set-up the email server within the CommCell Console. See E-Mail Server Configuration for more information.

SNMP TRAPS

Alerts can be sent by a CommServe, using the SNMP protocol, to other computers in the form of SNMP traps, provided that the SNMP Enabler software is installed on the CommServe computer and SNMP was selected as the alert notification type. See SNMP Enablers for more information.

SYSTEM EVENT VIEWER

Alerts can be sent to the Windows System Event Viewer on the CommServe. Event Viewer alert notifications can be customized by adding alert token arguments to the alert configuration. The tokens will be included in the body of the alert notification message.

RUN COMMAND

Alerts can be sent by configuring a Run Command.

The Run Command can be located on the CommServe or remote machines, but is executed only on the CommServe machine. The command can be configured with arguments; multiple arguments should be separated by spaces, which the system allows.

SAVE TO DISK

Alert notification messages can be sent in the form of a text file to a designated directory either locally or on a network share. This is useful when it is necessary to quickly obtain a listing of the failed items in an operation.

RSS FEEDS

Alert notification messages can be sent in the form of an RSS feed, which can be automatically integrated with your Web Browser.

ALERT TOKENS

An alert token is a parameter that can be added to an alert configuration so that when initiated the desired status information will be appended to the alert notification message. Each alert notification has a different set of tokens available for configuration depending on the criteria selected for the alert. See Default Alert Notification Messages and Tokens for more information.

The following table describes all the alert tokens:

Token	Description
<AGENT TYPE NAME>	The name of the agent.
<ALERT CATEGORY - ALERT TYPE>	The alert category and type.
<ALERT NAME>	The alert display name.
<ALL CLIENT LIST>	A list of all the clients for which updates are selected to be installed.
<BACKUPSET NAME>	The name of the backup set.
<CLIENT LIST>	The name of the clients included in the operation.
<CLIENT NAME>	The name of the client.
<CLIENT RELEASE LIST>	A list of client names and releases.
<CLIENT STATUS LIST>	A list of client names and the status of the update installation operation on each client.

<COMMCELL NAME>	The name of the CommCell.
<COMMENT>	Information regarding the detected condition.
<CONDITION CLEARED Y/N>	Informs a user if the detected condition has cleared.
<CONTENTS>	The list of updates available for download.
<CONTENTS DOWNLOADED>	The list of updates downloaded.
<COPIED DATA SIZE>	The size of data that was copied.
<COPIED MEDIA LIST>	The list of media that was copied.
<COPY NAME>	The copy name.
<CS UPGR TIME>	The last time the CommServe was upgraded.
<CURRENT BACKUP SIZE>	The current size of the backup data.
<DATE OF LAST SUCCESSFUL JOB>	The last date at which a job completed successfully.
<DESCRIPTION>	Information regarding the condition detected.
<DESTINATION LOCATION>	Media destination location.
<DETECTED CRITERIA>	Alert criteria that was detected.
<DISK SPACE INFO>	Disk space information: volume name, volume size, free space.
<DISK SPACE LOW Y/N>	Informs user if the disk space for the software installation directory, CommCell database, Quick Recovery Agent, QSnap, or ContinuousDataReplicator is low.
<DOWNLOAD SIZE (MB)>	The size of the files that have been downloaded.
<DRIVE NAME>	The name of the drive.
<DRIVEPOOL NAME>	The name of the drive pool.
<ELAPSED TIME>	The amount of time used for the operation.
<END TIME>	The time the operation ended.
<ERR CODE>	The error code for the job pending or job failure reason.
<EXPORT LOCATION>	The name of the media export location.
<EXTENDED RET.CANDIDATE Y/N>	Indicates whether the job qualifies for extended retention.
<FAILED ATTEMPT TIME LIST>	The time at which failed login occurred.
<FAILED ATTEMPTS COUNT>	The number of failed login attempts.
<FAILED CLIENT LIST>	A list of clients that failed to install updates.
<FAILED COUNT>	The number of failed objects.
<FAILED OBJECTS>	A list of failed objects in an attachment.
<FAILURE REASON>	A reason why there was a failure.
<FILES DOWNLOADED>	A list of the downloaded files.
<FORCE DECONFIG Y/N>	Informs a user if a CommCell object was de-configured.
<FREE SPACE>	Free space on related volume.
<GUI CLIENT NAME>	Name of the client displayed in the user interface.
<INITIATOR>	VaultTracker policy name that initiated the VaultTracker action.
<INSTANCE NAME>	The name of the instance.
<JOB ID>	The Job ID assigned by the Job Manager for the job.
<JOBS RUNNING CLIENT LIST>	A list of client names that have jobs running at the time of update installation.
<JOBS TOBE COPIED>	The number of jobs to be copied.
<LEVEL>	The backup level. Note that for a File Archiver /DataAgent the status of the Index will be displayed for this token.
<LIBRARY NAME>	The name of the library.
<LICENSE EXPIRED>	The name of the license that will expire.
<LOW CACHE CLIENT LIST>	A list of client names that have low cache at the time of update installation.
<MAILBOX NAME>	The name of the mailbox.
<MESSAGE COUNT>	The number of messages in the mailbox.
<MEDIA LABEL>	The label/barcode of the media.
<MEDIA FAILED>	The media that failed to be erased.
<MEDIA LIST>	A list of media used during the operation.
<MEDIA LOCATION LIST>	A list of media and their locations.
<MEDIA REQUIRE LIST>	The media required for a data recovery operation.
<MEDIA SPACE LEFT>	For disk media, the space remaining on a disk. For tape media, the remaining spare media in a scratch pool.
<MEDIA SUCCEEDED>	The media that was successfully erased.
<MEDIA TOBE COPIED COUNT>	The number of media to be copied.
<MEDIAAGENT NAME>	The name of the MediaAgent.
<MORE MEDIA Y/N>	A yes/no token, which specifies whether more media is to be exported.
<MOUNTPATH NAME>	The name of the mount path.
<NO. OF DAYS LEFT FOR LICENSE EXPIRY>	The number of days remaining until license expires.
<NO SUCCESSFUL JOB SINCE>	The number of days since a data protection operation did not complete successfully.
<NUMBER OF ITEMS>	The number of items restored/recovered during the operation.
<OLDEST JOB ENDDATE>	The end date of the oldest job to be copied.
<OPERATION TYPE>	The name of the operation.
<OTHER LIBRARY>	The library to which the media belongs.
<OWNER EMAIL>	The email address of the user who created the alert.
<OWNER NAME>	The user who created the alert.
<PERCENTAGE CHANGE>	The percentage change of data size from previous job to current job.

<PREVIOUS JOB ID>	The previous job identification number.								
<PREVIOUS BACKUP SIZE>	The previous backup job data size.								
<PROPERTY MODIFIED Y/N>	A yes/no token, which specifies whether a property has been modified.								
<PROTECTED COUNT>	The number of protected objects.								
<PROTECTED OBJECTS>	A list of protected objects and file sizes in an attachment. File sizes are displayed in bytes.								
<PRUNED JOB COUNT>	The number of jobs that have aged.								
<PRUNED MEDIA BARCODE LIST>	The barcode list of aged media.								
<RETAIN UNTIL>	The predicted ending retention date of the job.								
<RD JOB Y/N>	A yes/no token, which specifies whether a job was initiated to a Recovery Director /DataAgent.								
<RECOVERED COUNT>	The number of objects recovered.								
<RECOVERED OBJECTS>	A list of recovered objects in an attachment.								
<REPSET NAME>	The name of the replication set.								
<RESOURCE WAIT TIME>	Time elapsed while a job is waiting for a resource.								
<RESTORE USER NAME>	The user that initiated the restore operation from the Search Console.								
<SCHEDULE NAME>	The name of the schedule.								
<SCHEDULE TIME>	The time the operation was scheduled.								
<SERVER RELEASE>	CommCell release number.								
<SIZE>	The size of the files restored during the operation.								
<SIZE OF DATA TO BE COPIED>	The size of the data to be copied.								
<SKIPPED COUNT>	The number of objects that were skipped during a data recovery operation.								
<SKIPPED OBJECTS>	A list of skipped objects in an attachment.								
<SNAPSHOT VOLUME UNIT>	The name of the snapshot volume unit.								
<SOURCE LOCATION>	The name of the source location.								
<SP LIST>	A list of the storage policies used in the operation.								
<SP NAME>	The name of the storage policy.								
<SPAREPOOL/MOUNTPATH NAME>	The spare media pool or mount path name.								
<START TIME>	The time the operation started.								
<STATUS>	The status of the operation.								
<STORAGE POLICIES USED>	The name of the storage policies associated with the data protection operation.								
<SUBCLIENT NAME>	The name of the subclient.								
<SUBJECT BEGIN>	The beginning of the notification.								
<SUBJECT END>	The end of the notification.								
<SUCCESSFUL CLIENT LIST>	A list of clients that were updated successfully.								
<THRESHOLD>	The threshold value for the library, drive and media.								
<TIME>	The time (as per the time zone of the CommServe) the condition was detected.								
<TIME OF LAST SUCCESSFUL JOB>	The last time at which a job completed successfully.								
<TRANSIT LOCATION>	The name of the transient location.								
<UNKNOWN CLIENT LIST>	A list of clients whose status was unable to be determined after the installation of updates.								
<UNREACHABLE CLIENT LIST>	A list of clients that are unreachable.								
<UP-TO-DATE CLIENT LIST>	A list of clients that already have all of the updates required.								
<USER NAME>	The CommCell user that initiated the operation.								
<USER NAME LIST>	A list of user names entered for the failed login attempts.								
<UTC_TIME>	The time the condition was detected as displayed in UTC time.								
<VOLUME NAME>	The name of the volume.								
<WORKFLOW>	The name of the Recovery Director workflow.								
<XFER BYTES>	Data transferred in bytes.								
<XFER GB PER HOUR>	Data transferred in gigabytes per hour.								
<XFER SECS>	Number of seconds for the data transfer to occur.								
<XFER SIZE>	Amount of data transferred automatically displayed in the size unit respective of the size amount. Refer to the following:								
	<table border="1"> <thead> <tr> <th>If amount of data transferred is equal to:</th> <th>Then, amount will be automatically displayed as:</th> </tr> </thead> <tbody> <tr> <td>Less than 1 MB</td> <td>Bytes</td> </tr> <tr> <td>Greater than 1 MB, Less than 1 GB</td> <td>Megabytes</td> </tr> <tr> <td>Greater than 1 GB</td> <td>Gigabytes</td> </tr> </tbody> </table>	If amount of data transferred is equal to:	Then, amount will be automatically displayed as:	Less than 1 MB	Bytes	Greater than 1 MB, Less than 1 GB	Megabytes	Greater than 1 GB	Gigabytes
If amount of data transferred is equal to:	Then, amount will be automatically displayed as:								
Less than 1 MB	Bytes								
Greater than 1 MB, Less than 1 GB	Megabytes								
Greater than 1 GB	Gigabytes								
<AUTOMATED CONTENT CLASSIFICATION_POLICY_NAME>	The name of the Automated Content Classification Policy.								
<LEGAL HOLD PHASE SELECTED Y/N>	A yes/no token, which specifies whether Legal Hold phase is selected.								
<NO.OF ITEMS FAILED IN LEGAL HOLD PHASE>	Number of items failed in Legal Hold phase.								
<NO.OF ITEMS FAILED IN ERM CONNECTOR PHASE>	Number of items failed in ERM Connector phase.								
<NO.OF ITEMS FAILED IN RESTORE TO REVIEW SET PHASE>	Number of items failed in Restore to Review Set phase.								
<NO.OF ITEMS FAILED TO RESTORE>	Number of items failed to restore.								
<NO.OF ITEMS FAILED TO SEARCH>	Number of items failed to search.								
<NO.OF ITEMS FAILED TO TAG>	Number of items failed to tag.								
<NO.OF ITEMS RESTORED SUCCESSFULLY>	Number of items restored successfully.								

<NO.OF ITEMS SEARCHED SUCCESSFULLY>	Number of items searched successfully.
<NO.OF ITEMS SELECTED FOR LEGAL HOLD>	Number of items selected for Legal Hold.
<NO.OF ITEMS SELECTED FOR ERM CONNECTOR>	Number of items selected for ERM Connector
<NO.OF ITEMS SELECTED FOR TAGGING>	Number of items selected for Tagging.
<NO.OF ITEMS SELECTED TO RESTORE TO REVIEW SET>	Number of items selected for restoring to review set.
<NO.OF ITEMS SELECTED TO RESTORE>	Number of items selected for restore.
<NO.OF ITEMS SELECTED TO SEARCH>	Number of items selected for search.
<NO.OF ITEMS SUCCEEDED IN LEGAL HOLD PHASE>	Number of items succeeded in Legal Hold phase.
<NO.OF ITEMS SUCCEEDED IN ERM CONNECTOR PHASE>	Number of items succeeded in ERM Connector phase.
<NO.OF ITEMS SUCCEEDED IN RESTORE TO REVIEW SET PHASE>	Number of items succeeded in restore to review set phase.
<NO.OF ITEMS TAGGED SUCCESSFULLY>	Number of items tagged successfully.
<PHASES_IN_JOB>	List of phases for the job.
<ERM CONNECTOR PHASE SELECTED Y/N>	A yes/no token, which specifies whether ERM Connector phase is selected.
<RESTORE PHASE SELECTED Y/N>	A yes/no token, which specifies whether restore phase is selected.
<RESTORE TO REVIEW SET PHASE SELECTED Y/N>	A yes/no token, which specifies whether restore to review set phase is selected.
<SEARCH PHASE SELECTED Y/N>	A yes/no token, which specifies whether search phase is selected.
<STATUS OF LEGAL HOLD PHASE>	Status of the Legal Hold phase.
<STATUS OF ERM CONNECTOR PHASE>	Status of the ERM Connector phase.
<STATUS OF RESTORE PHASE>	Status of the restore phase.
<STATUS OF RESTORE TO REVIEW SET PHASE>	Status of the restore to review set phase.
<STATUS OF SEARCH PHASE>	Status of the search phase.
<STATUS OF TAGGING PHASE>	Status of the tagging phase.
<TAGGING PHASE SELECTED Y/N>	A yes/no token, which specifies whether tagging phase is selected.

[Back To Top](#)

Alerts and Monitoring - How To

[Topics](#) | [How To](#) | [Example](#) | [Support](#) | [Related Topics](#)

[Configure Alerts](#)

[Configure Job-Based Alerts](#)

[Modify Alerts](#)

[Modify Job-Based Alerts](#)

[Delete Alerts](#)

[Delete Job-Based Alerts](#)

[Test a Configured Alert](#)

[Configure SNMP Traps](#)

[Add Additional Computers to Receive SNMP Traps](#)

CONFIGURE ALERTS

In order for alerts to reach their intended recipients, alerts must first be configured. The following steps need to be taken in order to configure alerts:

- Specify an E-Mail Server
- Select an Alert Category and Alert Type
- Associate Entities with the Alert
- Select the Threshold and Notification Criteria
- Select the Locale
- Select the Notification Type
- Select the CommCell Users and/or CommCell User Groups to Receive the Alert

Before You Begin

- Verify that you have specified a valid SMTP mail server, a valid e-mail or pager address, and the recipient is enabled as a CommCell user with the correct capabilities needed for the alert type. Additionally, make sure that the sender's address specified in the **E-Mail and IIS Server Settings** dialog box is valid.

Required Capability: See Capabilities and Permitted Actions

Procedure

Specify an E-Mail Server

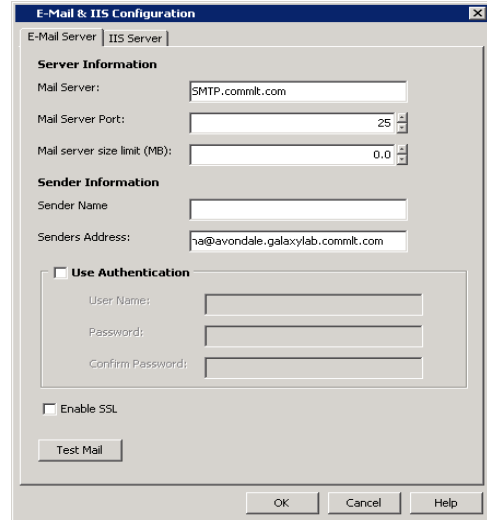
1. From the CommCell Browser, right-click the **CommCell** icon, click **Control Panel**, and then click **E-Mail and IIS Configuration**. From the **E-Mail and IIS Configuration** dialog box, select the E-Mail Server tab, and specify a valid Mail Server to be used by alerts, scheduled reports and log files. The Mail Server must support SMTP messages.

Select the port number in the **Mail Server Port** box. The default Mail Server port number is 25.

Specify the **Mail Server Size Limit** per e-mail.

Specify a valid e-mail address in the **Senders Address** box.

Click **OK**.



Select an Alert Category and Alert Type

2. From the CommCell Browser, right-click the **CommCell** icon, click **Control Panel**, and then click **Alerts**. From the **Alerts** window, click **Add**.

In the General Information step of the Alert Wizard dialog box:

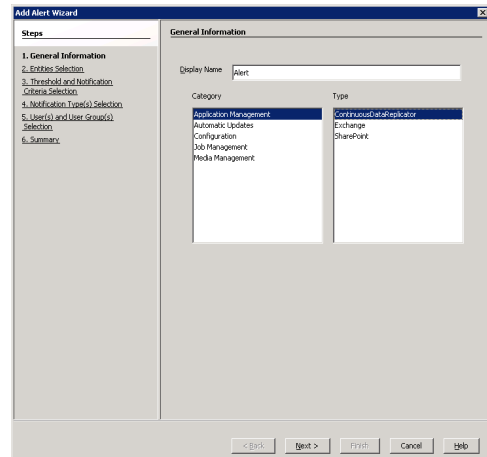
Enter a name for the alert in the **Display Name** box.

Select a category and alert type. See Available Alerts and Alert Descriptions for a complete list of available alerts.

Click **Next**.

NOTES

Depending on what options you select, your screen may look different than the example shown.



Associate Entities with the Alert

3. Associate entities with the alert (if applicable).

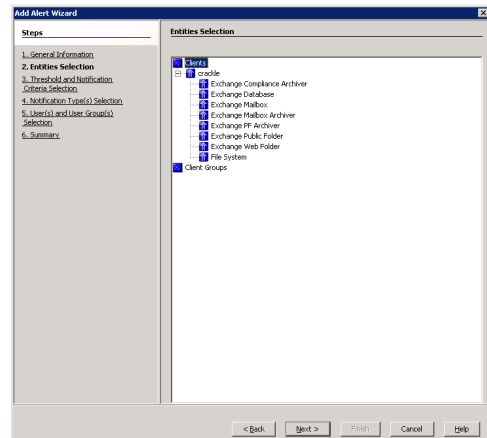
NOTES

- Alerts must be associated with an entity based on the alert type. Once conditions with the entity meet a pre-selected criteria, an alert will be generated based on those conditions. Entities differ according to the type of alert selected. See Available Alerts and Alert Descriptions for a list of entities available for each alert type.
- A user must have the correct associations and capabilities to associate entities with alerts. See the capabilities column in Available Alerts and Alert Descriptions for more information.

Click **Next**.

NOTES

Depending on what options you select, your screen may look different than the example shown.



Select the Threshold and Notification Criteria

- Select the conditions that will initiate the alert in the Alert Wizard's Threshold and Notification Criteria Selection dialog box. Then enable or disable the **Send Individual Notification for This Alert** option. (When enabled, recipients will only receive one notification for this alert.)

Click **Next**.

NOTES

- The threshold and notification criteria determine when and at which frequency an alert is generated.
- An alert is sent:
 - Once conditions within the entity have met the selected criteria for the alert. For example, if the criteria of *Job Skipped* is selected for a Data Protection alert, then an alert will be sent if a data protection operation is skipped
 - Either:
 - Repeat if the condition persists for certain length of time. (Available for the Device Status and Library Management alerts.)
 - When the condition clears. (Available for the Device Status and Library Management alerts only.)
 - After a specified number of attempts during a phase or network failure. (Available for the Auxiliary Copy and Data Protection alerts.)
- If the alert notification was configured to send an escalated alert. If this option is available, select the time at which the escalated alert notification should be sent, the frequency and whether notification should be sent when the condition clears.
- If configuring a Job Management Data Protection alert, you can select from the following additional notification options:

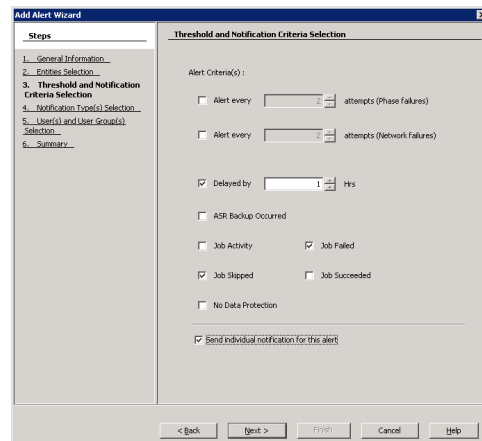
Notify only when jobs qualify for extended retention

If selected, when a data protection job meets the thresholds of the configured alert criteria, users will only be notified of those jobs that are set for extended retention.

Notify only when job contains failed objects

If selected, when a data protection job meets the thresholds of the configured alert criteria, users will only be notified of those jobs that contain failed objects.

- Depending on what options you select, your screen may look different than the example shown.

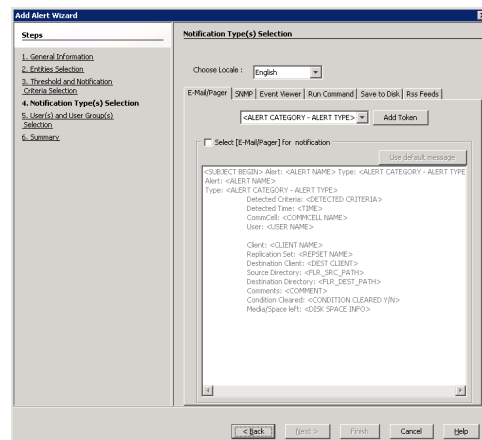


Select the Locale

- Select the language (locale) in which the alert is to be sent to its intended recipient in the Alert Wizard's Notification Type(s) Selection dialog box.

NOTES

- The locale can be different than the locale of the CommCell Console. A warning message will prompt you to confirm the change of the locale.
- Depending on what options you select, your screen may look different than the example shown.



Select the Notification Type

- Select the way in which the alert is to be sent to its intended recipient. E-mail/pager messages can be customized by adding tokens to the body of the e-mail. The following notification types are available:

- E-Mail/Pager

If you wish to send the alert by e-mail or pager:

Click the **E-Mail/Pager** tab.

Click the **Select [E-Mail/Pager] for notification** checkbox.

If you wish to customize the e-mail or pager notification, click a token from the list and then click **Add Token**.

Click **Next**.

NOTES

Depending on what options you select, your screen may look different than the example shown.

- **SNMP**

If you wish to send the alert by a SNMP trap:

Click the **SNMP** tab.

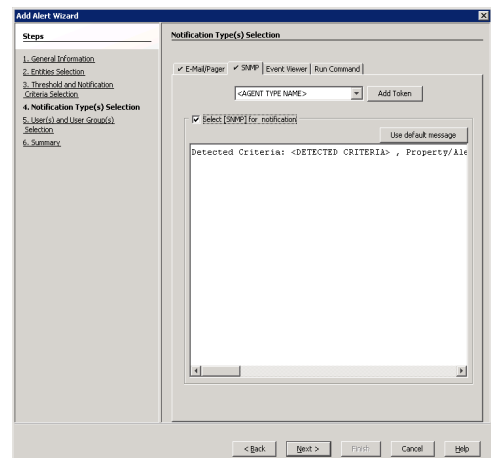
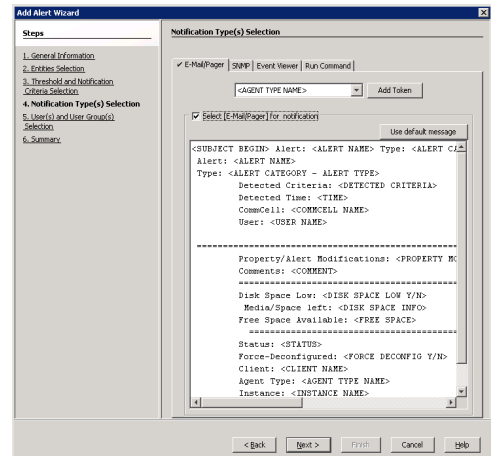
Click the **Select [SNMP] for notification** checkbox.

If you wish to customize the SNMP notification, click a token from the list and then click **Add Token**.

Click **Next**.

NOTES

Depending on what options you select, your screen may look different than the example shown.



- **Event Viewer**

If you wish to send the alert to the System Event Viewer:

Click the **Event Viewer** tab.

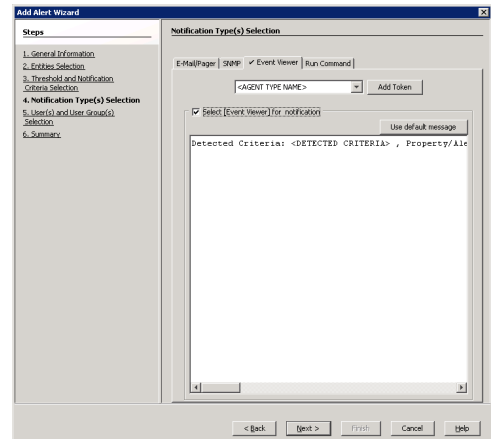
Click the **Select [Event Viewer] for notification** checkbox.

If you wish to customize the Event Viewer message, click a token from the list and then click **Add Token**.

Click **Next**.

NOTES

Depending on what options you select, your screen may look different than the example shown.



- **Run Command**

If you wish to send the alert by executing a command script:

Click the **Run Command** tab.

Click the **Select [Run Command] for notification** checkbox.

Click **Use Local Drive** or **Use Network Share**. Use the **Change** button to change the account information to access the network share.

Enter the location of the Command Processor executable file in the **Command Script Location** box, or click **Browse** to browse to the location, e.g., C:\WINDOWS\system32\cmd.exe.

Enter the following in the **Arguments** field prior to adding any arguments: /c C:\Tmp\runCommandTest.bat. Where the \C signifies that the Command Processor must carry out the given command in the following string and then terminate. Note that C:\Tmp\runCommandTest.bat is the location of the batch file you wish to run

when the alert criteria threshold is met.

Add the arguments by clicking on the **Browse** button. Manually add quotation marks around the tokens, e.g., "\$<DETECTED CRITERIA>\$"; this resolves any white space issues. The Arguments filed will resemble the following format:
/C C:\Tmp\runCommandTest.bat "\$<ALERT NAME>\$" "\$<DETECTED CRITERIA>\$"

The following is the content of the batch file used in this example:

```
REM runCommandTest.bat
@echo %date% %time% >> c:\tmp\alert1.log
echo %~1>>c:\tmp\alert1.log
echo %~2>>c:\tmp\alert1.log
echo %~3>>c:\tmp\alert1.log
echo %~4>>c:\tmp\alert1.log
echo %~5>>c:\tmp\alert1.log
echo %~6>>c:\tmp\alert1.log
echo %~7>>c:\tmp\alert1.log
echo %~8>>c:\tmp\alert1.log
echo %~9>>c:\tmp\alert1.log
REM End Batch File
```

Note the '~' character between the '%' character and the parameter position number above; this signifies the command processor to strip off the quotation characters at the beginning and end of the parameter. If this is not done, the quotation marks remain as part of the parameter, which may be useful if the batch file is calling another program or batch file.

Click **Next**.

NOTES

- The Run Command can be located on the CommServe or remote machines, but is executed only on the CommServe machine.
- Depending on what options you select, your screen may look different than the example shown.

- Save to Disk

If you wish to send the alert to a local directory or network share:

Click the **Save to Disk** tab.

Click the **Select [Save to Disk] for notification** checkbox.

Click **Use Local Drive** or **Use Network Share** and specify the **Location**. Use the **Change** button to change the account information to access the network share.

Click **Next**.

NOTES

Depending on what options you select, your screen may look different than the example shown.

- RSS Feeds

If you wish to send the alert to an RSS feed:

Click the **Save to Disk** tab.

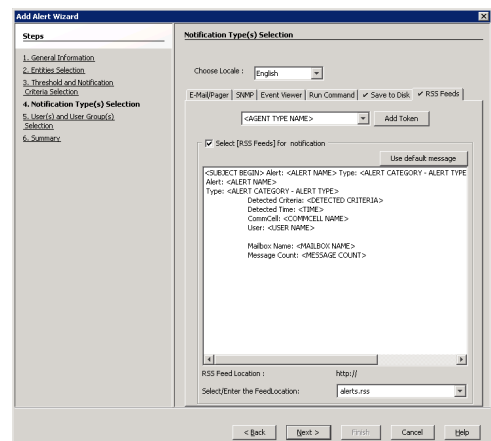
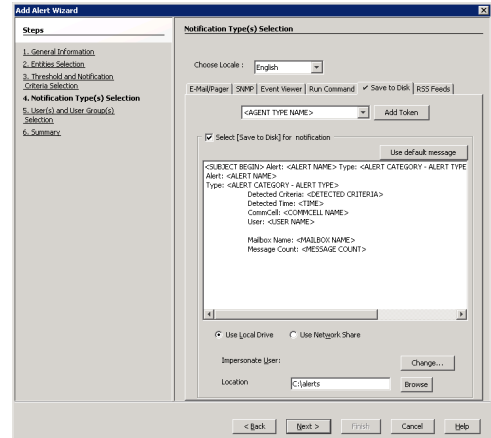
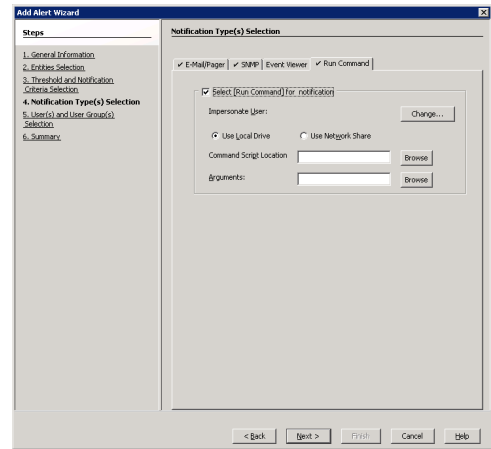
Click the **Select [RSS Feeds] for notification** checkbox.

Select or Enter the **Feed Location**.

Click **Next**.

NOTES

Depending on what options you select, your screen may look different than the example shown.



Select the CommCell Users and/or CommCell User Groups to Receive the Alert

7. Select the CommCell users and/or CommCell user groups that will receive the alert; or enter the e-mail address(es) of the recipient(s) in the **Email to Recipient** field; these recipients can reside within an external domain. See User Administration and

Security for more information.

Click **Next**.

NOTES

- An alert can be configured to send e-mail notifications to user groups created from within the CommCell Console as well as external domain user groups. However, individual external domain users will not receive the alert notification e-mail if they have not previously logged on to the CommCell Console. Users (from the user groups created from within the CommCell Console) will receive the alert e-mail notification regardless of their login status.
- This step is not necessary for alerts sent as SNMP traps or to the Windows System Event Viewer.
- Depending on what options you select, your screen may look different than the example shown.

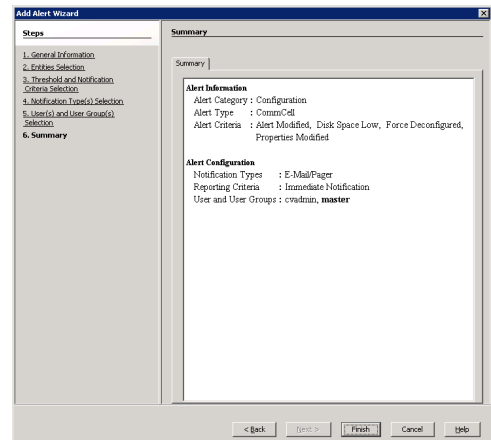
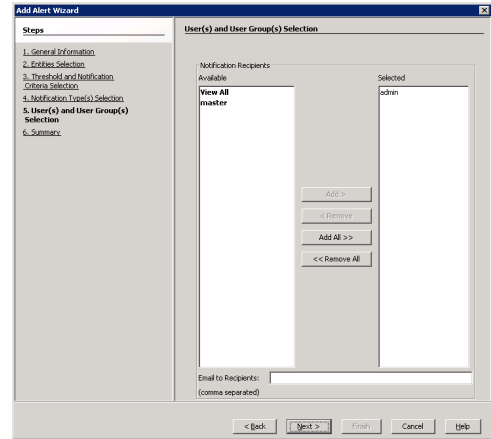
8. The Summary step displays a summary of the options that you have selected for the alert.

Click **Finish**.

The alert is now configured and displayed in the **Alerts** window.

NOTES

- If the e-mail server and sender's address are not configured correctly, the alerts will not be sent to the intended e-mail and pager recipients. If you want to test that the alert is configured correctly, right-click on the alert in this window, and click **Test**. A test alert will be sent to the configured recipients; this alert will not contain any data.
- Depending on what options you select, your screen may look different than the example shown.



CONFIGURE JOB-BASED ALERTS

In order for alerts to reach their intended recipients, alerts must first be configured. The following steps need to be taken in order to configure alerts:

- Select an Alert Category and Alert Type
- Associate Entities with the Alert
- Select the Threshold and Notification Criteria
- Select the Locale
- Select the Notification Type
- Select the CommCell Users and/or CommCell User Groups to Receive the Alert

Before You Begin

- Verify that you have specified a valid SMTP mail server, a valid e-mail or pager address, and the recipient is enabled as a CommCell user with the correct capabilities needed for the alert type. Additionally, make sure that the sender's address specified in the **Email and IIS Server Settings** dialog box is valid.

Required Capability: See Capabilities and Permitted Actions

Procedure

Getting Started

1. You can create job-based alerts while configuring an immediate job, scheduled job, configuring a schedule policy, or for a running job. While in the process of these configurations you will encounter an opportunity to create the alert, such as a tab or button. For a running job, right click on the job in the Job Controller window to initiate the popup menu.

Click **Add Alert**.

NOTES

Depending on what options you select or what job you are creating, your screen may look different than the example shown.



Select an Alert Category and Alert Type

2. From the **Alerts** window, click **Add**.

In the General Information step of the Alert Wizard dialog box:

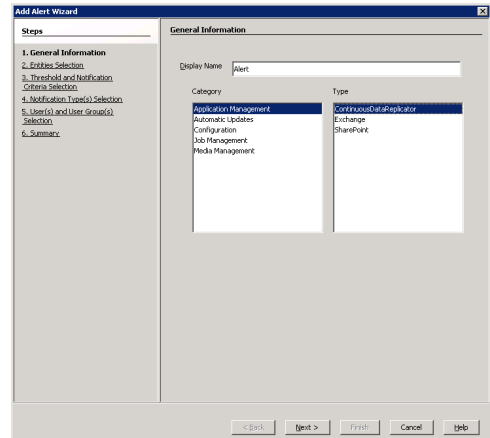
Enter a name for the alert in the **Display Name** box.

Select a category and alert type. See Available Alerts and Alert Descriptions for a complete list of available alerts.

Click **Next**.

NOTES

Depending on what options you select, your screen may look different than the example shown.



Associate Entities with the Alert

3. Associate entities with the alert (if applicable).

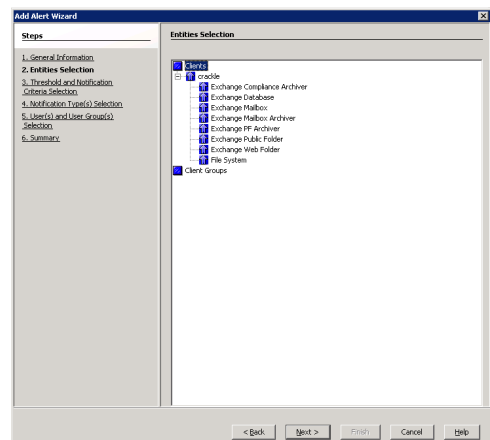
NOTES

- Alerts must be associated with an entity based on the alert type. Once conditions with the entity meet a pre-selected criteria, an alert will be generated based on those conditions. Entities differ according to the type of alert selected. See Available Alerts and Alert Descriptions for a list of entities available for each alert type.
- A user must have the correct associations and capabilities to associate entities with alerts. See the capabilities column in Available Alerts and Alert Descriptions for more information.

Click **Next**.

NOTES

Depending on what options you select, your screen may look different than the example shown.



Select the Threshold and Notification Criteria

4. Select the conditions that will initiate the alert in the Alert Wizard's Threshold and Notification Criteria Selection dialog box. Then enable or disable the **Send Individual Notification for This Alert** option. (When enabled, recipients will only receive one notification for this alert.)

Click **Next**.

NOTES

- The threshold and notification criteria determine when and at which frequency an alert is generated.
- An alert is sent:
 - Once conditions within the entity have met the selected criteria for the alert. For example, if the criteria of Job Skipped is selected for a Data Protection alert, then an alert will be sent if a data protection operation is skipped
 - Either:
 - Repeat if the condition persists for certain length of time. (Available for the Device Status and Library Management alerts only.)
 - When the condition clears. (Available for the Device Status and Library Management alerts only.)
 - After a specified number of attempts during a phase or network failure. (Available for the Auxiliary Copy and Data Protection alerts only.)
- If the alert notification was configured to send an escalated alert. If this option is available, select the time at which the escalated alert notification should be sent, the frequency and whether notification should be sent when the condition clears.
- If configuring a Job Management Data Protection alert, you can select from the following additional notification options:

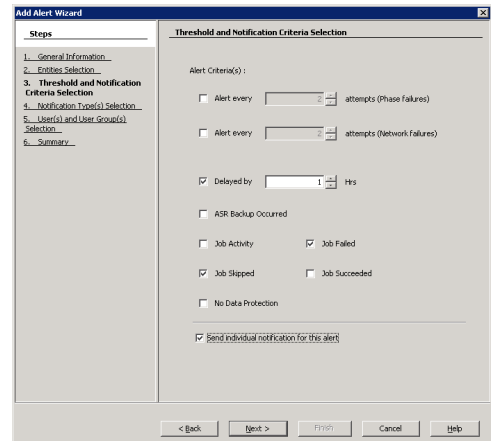
Notify only when jobs qualify for extended retention

If selected, when a data protection job meets the thresholds of the configured alert criteria, users will only be notified of those jobs that are set for extended retention.

Notify only when job contains failed objects

If selected, when a data protection job meets the thresholds of the configured alert criteria, users will only be notified of those jobs that contain failed objects.

- Depending on what options you select, your screen may look different than the example shown.

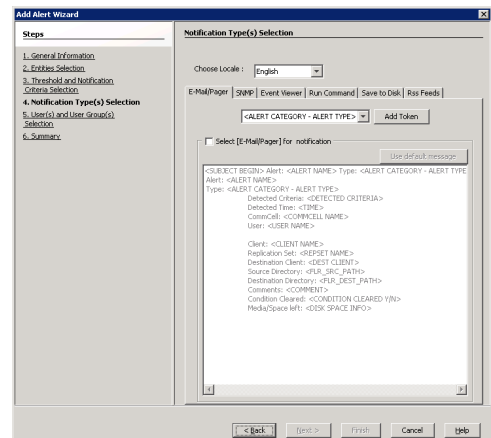


Select the Locale

5. Select the language (locale) in which the alert is to be sent to its intended recipient in the Alert Wizard's Notification Type(s) Selection dialog box.

NOTES

- The locale can be different than the locale of the CommCell Console. A warning message will prompt you to confirm the change of the locale.
- Depending on what options you select, your screen may look different than the example shown.



Select the Notification Type

6. Select the way in which the alert is to be sent to its intended recipient. E-mail/pager messages can be customized by adding tokens to the body of the e-mail. The following notification types are available:

- E-Mail/Pager

If you wish to send the alert by e-mail or pager:

Click the **E-Mail/Pager** tab.

Click the **Select [E-Mail/Pager] for notification** checkbox.

If you wish to customize the e-mail or pager notification, click a token from the list and then click **Add Token**.

Click **Next**.

NOTES

Depending on what options you select, your screen may look different than the example shown.

- **SNMP**

If you wish to send the alert by a SNMP trap:

Click the **SNMP** tab.

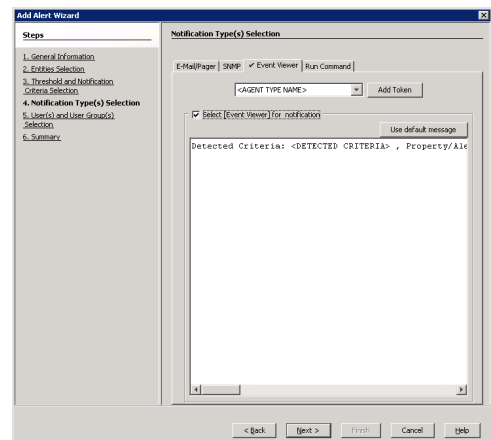
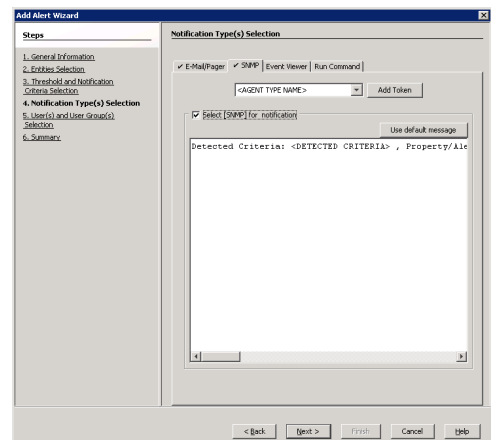
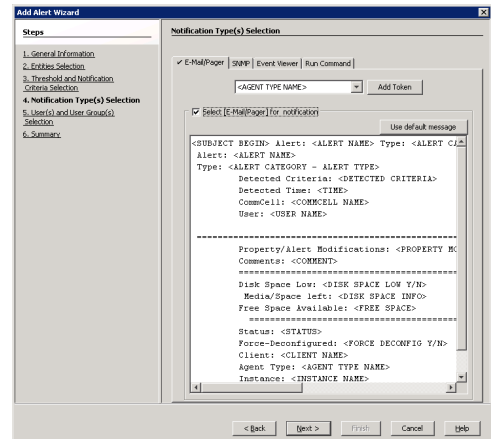
Click the **Select [SNMP] for notification** checkbox.

If you wish to customize the SNMP notification, click a token from the list and then click **Add Token**.

Click **Next**.

NOTES

Depending on what options you select, your screen may look different than the example shown.



- **Event Viewer**

If you wish to send the alert to the System Event Viewer:

Click the **Event Viewer** tab.

Click the **Select [Event Viewer] for notification** checkbox.

If you wish to customize the Event Viewer message, click a token from the list and then click **Add Token**.

Click **Next**.

NOTES

Depending on what options you select, your screen may look different than the example shown.

- **Run Command**

If you wish to send the alert by executing a command script:

Click the **Run Command** tab.

Click the **Select [Run Command] for notification** checkbox.

Click **Use Local Drive** or **Use Network Share**. Use the **Change** button to change the account information to access the network share.

Enter the location of the Command Processor executable file in the **Command Script Location** box, or click **Browse** to browse to the location, e.g., C:\WINDOWS\system32\cmd.exe.

Enter the following in the **Arguments** field prior to adding any arguments: /C C:\Tmp\runCommandTest.bat. Where the \C signifies that the Command Processor must carry out the given command in the following string and then terminate. Note that C:\Tmp\runCommandTest.bat is the location of the batch file you wish to run when the alert criteria threshold is met.

Add the arguments by clicking on the **Browse** button. Manually add quotation marks around the tokens, e.g., "\$<DETECTED CRITERIA>\$"; this resolves any white space issues. The Arguments field will resemble the following format:

C:\Tmp\runCommandTest.bat "\$<ALERT NAME>\$" "\$<DETECTED CRITERIA>\$"

The following is the content of the batch file used in this example:

```
REM runCommandTest.bat
@echo %date% %time% >> c:\tmp\alert1.log
echo %~1>>c:\tmp\alert1.log
echo %~2>>c:\tmp\alert1.log
echo %3>>c:\tmp\alert1.log
echo %4>>c:\tmp\alert1.log
echo %5>>c:\tmp\alert1.log
echo %6>>c:\tmp\alert1.log
echo %7>>c:\tmp\alert1.log
echo %8>>c:\tmp\alert1.log
echo %9>>c:\tmp\alert1.log
REM End Batch File
```

Note the '~' character between the '%' character and the parameter position number above; this signifies the command processor to strip off the quotation characters at the beginning and end of the parameter. If this is not done, the quotation marks remain as part of the parameter, which may be useful if the batch file is calling another program or batch file.

Click **Next**.

NOTES

- The Run Command can be located on the CommServe or remote machines, but is executed only on the CommServe machine.
- Depending on what options you select, your screen may look different than the example shown.
- Save to Disk

If you wish to send the alert to a local directory or network share:

Click the **Save to Disk** tab.

Click the **Select [Save to Disk] for notification** checkbox.

Click **Use Local Drive** or **Use Network Share** and specify the **Location**. Use the **Change** button to change the account information to access the network share.

Click **Next**.

NOTES

Depending on what options you select, your screen may look different than the example shown.

- RSS Feeds

If you wish to send the alert to an RSS feed:

Click the **Save to Disk** tab.

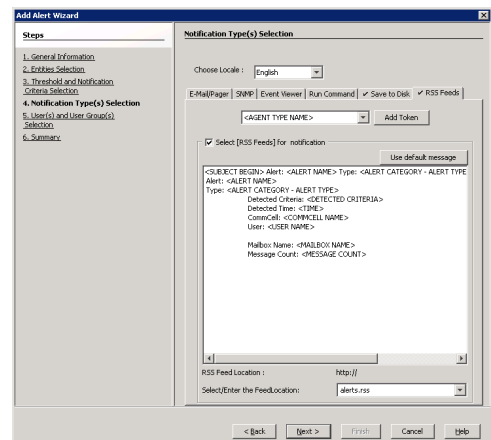
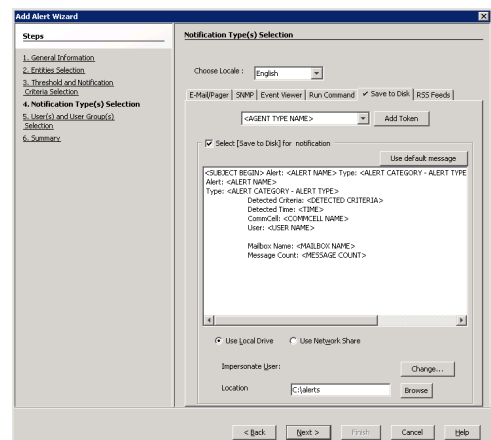
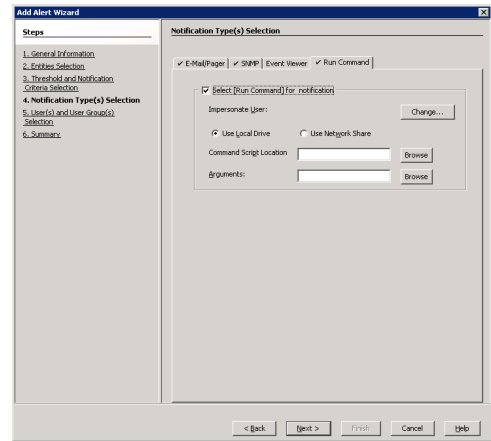
Click the **Select [RSS Feeds] for notification** checkbox.

Select or Enter the **Feed Location**.

Click **Next**.

NOTES

Depending on what options you select, your screen may look different than the example shown.



Select the CommCell Users and/or CommCell User Groups to Receive the Alert

7. Select the CommCell users and/or CommCell user groups that will receive the alert; or enter the e-mail address(es) of the recipient(s) in the **Email to Recipient** field; these recipients can reside within an external domain. See User Administration and Security for more information.

Click **Next**.

NOTES

- An alert can be configured to send e-mail notifications to user groups created from within the CommCell Console as well as external domain user groups. However, individual external domain users will not receive the alert notification e-mail if they have not previously logged on to the CommCell Console. Users (from the user groups created from within the CommCell Console) will receive the alert e-mail notification regardless of their login status.
- This step is not necessary for alerts sent as SNMP traps or to the Windows System Event Viewer.
- Depending on what options you select, your screen may look different than the example shown.

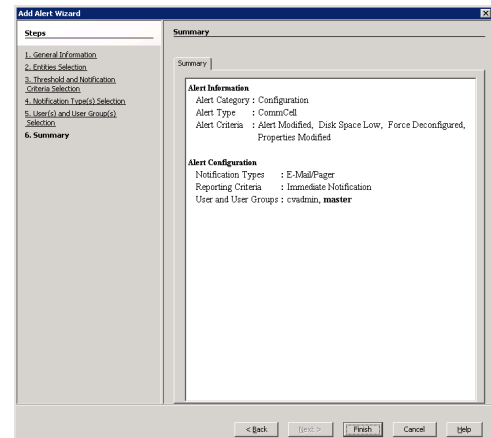
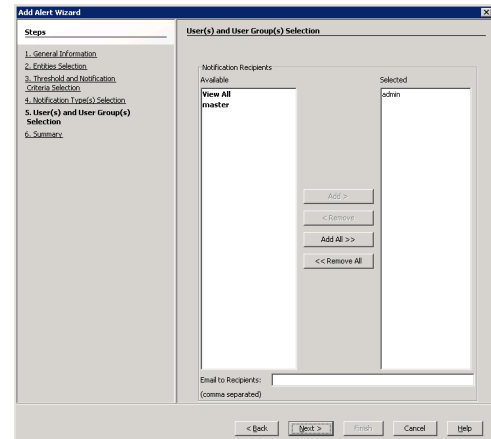
8. The Summary step displays a summary of the options that you have selected for the alert.

Click **Finish**.

The alert is now configured and displayed in the **Alerts** window.

NOTES

- If the e-mail server and sender's address are not configured correctly, the alerts will not be sent to the intended e-mail and pager recipients. If you want to test that the alert is configured correctly, right-click on the alert in this window, and click **Test**. A test alert will be sent to the configured recipients; this alert will not contain any data.
- Depending on what options you select, your screen may look different than the example shown.

**MODIFY ALERTS**

Required Capability: See Capabilities and Permitted Actions

- To send alerts to CommCell users, a user must belong to one of the following user groups to assign a user to receive alerts:
 - The Master user group.
 - A user group that has the Alert Management Capability and that is associated with the object for which you want to configure the alert. Users can set alerts for themselves without an association or capability.

▶ To modify an alert:

1. From the CommCell Browser, right-click the **CommCell** icon, click **Control Panel**, and then click **Alerts**.
2. From the Alerts window, select an alert and then click **Modify**.
3. Follow the steps from the **Modify Alert Wizard**.
4. Click **Finish** from the **Summary** window.

MODIFY JOB-BASED ALERTS

Required Capability: See Capabilities and Permitted Actions

▶ To modify a job-based alert for a running job:

1. From the Job Controller window, right-click on the job associated with the alert you wish to modify.
2. Select **Modify Alert** from the popup menu. This will launch the **Modify Alert Wizard**.
3. Click **Finish** to save your changes.

▶ To modify a job-based alert for a scheduled job:

1. From the CommCell Browser, right-click the CommServe, and select **All Tasks** and **Schedules**.
2. From the Scheduled Jobs window, highlight the job associated with the alert you wish to delete, and click **Modify Alert**. This will launch the **Modify Alert**

Wizard.

3. Click **Finish** to save your changes.
-

DELETE ALERTS

Required Capability: See Capabilities and Permitted Actions

▶ To delete an alert:

1. From the CommCell Browser, right-click the **CommCell** icon, click **Control Panel**, and then click **Alerts**.
2. From the Alerts window, select the alert and then click **Delete**.
3. Click **Yes** from the confirmation window.

The alert is now deleted.

DELETE JOB-BASED ALERTS

Required Capability: See Capabilities and Permitted Actions

▶ To delete a job-based alert for a running job:

1. From the Job Controller window, right-click on the job associated with the alert you wish to delete.
2. Select **Delete Alert** from the popup menu.
3. Click **Yes** from the confirmation window. The job-based alert is now deleted.

▶ To delete a job-based alert for a scheduled job:

1. From the CommCell Browser, right-click the CommServe, and select **All Tasks** and **Schedules**.
 2. From the Scheduled Jobs window, highlight the job associated with the alert you wish to delete.
 3. Click the **Delete Alert** button.
 4. Click **Yes** from the confirmation window. The job-based alert is now deleted.
-

TEST A CONFIGURED ALERT

Required Capability: See Capabilities and Permitted Actions

▶ To test an alert:

1. From the CommCell Browser, right-click the **CommCell** icon, click **Control Panel**, and then click **Alerts**.
 2. From the Alerts window, right-click on an alert, and click **Test**. Follow the prompts to verify the configuration selections.
 3. Click **OK**. A test message will be sent to the recipients of the configured alert.
-

CONFIGURE SNMP TRAPS

▶ To configure SNMP Traps, you must:

1. Make sure that SNMP Services are started on the CommServe computer.
 2. Install the CommServe SNMP Enabler software on the CommServe computer. See *Install the CommServe SNMP Enabler* for step-by-step instructions.
 3. Check that the computers to receive the SNMP Traps are properly set up with the appropriate trap receiver software.
 4. Make sure that SNMP is selected as the notification method for the alert. See *Configure Global Alerts*.
 5. You can add additional computers to receive SNMP Traps. See *Add Additional Computers to Receive SNMP Traps*.
-

ADD ADDITIONAL COMPUTERS TO RECEIVE SNMP TRAPS

Once the CommServe SNMP Traps software is installed on the CommServe computer, you can add additional computers to receive SNMP Traps.

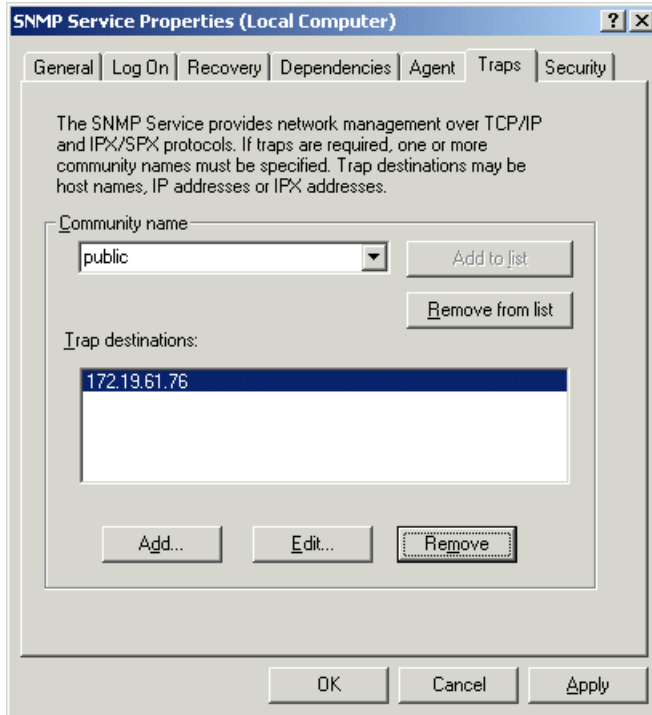
Before You Begin

- A computer must have a SNMP trap receiver program to receive SNMP traps and

- A computer can receive SNMP Traps and alerts from a CommServe without installing the CommServe software.

▶ To add additional computers to receive SNMP Traps:

1. From the CommServe computer, navigate to `Programs\Tools\Administrative Tools\Services`.
2. Right-click `SNMP Services`, then select `Properties`.
3. From the `Traps` tab of the `SNMP Service Properties` dialog box, type the `Community name` and add `Trap destinations` from the `Trap destinations` pane.



4. Click `OK` to save your changes.
5. Restart `SNMP Services` by right-clicking `SNMP Services` and by selecting `Restart`.

[Back to Top](#)

SNMP Enablers

Topics | How To | Related Topics

Overview

SNMP Trap Messages Received by the Trap Receiver Software

- List of Trap Messages

Object Types

License Requirements

OVERVIEW

Alerts can be sent by a CommServe, using the SNMP protocol, to other computers in the form of SNMP Enablers, provided that the SNMP Enabler software is installed on the CommServe computer and SNMP was selected as the alert notification type. For information on installing the SNMP Enabler on the CommServe computer in clustered and non-clustered environments, see:

- Install the CommServe SNMP Enabler
- Install the CommServe SNMP Enabler - Clustered Environment - Virtual Server

An SNMP trap is used for alert notification sent by the CommServe via the SNMP protocol to another computer that receives the SNMP trap using a trap receiver software. An SNMP trap is sent just once each time an alert is generated by the CommServe. These traps are sent in the Management Information Protocol (MIB) format described in [SNMP Trap Messages Received by the Trap Receiver Software](#).

A CommServe computer can send alerts via SNMP traps to multiple computers. These computers can receive these alerts even if they do not have CommServe software installed.

Once an alert is configured and then sent as an SNMP trap, it cannot be resent. Hence, if the connection is lost between the CommServe computer that sent the trap and the remote computer receiving the trap, the trap will not be re-sent once the connection between both computers is restored.

SNMP alert notifications can be customized by adding alert token arguments to the alert configuration. The tokens will be included in the body of the alert notification message.

SUPPORT INFORMATION

SNMP Version 1 (SNMPv1) is the currently supported SNMP protocol.

SNMP TRAP MESSAGES RECEIVED BY THE TRAP RECEIVER SOFTWARE

This section provides an example of an SNMP trap alert message and a description of the fields in the message. The following is an example of an SNMP trap message:

```

Agent Address: 172.19.71.67
Trap OID: .1.3.6.1.4.1.14604.2.2
Time Stamp: 74945
Generic: 6
Specific: 1013
Varbind OID: .1.3.6.1.4.1.14604.2.2.3.0
Varbind Encoding: OCTET STRING
Varbind Value: CommCell - Properties Modified
Varbind OID: .1.3.6.1.4.1.14604.2.2.2.4.0
Varbind Encoding: OCTET STRING
Varbind Value: Tue, 04 Mar 2003 23:11:38 Eastern Standard Time
Varbind OID: .1.3.6.1.4.1.14604.2.2.2.5.0
Varbind Encoding: OCTET STRING
Varbind Value: cvadmin
Varbind OID: .1.3.6.1.4.1.14604.2.2.2.6.0
Varbind Encoding: OCTET STRING
Varbind Value: jade
Varbind OID: .1.3.6.1.4.1.14604.2.2.2.7.0
Varbind Encoding: OCTET STRING
Varbind Value: *
Varbind OID: .1.3.6.1.4.1.14604.2.2.2.8.0
Varbind Encoding: OCTET STRING
Varbind Value: *
Varbind OID: .1.3.6.1.4.1.14604.2.2.2.9.0
Varbind Encoding: OCTET STRING
Varbind Value: *
Varbind OID: .1.3.6.1.4.1.14604.2.2.2.10.0
Varbind Encoding: OCTET STRING
Varbind Value: *
Varbind OID: .1.3.6.1.4.1.14604.2.2.2.11.0
Varbind Encoding: OCTET STRING
Varbind Value: *
Varbind OID: .1.3.6.1.4.1.14604.2.2.2.12.0
Varbind Encoding: OCTET STRING
Varbind Value: *
Varbind OID: .1.3.6.1.4.1.14604.2.2.2.13.0
Varbind Encoding: OCTET STRING
Varbind Value: *
Varbind OID: .1.3.6.1.4.1.14604.2.2.2.14.0
Varbind Encoding: OCTET STRING
Varbind Value: CommCell - Properties Modified
Varbind OID: .1.3.6.1.4.1.14604.2.2.2.15.0
Varbind Encoding: OCTET STRING
Varbind Value: *
Varbind OID: .1.3.6.1.4.1.14604.2.2.2.16.0
Varbind Encoding: OCTET STRING
Varbind Value: 0
Varbind OID: .1.3.6.1.4.1.14604.2.2.2.17.0
Varbind Encoding: OCTET STRING
Varbind Value: Maximum Events in event log changed from [14000]
to [16000]<A>Job Alive check interval changed from [124] to
[120]<A>
    
```

Part 1

The Management Information Base (MIB) file is automatically installed when the SNMP Enabler is installed on a CommServe computer. This file is located at <software installation path>\MIB\Simpana.mib.

The following table lists the fields displayed as identified in Part 1 of the previous sample SNMP trap message, and the MIB definition:

Field	MIB Definition
Agent Address: 172.19.71.67	Address of the agent generating the trap.
Trap OID: .1.3.6.1.4.1.14604.2.2	The first part of the Trap OID indicates the vendor's identification number of the network management system contained in the entity. In this example, this number is the Enterprise identification number. The last part of the Trap OID, 2.2, indicates products and the software, respectively.
Time Stamp: 74945	The time in hundredths of a second since the network management portion of the system was last re-initialized.
Generic: 6	The generic trap type. The number 6 means it is enterprise specific.
Specific: 1013	The specific trap type. Each alert type will be sent using a unique identification number. The alert type (e.g., Data Protection, Disaster Recovery Backup, Data Aging, etc.) can be identified in the content of the trap message.

Part 2

The example that follows describes the Varbind OID field as identified as Part 2 of the SNMP trap message:

```

Varbind OID: .1.3.6.1.4.1.14604.2.2.3.0
    
```

LIST OF TRAP MESSAGES

The following table provides a list of Trap Messages generated by the SNMP Enabler.

Alert Number	OID	Alert Name	Category Name	Alert Criteria
1001	.1.3.6.1.4.1.14604.2.2.2.0.1001	Data Aging	Job Management	Failed
				Job Activity
				Job Succeeded with Errors
				Skipped
				Succeeded (Not trapped)
1002	.1.3.6.1.4.1.14604.2.2.2.0.1002	Auxiliary Copy	Job Management	Alert every "n" attempts (Network failures)
				Alert every "n" attempts (Phase failures)
				Auxiliary copy fallen behind alert Delayed by "n" Hrs
				Failed
				Job Activity
				Job Succeeded with Errors
				Skipped
				Succeeded (Not trapped)
1003	.1.3.6.1.4.1.14604.2.2.2.0.1003	Data Protection	Job Management	Alert every "n" attempts (Network failures)
				Alert every "n" attempts (Phase failures)
				ASR Backup Has occurred.
				Decrease in Data size by <1,2,10,0,-1> %
				Delayed by "n" Hrs
				Failed
				Increase in Data size by <1,2,10,0,-1> %
				Job Activity
				Job Succeeded with Errors
				No Data Protection
				Skipped
				Succeeded (Not trapped)
1004	.1.3.6.1.4.1.14604.2.2.2.0.1004	Data Recovery	Job Management	Failed
				Job Activity
				Job Started
				Job Succeeded with Errors
				List Media
				Skipped
1005	.1.3.6.1.4.1.14604.2.2.2.0.1005	Express Recovery	Job Management	Delayed by "n" Hrs
				Failed
				Job Activity
				Job Succeeded with Errors
				Skipped
				Succeeded (Not trapped)
1006	.1.3.6.1.4.1.14604.2.2.2.0.1006	Data Verification	Job Management	Delayed by "n" Hrs
				Failed
				Job Activity
				Job Succeeded with Errors
				Skipped

				Succeeded (Not trapped)
1007	.1.3.6.1.4.1.14604.2.2.2.0.1007	Media Inventory	Job Management	Failed
				Job Succeeded with Errors
				Succeeded (Not trapped)
1009	.1.3.6.1.4.1.14604.2.2.2.0.1009	Media Erase	Job Management	Failed
				Job Activity
				Job Succeeded with Errors
				Succeeded (Not trapped)
1010	.1.3.6.1.4.1.14604.2.2.2.0.1010	Clients	Configuration	Disk Space Low
				Properties Modified
1012	.1.3.6.1.4.1.14604.2.2.2.0.1012	CommCell	Configuration	Alert every <1,3,3,1,-1> failed login attempts
				Alert Modified
				Disk Space Low
				Force deconfigured
				Properties Modified
1013	.1.3.6.1.4.1.14604.2.2.2.0.1013	MediaAgents	Configuration	Disk Space Low
				MediaAgent went Offline
				Properties Modified
1014	.1.3.6.1.4.1.14604.2.2.2.0.1014	Schedules	Configuration	Scheduler Changes
1015	.1.3.6.1.4.1.14604.2.2.2.0.1015	Storage Policy	Configuration	Properties Modified
1016	.1.3.6.1.4.1.14604.2.2.2.0.1016	Library	Configuration	Properties Modified
1017	.1.3.6.1.4.1.14604.2.2.2.0.1017	Library Management	Media Management	Insufficient Storage
				Maintenance Occurred
				Maintenance Required
				Media Handling Errors
				Media Handling Required
				Media Mount and Usage Errors
				Media Ready in CAP Alert
				Media Recalled
User overwrite of Media				
1018	.1.3.6.1.4.1.14604.2.2.2.0.1018	VaultTracker	Media Management	Failed
				Initiated
				Job Succeeded with Errors
				Media Handling Required
				Media Picked up
				Media Reached Destination
				Media Returned to Source
				Rolled Back
Succeeded (Not trapped)				
1019	.1.3.6.1.4.1.14604.2.2.2.0.1019	Download Updates	Automatic Updates	Failed
				Job Succeeded with Errors
				Succeeded (Not trapped)
1020	.1.3.6.1.4.1.14604.2.2.2.0.1020	Install Updates	Automatic Updates	Failed
				Initiated
				Job Succeeded with Errors

				Succeeded (Not trapped)
1021	.1.3.6.1.4.1.14604.2.2.2.0.1021	Device Status	Media Management	Drive went Offline
				Library went Offline
				Mountpath went Offline
1022	.1.3.6.1.4.1.14604.2.2.2.0.1022	Erase Data	Job Management	Failed
				Job Activity
				Job Succeeded with Errors
				Skipped
				Succeeded (Not trapped)
1023	.1.3.6.1.4.1.14604.2.2.2.0.1023	Exchange Agent Specific Alerts	Application Management	Journal Mailboxes message Count Exceeded
1024	.1.3.6.1.4.1.14604.2.2.2.0.1024	Updates Available For Download	Automatic Updates	Updates Available
1025	.1.3.6.1.4.1.14604.2.2.2.0.1025	File Replication Alerts	Application Management	Log file volume reached low watermark
				No log transfer activity
1026	.1.3.6.1.4.1.14604.2.2.2.0.1026	Upgrades and Updates	Automatic Updates	Release Upgrade Required
				Updates Required
1028	.1.3.6.1.4.1.14604.2.2.2.0.1028	Continuous Data Replication	Job Management	Alert every "n" attempts (Network failures)
				Alert every "n" attempts (Phase failures)
				Delayed by "n" Hrs
				Failed
				Job Activity
				Job Succeeded with Errors
				Skipped
				Succeeded (Not trapped)
1029	.1.3.6.1.4.1.14604.2.2.2.0.1029	Offline Content Indexing		Delayed by "n" Hrs
				Failed
				Job Activity
				Job Succeeded with Errors
				Skipped
				Succeeded (Not trapped)
1030	.1.3.6.1.4.1.14604.2.2.2.0.1030	SharePoint Agent Specific Alerts		Virtual Servers Added
				V2 upgraded to V3
1031	.1.3.6.1.4.1.14604.2.2.2.0.1031	Windows File System Agent Specific Alerts	SRM Thresholds	Not trapped
1032	.1.3.6.1.4.1.14604.2.2.2.0.1032	Oracle Agent Specific Alerts	SRM Thresholds	Not trapped
1033	.1.3.6.1.4.1.14604.2.2.2.0.1033	SQL Server Agent Specific Alerts	SRM Thresholds	Not trapped
1034	.1.3.6.1.4.1.14604.2.2.2.0.1034	NAS Agent Specific Alerts	SRM Thresholds	Not trapped
1035	.1.3.6.1.4.1.14604.2.2.2.0.1035	Exchange Agent Specific Alerts	SRM Thresholds	Not trapped
1036	.1.3.6.1.4.1.14604.2.2.2.0.1036	SharePoint Agent Specific Alerts	SRM Thresholds	Not trapped
1037	.1.3.6.1.4.1.14604.2.2.2.0.1037	Unix File System Agent Specific Alerts	SRM Thresholds	Not trapped
1038	.1.3.6.1.4.1.14604.2.2.2.0.1038	Cost Analysis	SRM Thresholds	Not trapped
1039	.1.3.6.1.4.1.14604.2.2.2.0.1039	Netware Agent Specific Alerts	SRM Thresholds	Not trapped
1051	.1.3.6.1.4.1.14604.2.2.2.0.1051	SRM Data Collection	Job Management	Alert every "n" attempts (Network failures)
				Alert every "n" attempts (Phase failures)
				Failed
				Job Activity

				Job Succeeded with Errors
				No Data Protection
				Skipped
				Succeeded (Not trapped)
1052	.1.3.6.1.4.1.14604.2.2.2.0.1052	Report	Job Management	Failed
				Job Activity
				Job Succeeded with Errors
				Skipped
				Succeeded (Not trapped)
1053	.1.3.6.1.4.1.14604.2.2.2.0.1053	Information Management	Job Management	Delayed by "n" Hrs
				Failed
				Job Activity
				Job Succeeded with Errors
				Skipped
				Succeeded (Not trapped)

OBJECT TYPES

The following table lists the object types and their corresponding MIB definitions that are displayed in the `Varbind` OID fields of the SNMP trap example message.

Object Type	MIB Definition
3	Alert type.
4	Date and time of the alert.
5	The CommCell user that performed the operation.
6	The CommCell that generated the alert.
7	The name of the CommCell client.
8	The name of the CommCell agent.
9	The name of the CommCell instance.
10	The name of the CommCell backup set.
11	The name of the CommCell subclient.
12	The name of the CommCell MediaAgent.
13	The name of the library.
14	The name of the media.
15	The name of the CommCell storage policy.
16	The Job ID.
17	The CommCell alert message.

LICENSE REQUIREMENTS

This feature requires a Feature License to be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

[Back To Top](#)

SNMP Enablers - How To

[Topics](#) | [How To](#) | [Related Topics](#)

Configure SNMP Traps

Add Additional Computers to Receive SNMP Traps

CONFIGURE SNMP TRAPS

▶ To configure SNMP Traps, you must:

1. Make sure that SNMP Services are started on the CommServe computer.
 2. Install the CommServe SNMP Enabler software on the CommServe computer. See [Install the CommServe SNMP Enabler](#) for step-by-step instructions.
 3. Check that the computers to receive the SNMP Traps are properly set up with the appropriate trap receiver software.
 4. Make sure that SNMP is selected as the notification method for the alert. See [Configure Global Alerts](#).
 5. You can add additional computers to receive SNMP Traps. See [Add Additional Computers to Receive SNMP Traps](#).
-

ADD ADDITIONAL COMPUTERS TO RECEIVE SNMP TRAPS

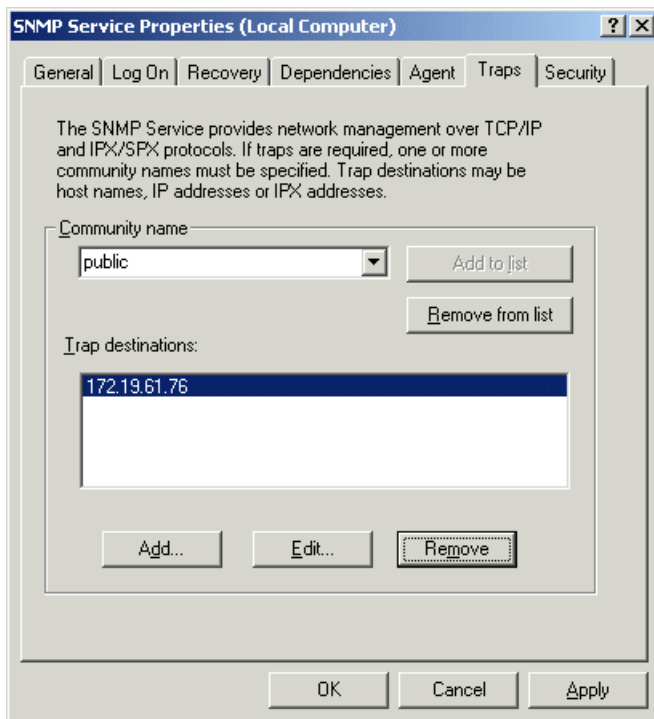
Once the CommServe SNMP Traps software is installed on the CommServe computer, you can add additional computers to receive SNMP Traps.

Before You Begin

- A computer must have a SNMP trap receiver program to receive SNMP traps and
- A computer can receive SNMP Traps and alerts from a CommServe without installing the CommServe software.

▶ To add additional computers to receive SNMP Traps:

1. From the CommServe computer, navigate to `Programs\Tools\Administrative Tools\Services`.
2. Right-click `SNMP Services`, then select `Properties`.
3. From the `Traps` tab of the `SNMP Service Properties` dialog box, type the `Community` name and add `Trap destinations` from the `Trap destinations` pane.



4. Click `OK` to save your changes.
 5. Restart SNMP Services by right-clicking `SNMP Services` and by selecting `Restart`.
-

[Back To Top](#)

Event Viewer

Topics | How To | Related Topics

Overview

The Event Viewer Window

Event Search Queries

Related Reports

OVERVIEW

The Event Viewer allows you to monitor activities that are occurring within the CommCell. This information is useful for troubleshooting and informational purposes. For example, you may want to know if your system is experiencing hardware problems, or what jobs have started or completed.

In addition to events, there are other ways you can obtain information about conditions within the CommCell, such as from configured Alerts, or from Log Files.

THE EVENT VIEWER WINDOW

Events are displayed in the Event Viewer with the severity levels of Information, Minor, Major, and Critical, along with additional information, such as, the subsystem that generated the event.

By default, the maximum number of events displayed in the Event Viewer is 200. You can modify this number from the `Event Filter` tab of the `User Preferences` dialog box. You can also filter the types of events to be displayed based on the severity level.

By default, the Event Viewer displays the following columns:

Severity	An icon indicating the following severity levels:	
	Information	Indicates a normal, expected event. Reported information events include the initiation and completion of key jobs and operations.
	Minor	Indicates an abnormal or unexpected event that does not affect running processes.
	Major	Indicates a major error affecting a single client or application.
	Critical	Indicates critical system conditions affecting multiple clients or applications.
Event ID	A unique identifier indicating the order in which the events are received by the CommServe. The most recent events are displayed at the beginning of the Event Viewer window.	
Job ID	A unique identifier for each data protection, data recovery or administration operation.	
Date	The date when the event was generated based on the CommServe time zone.	
Time	The time when the event was generated based on the CommServe time zone.	
Program	The subsystem that generated the event. (For example, the Job Manager or Media Manager.)	
Computer	The computer from which the event was generated.	

Description	A detailed description of the event.
-------------	--------------------------------------

VIEW THE DETAILS OF AN EVENT

If a particular event is not entirely visible in the Event Viewer, the complete description can be viewed in the `Event Details` dialog box.

If a user is not part of the `View All` user group, then that user will not see CommCell objects for which the user's member user group(s) does not have associations. Furthermore, users will not be able to view the Job Controller or Event Viewer details associated with the CommCell objects for which they do not have permissions. Note that a user will not be able to view these CommCell objects upon logging onto the CommCell Console after the restrictions have been set.

EVENT SEARCH QUERIES

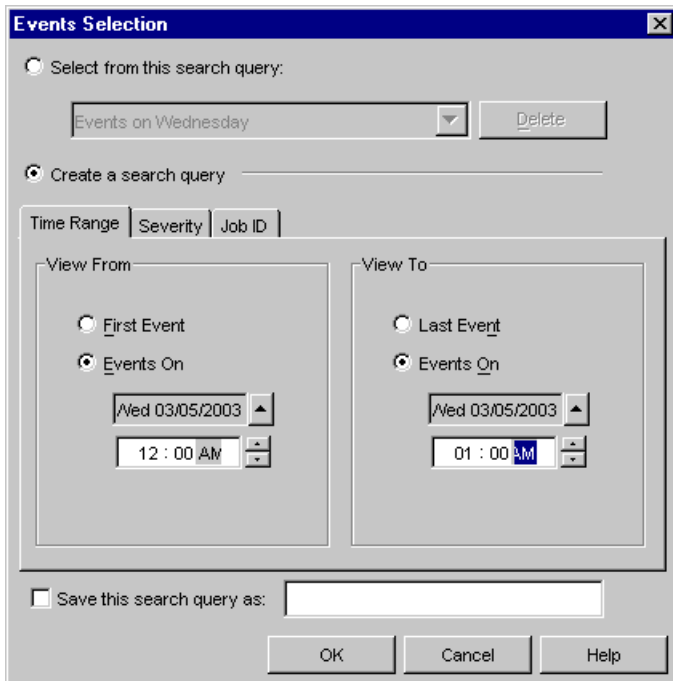
To view only selected events from the Event Viewer, a search query can be created to display only those events that correspond to a time range and severity level, or a Job ID. The results of your query are displayed in the `All Found Events` window.

CREATE AND SAVE A SEARCH QUERY BASED ON TIME RANGE AND SEVERITY

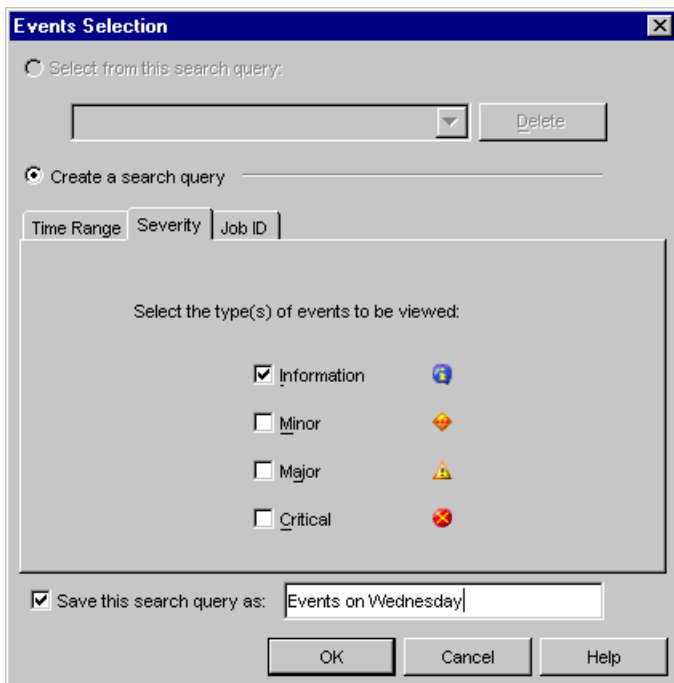
A search query for a particular time range and severity level can be created and saved for re-use.

For example, a list of all the events in the Event Viewer that had a severity of `Information` that occurred between 12:00 a.m. and 1:00 a.m. is required.

In the sample image that follows, a time range of 12:00 a.m. to 1:00 a.m. is specified in the `Time Range` tab of the `Events Selection` dialog box.



An event severity of `Information` is selected from the `Severity` tab, and the search query is saved with a defined name.

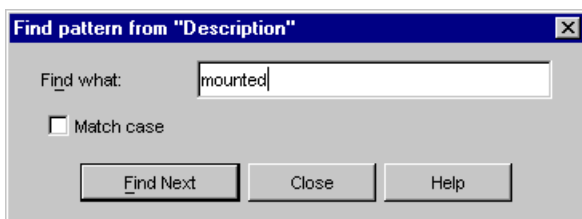


A list of the filtered events are then displayed in the All Found Events window. The results are not dynamically updated.

All Found Events Associated with query: Events on Wednesday (Total: 8 events)							
...	Event ID	Job ID	Date	Time	Program	Computer	Description
?	69		2003/03/05	00:25:24	MediaManager	purple	Media with barcode [000167] unmounted from library [Lib...
?	68		7 2003/03/05	00:03:49	JobManager	purple	Backup job [7] completed.
?	67		7 2003/03/05	00:01:54	MediaManager	purple	Media with barcode [000167], side [A_16], mounted on li...
?	66		8 2003/03/05	00:00:04	JobManager	purple	Another backup is running for client [purple], iDataAgent ...
?	65		8 2003/03/05	00:00:03	JobManager	purple	Backup job [8] has been converted to a full backup beca...
?	64		7 2003/03/05	00:00:03	JobManager	purple	Backup job [7] has been converted to a full backup beca...
?	63		8 2003/03/05	00:00:03	JobManager	purple	New backup request received for Client [purple], Applica...
?	62		7 2003/03/05	00:00:03	JobManager	purple	New backup request received for Client [purple], Applica...

You can also use the Find pattern from "Description" dialog box to find the events in the All Found Events window that match a particular character string. If the search for a particular character string falls outside of the viewable window, you can use the scroll bar to view the search result.

In the sample image that follows, mounted is entered as a character string.



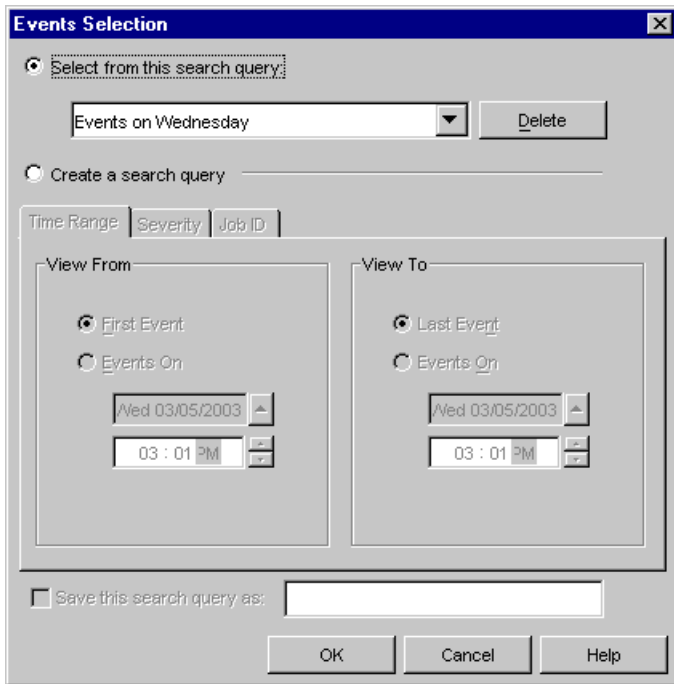
Once entered, the first event matching the character string will be highlighted in the All Found Events window.

All Found Events Associated with query: Events on Wednesday (Total: 8 events)							
...	Event ID	Job ID	Date	Time	Program	Computer	Description
	69		2003/03/...	00:25:24	MediaMa...	purple	Media with barcode [000167] unmounted from librar...
	68	7	2003/03/...	00:03:49	JobMan...	purple	Backup job [7] completed.
	67	7	2003/03/...	00:01:54	MediaMa...	purple	Media with barcode [000167], side [A_16], mounted ...
	66	8	2003/03/...	00:00:04	JobMan...	purple	Another backup is running for client [purple], iDataA...
	65	8	2003/03/...	00:00:03	JobMan...	purple	Backup job [8] has been converted to a full backup ...
	64	7	2003/03/...	00:00:03	JobMan...	purple	Backup job [7] has been converted to a full backup ...
	63	8	2003/03/...	00:00:03	JobMan...	purple	New backup request received for Client [purple], Ap...
	62	7	2003/03/...	00:00:03	JobMan...	purple	New backup request received for Client [purple], Ap...

From the All Found Events window, you can view more detailed information about each event from the Event Details dialog box.

Event Details			
Event			
Event ID:	69	Severity:	Information
Date:	2003/03/05	Time:	00:25:24
Source			
Computer:	purple		
Program:	MediaManager		
Job ID:			
Description:			
Media with barcode [000167] unmounted from library [Library2] and drive [Lib2_Drive1]. Mount Point [\\.\Tape0].			<input type="button" value="↑"/> <input type="button" value="↓"/>
<input type="button" value="Close"/>		<input type="button" value="Help"/>	

If the search query is saved, it can be selected from the Select from this search query field. A list of the filtered events are then displayed in the All Found Events window.

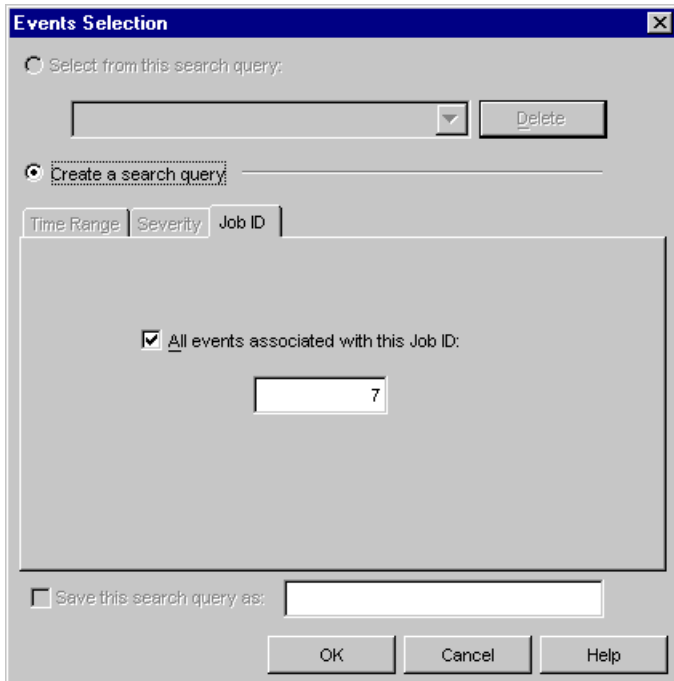


CREATE A SEARCH QUERY BASED ON JOB ID

You can create a search query to display only those events that are associated with a particular Job ID. A search query based on a particular Job ID cannot be saved.

For example, a list of all the events in the Event Viewer that are associated with Job ID 7 is required.

Job ID 7 is specified in the All Events associated with this Job ID field of the Job ID tab.



All events that have a Job ID of 7 are then displayed in the All Found Events window.

All Found Events Associated with Job ID: 7 (Total: 4 events)							
...	Event ID	Job ID	Date	Time	Program	Computer	Description
?	68	7	2003/03/05	00:03:49	JobManager	purple	Backup job [7] completed.
?	67	7	2003/03/05	00:01:54	MediaManager	purple	Media with barcode [000167], side [A_16], mounted on libr...
?	64	7	2003/03/05	00:00:03	JobManager	purple	Backup job [7] has been converted to a full backup becau...
?	62	7	2003/03/05	00:00:03	JobManager	purple	New backup request received for Client [purple], Applicati...

RELATED REPORTS

EVENT REPORT

The Event Report provides a list of the events based on the selected filter criteria.

[Back To Top](#)

Event Viewer - How To

[Topics](#) | [How To](#) | [Related Topics](#)

[Change Table Views](#)

[Change the Default Event Viewer Display](#)

[Create a Search Query](#)

[Open a Console Window](#)

[Set the Maximum Number of Events Retained by the System](#)

[View Event Details in the Event Viewer](#)

CHANGE TABLE VIEWS

▶ To change the table views for the Job Controller and Event Viewer:

1. From the Job Controller or Event Viewer windows in the CommCell Console, perform either of the following:
 - Right-click any field within the associated window.
 - OR
 - Click the Table Menu icon at the upper right hand corner of the associated window.

The available options for that window are displayed.
2. Select or deselect the parameters you want presented in the respective window.

CHANGE THE DEFAULT EVENT VIEWER DISPLAY

▶ To change the default Event Viewer display:

1. From the CommCell Console, select **Tools** | **Control Panel**.
2. From the **Control Panel**, select **User Preferences**.
3. From the Event Filter tab, select the severity level(s) that you want to use as the default.
4. Type the maximum number of events to be displayed in the Event Viewer (Default = 200).

5. Click **OK** to save your changes.
-

CREATING A SEARCH QUERY

▶ To create a search query from the Event Viewer:

1. From the CommCell Browser, right-click the CommServe icon, select **All Tasks** and **Event Search**, or right-click an event in the Event Viewer, then select **Search Events**.
 2. From the **Events Selection** dialog box, select **Create a search query**.
 3. From either the Time Range, Severity, or Job ID tabs, select a time range, severity level or Job ID.
 4. If a time period an/or severity level criteria is used, you can save this search query for reference later. To do this, type a name in the **Save this search query as** field.
 5. A static All Found Events window displays the events that meet the criteria that you selected in the **Events Selection Dialog**.
 6. To view the details of a particular event, right click an event and select **Details**. Use the up and down arrows in the widow to view the details on the next and previous events in the window.
 7. To search the description column, right-click an event and select **Find**. From the Find Pattern From "Description" dialog box, type the character string that you want to search. The events that include the character string you typed are then highlighted when you click **Next** or **Find Next**.
 8. Click **OK**.
-

OPEN A CONSOLE WINDOW

▶ To open the CommCell Browser, Job Controller or Event Viewer window:

1. From the CommCell Console, select **Tools** and the desired window.
 2. Alternatively, click the desired icon from the toolbar.
-

SETTING THE MAXIMUM NUMBER OF EVENTS RETAINED BY THE SYSTEM

▶ To set the maximum number of events retained by the event log:

1. From the CommCell Browser, right-click the CommCell icon, and click **Control Panel**, and then click **System**.
 2. From the System dialog box, enter a number in the **Max. Number of Events Retained in Event Log** box (default = 10000).
 3. Click **OK**.
-

VIEW EVENT DETAILS IN THE EVENT VIEWER

▶ To view event details in the Event Viewer:

1. From the CommCell Console, click the **Event Viewer** icon if the window is not already open.
By default, the Event Viewer displays the Information, Minor, Major, and Critical events (up to 200) that took place in the last 24 hours.
 2. To view the details about a particular event, right-click an event and select **Detail**. The Event Details dialog box displays the details of the event and the up and down arrows allow you to view the details of the next and previous events of the event viewer.
 3. Click **OK**.
-

[Back to Top](#)

Reports - Overview

[Topics](#) | [How To](#) | [Troubleshoot](#) | [Support](#) | [Related Topics](#)

Overview

- [Report Features](#)
- [SRM Reports](#)
- [CommNet Reports](#)

Report Operations

- [Create a Report](#)
- [Save a Report Template](#)
- [Cancel a Running Report](#)
- [Schedule a Report](#)
- [View/Modify a Scheduled Report](#)
- [Save a Report as an XML File](#)

Related Alerts

OVERVIEW

A variety of reports can be created, each tailored to a particular aspect of data management. Through filter criteria, you can customize each report to include only the data that is required, including whether or not you want to save it to a local drive on the CommServe or a network drive in various formats. Once the criteria is specified, the report can be generated. Reports can then be scheduled and sent to a CommCell user or any valid email address from the Reports icon. Report templates can be customized and saved under the **Reports** node to be generated for later use.

By default, reports are generated in the same language as the CommCell Console. Also by default, scheduled reports are sent in the language of the CommCell Console on which they were scheduled. However, the report can be generated and scheduled in a different language than that of the CommCell Console. The languages currently supported are listed in [Languages - Support](#). To generate the same report in multiple languages, the report must be scheduled and sent to recipients separately.

To generate a report from a remote CommCell Console:

- The Microsoft Internet Information Server (IIS) must be installed and configured on the CommServe computer, or
- IIS and the CommCell Console must be installed on an alternate computer. The IIS Server settings must be configured to use the alternate computer's IIS Server.

REPORT FEATURES

These features are provided by reports:

- The appearance of some reports may be affected by the browser package or version.
- Reports can be saved in either HTML (default), Text, PDF, Iron Mountain, Style Sheet or XML formats. See [Support Information - Report Output Options](#) for more information.
- Reports are saved in the `<Software Directory>\Reports` directory for at least two days after the report is created. After the two-day period has elapsed, the reports are deleted automatically whenever another report is created.
- Reports can also be saved to a local or network location. If saving to a local folder on a client machine, a username and password is not required. For network locations, you may need to specify a username and password. Reports can also be uploaded to a File Transfer Protocol (FTP) Server.
- Job options and client properties can be optionally collapsed in a report. Typically, the options and properties are expanded in the report. When collapsed, the length of the report is reduced and they are exposed only when the link is selected in the report. This is available for reports, such as: Job Schedule Report, Job Summary Reports, and CommCell Configuration Reports.
- Each report is color coded. To print the report in color, ensure that your web browser printer settings are set up for color printing. See [Reports - Troubleshooting](#) for more information.
- Error Codes related to reports contain a failure reason and can be viewed in the Job Details, Job History, and all Job Summary Reports. By clicking on the code, you can view the articles in the customer support website. For more information, see [View Troubleshooting Article\(s\) Available from the Customer Support Website](#).

SRM REPORTS

SRM Reports provides a consolidated view of all storage resources, providing unified tools to analyze storage requirements and plan storage infrastructure for the purposes of asset management, capacity management, content management, and historical data management across the entire enterprise. See [SRM](#)

Reports - Overview for more information.

COMMNET REPORTS

CommNet reports allow you to view and analyze data related to various aspects of the entities that comprise your CommNet domain, including CommCells, libraries, clients, and MediaAgents. For more information, see CommNet Reports.

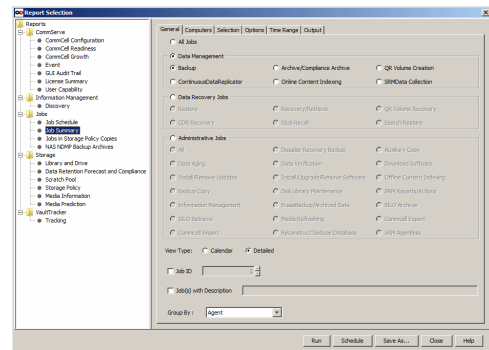
REPORT OPERATIONS

CREATE A REPORT

Each report can be selected from the Report Selection dialog box, which is displayed through the Reports icon or the Reports node in the CommCell Browser tree. Where applicable, filter options are available from the **General**, **Time Range**, and **Output** tabs. Some reports have additional tabs, such as the CommCell Configuration, CommCell Readiness, Job Summary, Media Information, and Tracking reports.

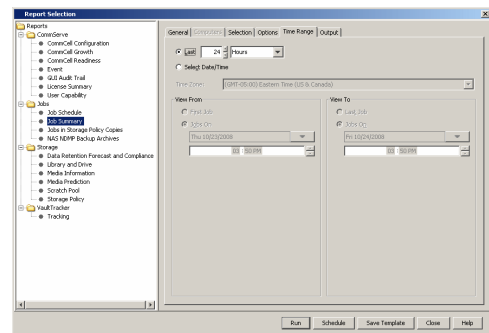
GENERAL TAB

The **General** tab allows you to select filter options based on the selected report.



TIME RANGE TAB

The **Time Range** tab allows you to select which time ranges to include in the report.



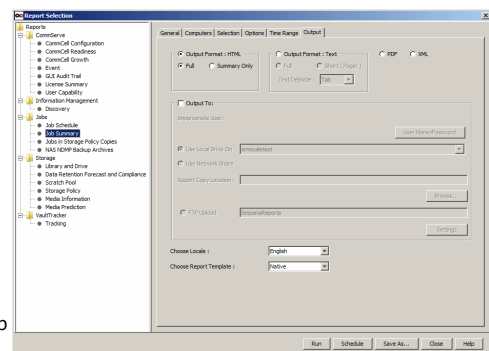
OUTPUT TAB

The **Output** tab allows you to select the output format of the report. The report can be generated and saved to a local drive on the CommServe or a network drive in HTML (default), Text, PDF, Iron Mountain, Style Sheet or XML formats. Ensure that the user account is accessible to the network path.

Reports can also be saved to a local or network location. If saving to a local folder on a client machine, a username and password is not required. For network locations, you may need to specify a username and password. Reports can also be uploaded to a File Transfer Protocol (FTP) Server.

By default, reports are generated and saved in the same language as the CommCell Console. However, the report can be generated in a different language than that of the CommCell Console by selecting a language in **Choose Locale**. The languages currently supported are listed in Languages - Support.

By default, all reports display information according to CommCell entities; that is, a NetBackup policy will appear as a subclient, and so on. However, select NetBackup from the **Choose Report Template** to display information according to the original NetBackup entity.



SAVE A REPORT TEMPLATE

Report templates can be customized and saved under the **Reports** node to be generated for later use.

Report templates that are saved by you are saved under the **My Reports** node. These

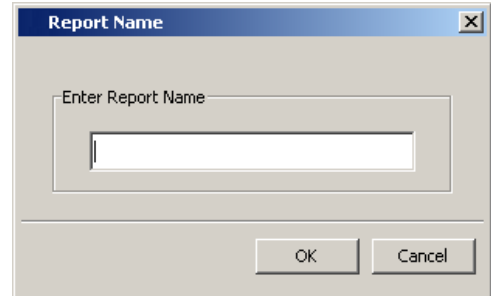
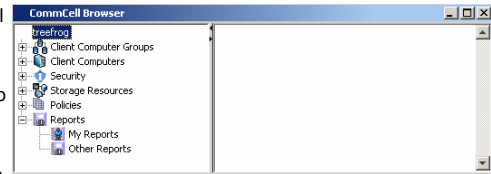
templates can be run, edited, scheduled, and can specify saving the generated report to a local drive on the CommServe or a network drive.

Report templates that have been saved by other users appear in the **Other Reports** node. These templates can be run, viewed, scheduled, and can specify saving the generated report to a local drive on the CommServe or a network drive.

Report templates in the **My Reports** node can be overwritten or saved as a new report template. Modifying and saving report templates in the **Other Reports** node will be saved as a new report in the **My Reports** node. Report templates belonging to another user will not be overwritten when saved.

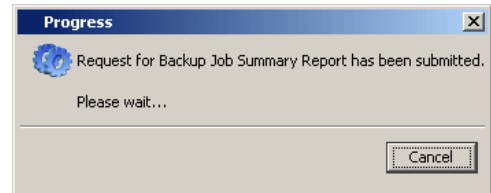
The `Report Name` dialog box allows you to enter a unique name to save a report template. All saved report templates should have a unique name for a specific user.

When a saved report is run, the saved name is displayed in the report output under the report title.



CANCEL A RUNNING REPORT

While running a report, the `Progress` dialog box allows you to stop running the report if you select the **Cancel** button.



SCHEDULE A REPORT

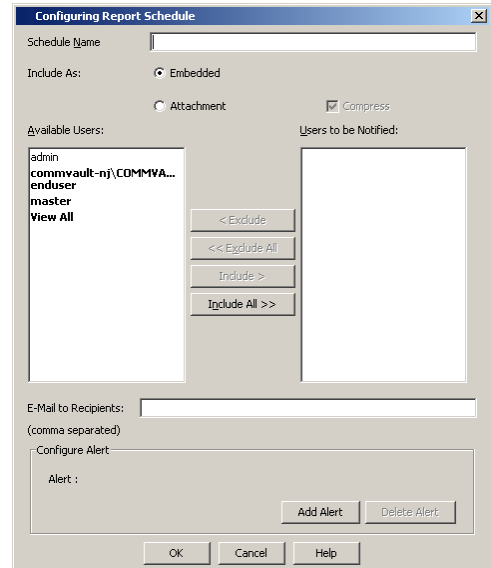
Reports can be scheduled and sent to a CommCell user or any valid email address from the Reports icon or while editing a report from the Reports tree in the CommCell Browser. The report can be sent embedded or as an attachment in an e-mail.

Before sending an email, you must set-up the email server within the CommCell Console. See `E-Mail Server Configuration` for more information.

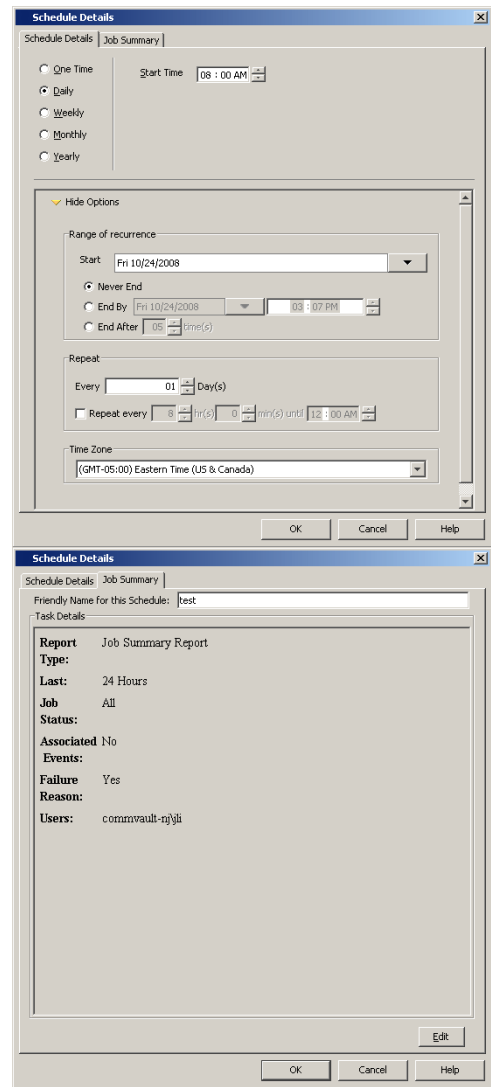
As a best practice, it is recommended that text-formatted reports be scheduled as attachments. This way, the reports are associated with Excel and delivered as Excel files. If text-formatted reports are scheduled as embedded, then they are delivered as plain text files. The file size of some reports can grow quite large and, if attached to an e-mail, the e-mail message will be rejected by the mail program because of the size. Optionally, large report files can be compressed to reduce the file size and alleviate the problem of an e-mail message being rejected.

The `Configuring Report Schedule` dialog box allows you to enter a name of the schedule, if the report should be sent embedded in an email or sent as an attachment, if the file should be compressed as an attachment, and also allows you to select the CommCell users or enter any valid email addresses for who should receive the report.

The user account used to access the CommCell Console when you schedule a report is the owner of the schedule. Only the owner of the schedule can modify the defined schedule pattern. If the owner's user account is deleted, the report will still be sent, but will not contain any data (because there aren't any user permissions). However, ownership of the scheduled report can be transferred to another user upon user account deletion, which is recommended if the report is still needed for your environment. For more information, see `Delete a User`.



The `Schedule Details` tab of the `Schedule Details` dialog box allows you to select the details of the schedule, such as the date, time, and time zone.



The `Job Summary` tab displays the filter options of the schedule.

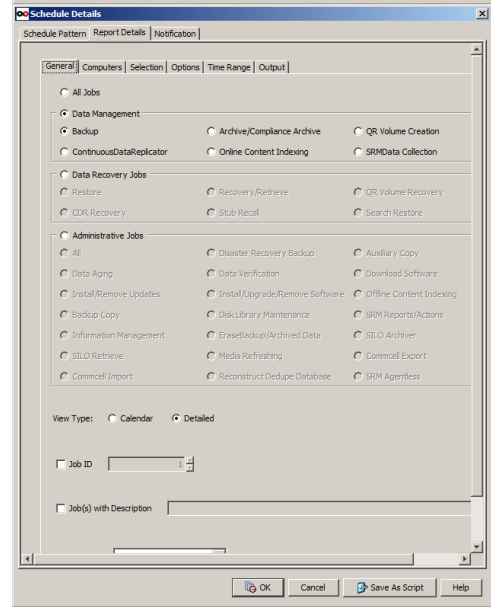
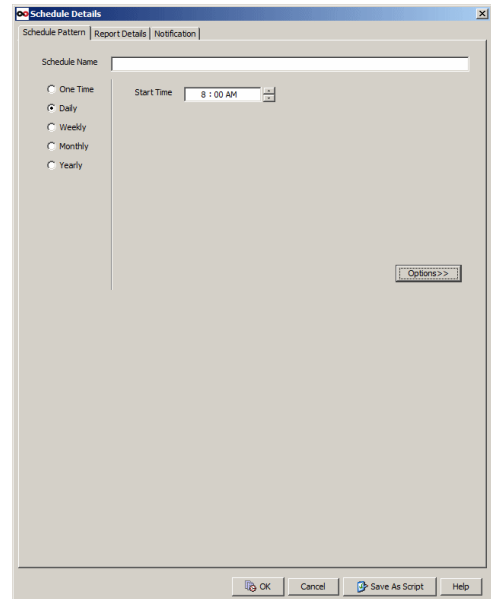
A scheduled report can be configured to be sent via e-mail to user groups created from within the CommCell Console as well as external domain user groups. However, individual external domain users will not receive the report via e-mail if they have not previously logged on to the CommCell Console. Users (from the user groups created from within the CommCell Console) will receive the report e-mail regardless of their login status.

VIEW/MODIFY A SCHEDULED REPORT

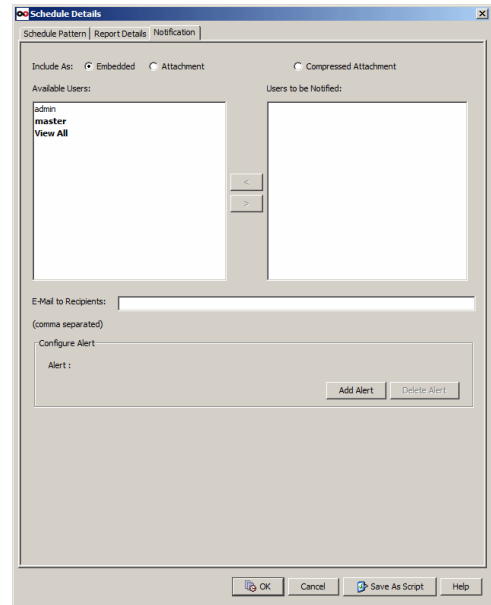
The report schedule can be viewed in the `Scheduled Jobs` window. Additional schedule modifications can be made from this window.

Scheduled report modifications can be made while scheduling and after creating the schedule from the `Modifying Scheduled Report` dialog box.

Additional tabs, if applicable, are available from the `Detail` tab.



Notification options are available from the `Notification` tab.

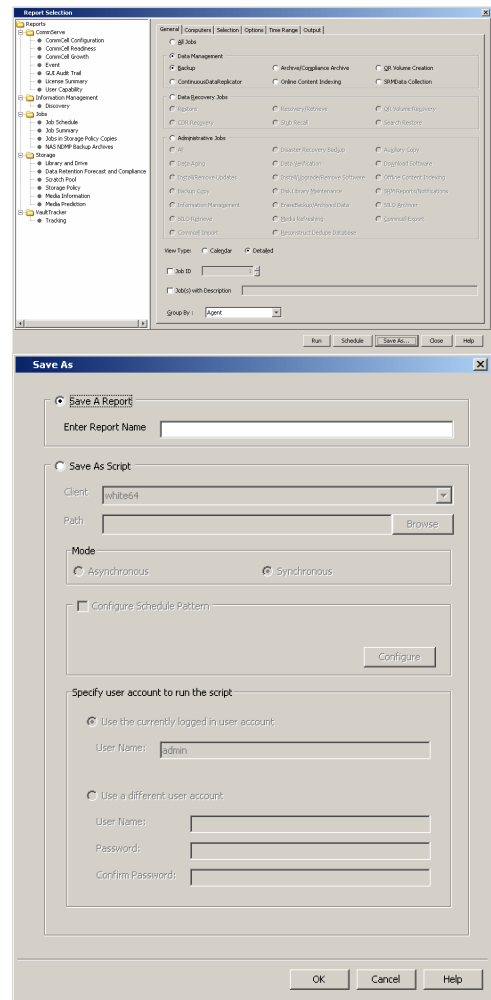


SAVE A REPORT AS AN XML FILE

The options of a report can be saved and run at a later point in time.

While creating a report, the options that you specify can be saved in an .xml file by using the **Save As Script** option. Once saved, it can later be executed from the command line interface using the `operation execute` command.

For more information, see [Command Line Interface - Save As Script](#).



In the **Save As** dialog box:

1. Click **Save As Script**.
2. Enter or **Browse** to a path and name for the script file to be saved on the CommServe computer.
3. In the **Path** field, select the location of the client on which you want to save the script. Either type the path or click **Browse** to navigate to a path and enter name for the script file to be saved on the CommServe computer.
4. Select **Synchronous** or **Asynchronous** execution. Some job types will always be performed asynchronously and the synchronous option will be disabled.
 - o A synchronous operation exits only when the operation has completed.
 - o An asynchronous operation submits the job to the CommServe and exits immediately, returning control to the calling program or script.
5. Click **OK** to save the operation as a script file.

If a script with same name exists, you can decide if the existing script must be overwritten. In addition, you can decide the extension of the save as script file.

RELATED ALERTS

The following Job Management Report alerts can be configured from the Alerts Wizard:

- Job Activity
- Job Failed
- Job Skipped
- Job Succeeded
- Job Succeeded with Errors

For more information, see:

- Alerts: Job Management
- Configure Alerts

[Back to Top](#)

Reports - How To

[Topics](#) | [How To](#) | [Troubleshoot](#) | [Support](#) | [Related Topics](#)

[Create a Report](#)

[Save a Report Template](#)

[Schedule a Report](#)

[Modify a Scheduled Report](#)

CREATE A REPORT

Required Capability: See Capabilities and Permitted Actions

Refer to the procedures in the corresponding reports for step-by-step instructions.

SAVE A REPORT TEMPLATE

Required Capability: See Capabilities and Permitted Actions

▶ To save a report template:

1. From the CommCell Console, click the Reports icon or expand the **My Reports** node, right-click the **General** node and select **New Report**.
2. From the **Report Selection** dialog box, click a report from the **Reports** pane.
3. From the report, select the appropriate filter options, and then click **Save As....** The **Save As...** dialog box is displayed.
4. Enter the name of the report and click **OK** to exit the screen.
5. A popup confirmation message appears.

Click **OK** to continue. The report template name displays in the under **General** of the **My Reports** node of the CommCell Browser.

Required Capability: See Capabilities and Permitted Actions

▶ To save a report template from the My Reports node:

1. From the CommCell Browser, right-click a report from the **My Reports** node and select **Edit** to display the report template for the selected report.
2. Modify the report's filter options as necessary and click **Save**.
3. From the **Report Name** dialog box, enter the name of the report and click **OK**. If you enter the same name as the existing report, the system prompts with an overwrite warning.

Click **Yes** to overwrite the existing report.

Click **No** to enter a new name.
4. Click **OK** to exit the screen.
5. A popup confirmation message appears.

Click **OK** to continue.

Required Capability: See Capabilities and Permitted Actions

▶ To save a report template from the Other Reports node:

1. From the CommCell Browser, right-click a report from the **Other Reports** node and select **View** to display the report template for the selected report.
2. Modify the report's filter options as necessary and click **Save As**.
3. From the **Report Name** dialog box, enter the new name of the report and click **OK** to exit the screen.
4. A popup confirmation message appears.

Click **OK** to continue. The report name displays in the **My Reports** node of the CommCell Browser.

SCHEDULE A REPORT

Required Capability: See Capabilities and Permitted Actions

Before you Begin

- Before scheduling a report, go to the **Tools** menu and select **Control Panel** and then click on the **E-Mail & IIS Configuration** icon. On the **E-Mail Server** tab:
 - Specify a valid **Mail Server**. The Mail Server must support SMTP messages.
 - Select the port number in the **Mail Server Port** box. The default Mail Server port number is 25.
 - Specify the **Mail Server Size Limit** per e-mail.
 - Specify a valid e-mail address in the **Senders Address** box.
- Ensure that the users who are to receive the report have a CommCell user account with a valid email address. Alternatively, any valid email address can also be entered in **Email to Recipients**.
- When scheduling more than one report, it is recommended that you select a different **Time of Day** to start each report. This will enhance performance.
- Text-formatted reports scheduled as email attachments are delivered in Excel format. Those scheduled as embedded are delivered as plain text files.

▶ To schedule a report:

1. From the CommCell Console, click the **Reports** icon.
2. Click a report from the **Reports** pane of the **Report Selection** dialog box.
3. From the report, select the appropriate filter options, and then click **Schedule**. The Select Users and Name dialog box is displayed.
4. If necessary, type a schedule name for the report in the **Schedule Name** field. Select the **Embedded** option if this report should be included in the body of the e-mail, or select the **Attachment** option if this report should be sent as an e-mail attachment. Select **Compress** if you want the report to be compressed to reduce the file size as an e-mail attachment. You can also move users and user groups from the **Available Users** list to the **Users to be Notified** list or specify any valid email address in **Email to Recipients**. Note the following:
 - A scheduled report can be configured to be sent via e-mail to user groups created from within the CommCell Console as well as external domain user groups. However, individual external domain users will not receive the report via e-mail if they have not previously logged on to the CommCell Console. Users (from the user groups created from within the CommCell Console) will receive the report e-mail regardless of their login status.
5. Click **OK**. The **Schedule Details** dialog box is displayed.
6. Make your selections in the Schedule Details (Schedule Details) dialog box.
7. To edit the report, from the **Job Summary** tab, click **Edit**.
8. From the Modifying Scheduled Report (General) dialog box, you can modify the schedule name of the report, modify the report mailing format such as embedded in an e-mail or as an e-mail attachment, and modify the users to be notified.
9. You can modify the report filter options, as necessary. From the **Modifying Scheduled Report (Detail)** tab, following the tabs and select the new filter options. Click **OK**.
10. Click **OK** to save your changes.
11. Click **Close**.

MODIFY A SCHEDULED REPORT

Required Capability: See Capabilities and Permitted Actions

▶ To modify a scheduled report:

1. From the CommCell Browser, right click the CommServe icon, then select **All Tasks -> Schedules**.
 2. From the Scheduled Jobs dialog box, select the report schedule you want to edit, then click **Edit**.
 3. From the **Job Summary** tab of the **Schedule Details** dialog box, click **Edit**.
 4. From the Modifying Scheduled Report (General) dialog box, modify the schedule name of the report in the **Name** field. you can modify the schedule name of the report, modify the report mailing format such as embedded in an e-mail or as an e-mail attachment, and modify the users and user groups to be notified.
 5. You can modify the report filter options, as necessary. From the **Modifying Scheduled Report (Detail)** tab, following the tabs and select the new filter options, as necessary. Click **OK**.
 6. Click **OK** to save your changes.
 7. Click **Close**.
-

[Back to Top](#)

Services

[Topics](#) | [How To](#) | [FAQs](#) | [Related Topics](#)

Overview

Service Dependencies

TCP Ports Used for Services

- Static Ports
- Dynamic Ports

Binding Services to Specific Network Interface Cards (NIC)

- CommServe Computers in Clustered Environments

Service Control

- Service Control for Windows
- Service Control on Windows Cluster
- Running Services Using a Windows User
- Service Control for Unix
- Service Control for NetWare
- Service Control for Content Indexing

GxAdmin Tool

OVERVIEW

Several services are required by the software to function. For example, all computer configurations minimally require the Base services to be running. CommServe services are installed exclusively on the CommServe computer, and MediaAgent services are installed exclusively on the MediaAgent computer. The following table describes the various CommCell components and the appropriate services that are required. Note that these services are automatically installed when the appropriate software is installed on the computer.

CommCell components	Service Group (as displayed in the Service Control Manager)	Service Name (as displayed in the Windows Local Services dialog box)	Service Name (as displayed in Windows Task Manager)	Description
Client only (any system)	Base services	Bull Calypso Client Event Manager	EvMgrC	Forwards events generated on the local machine to the CommServe. In addition it helps the CommServe to browse the application data on local machine.
		Bull Calypso Communications Service	CVD	Provides the ability to fetch or save metadata on the CommServe when data protection or data recovery operations are in progress.
CommServe only	Base services	Bull Calypso Server Event Manager	EvMgrS	Responsible for communicating with CommCell Console and receive the events from the Clients and/or MediaAgents.
		Bull Calypso Communications Service	CVD	Provides the ability to fetch or save metadata on the CommServe when data protection or data recovery operations are in progress.
	CommServe services	Bull Calypso Application Manager	AppMgrSvc	Provides access to server and client configuration for local and remote processes. This service is essential for the CommServe.
		Bull Calypso Job Manager	JobMgr	Responsible for running and controlling jobs and also communicate with the

				available resources.
		Bull Calypso Media & Library Manager	MediaManager	Responsible for controlling the hardware devices that are part of a CommCell.
		Bull Calypso Commands Manager	QSDK	Responsible for servicing command line requests and is therefore essential for command line operations.
		Bull Calypso Storage Resource Manager	SRMServer	Responsible for sending and receiving data to and from the SRM clients.
MediaAgent only	Base services	Bull Calypso Client Event Manager	EvMgrC	Forwards events generated on the local machine to the CommServe. In addition it helps the CommServe to browse the application data on local machine.
		Bull Calypso Communications Service	CVD	Provides the ability to fetch or save metadata on the CommServe when data protection or data recovery operations are in progress.
	MediaAgent services	Bull Calypso Media Mount Manager (GxMMM)	cvmountd	Responsible for interacting with the hardware devices that are attached to the local host and are part of the CommCell.
Migration Archiver Agents	DataArchiver Services	Bull Calypso HSM Recaller	CVMHSMService	Installed on clients with a Migration Archiver Agent. Responsible for archiving or recovering the files based on rules defined for the migration archiving operation.
ContinuousDataReplicator Agents	CDR Services	Bull Calypso Replication Service	CVRepSvc	Installed on Clients with ContinuousDataReplicator. Responsible for replicating data from one client computer to another client computer.
VSS Provider Agents	VSS Provider Service	Bull Calypso VSS Provider Service	VSS_SWPROV_SVC	Makes use of the Volume Shadow Service feature of the Windows Server 2003 operating system.
CommNet Server	CommNet Service	Bull Calypso Monitor Service	QNServer	Responsible for communicating with CommCells (including SRM) and the CommNet Browser for CommNet Server components.
Client only (non-CommServe Virtual Machines)	This service is not managed by the Service Control Manager. The Cluster Administrator must be used to control this service.	Bull Calypso Cluster Plugin	GxClusPlugin	Provides notification regarding whether or not the cluster group goes into an active or passive state. This service is essential for system functionality.
Client only	Data Archiver Services	Bull Calypso HSM NAS Recaller Service	GXSHMServiceNTAP	Recall files on a NAS Share.

For the Solaris File System *iDataAgent*, if the Bull Calypso Communications Service is on an IPv4-only stack (e.g., you do not have a local host IPv6 configured), be sure to do the following before you run a data protection operation:

1. Enable the IPv6 stack.
2. Change `nPreferredIFFamily` to 1 (i.e., force IPv4).
3. Remove or comment out `:::1` from `/etc/inet/ipnodes`.
4. Alter startup to run on just the local host IPv6. For example:

```

ifconfig lo0 inet6 plumb
route add -inet6 ::1/128 localhost
ifconfig lo0 inet6 up

```

SERVICE DEPENDENCIES

When a system has more than one CommCell component, the service dependencies are as follows:

Using the Service Control Manager to do the following:	Has the following effect:
Stop all services used by the system	Stops all services on that system.
Start all services used by the system	Starts all services on that system. If the DataArchiver agent is installed, starting all services starts the CVMHSM recaller service.
Stop the Base services	Stops all services on that system because all services depend on the Base services.
Start the Base services	Starts only the Base services. Restarting the other services can be done individually or by restarting all services simultaneously.
Stop the CommServe services	Stops only the CommServe services.
Start the CommServe services	Starts the Base and CommServe services.
Stop the MediaAgent services	Stops only the MediaAgent service.
Start the MediaAgent services	Starts the Base and the MediaAgent services.
Stop Data Archiver services	If the DataArchiver agent is installed, stopping this service stops the CVMHSM service for this agent.
Start Data Archiver services	If the DataArchiver agent is installed, starting this service starts the CVMHSM service for this agent.
Stop Data Classification services	If the Data Classification Enabler is installed, stopping this service stops the GXDCService (Windows) or DcSvc (Unix) and all child GxDC (Windows) processes for this enabler.
Start Data Classification services	If the Data Classification Enabler is installed, starting this service starts the GXDCService (Windows) or DcSvc (Unix) and all child GxDC processes for this enabler.
Stop CDR services	If ContinuousDataReplicator is installed, stopping this service stops the CVRepSvc Service for this agent.
Start CDR services	If ContinuousDataReplicator is installed, starting this service starts the CVRepSvc Service for this agent.
Stop VSS Provider Service	If the VSS Provider is installed, stopping this service stops the GxVSSProv Service for this agent.
Start VSS Provider Service	If VSS Provider is installed, starting this service starts the GxVSSProv Service for this agent.
Stop CommNet Service	If the CommNet Server is installed, stops the CommNet Service.
Start CommNet Service	If the CommNet Server is installed, starts the CommNet Service.

TCP PORTS USED FOR SERVICES

Base Services provide the key communications and control link between components. These services are assigned registered network port numbers and are identified in the `/Windows/System32/Drivers/etc/Services` file as Static Ports and Dynamic Ports.

STATIC PORTS

For types of static ports, see [Network TCP Port Requirements](#).

DYNAMIC PORTS

Cvd sessions also use free ports between 5000 and 32767 for communication during data protection and data recovery jobs. The system will dynamically assign a number of free ports to be used by each job to allow parallel data movement. The client, CommServe, and MediaAgent all send job related communications using that port number. Once the job is finished and no other job is pending, the dynamic ports are released.

For more information about ports used by the system, see [Network TCP Port Requirements](#).

BINDING SERVICES TO SPECIFIC NETWORK INTERFACE CARDS (NIC)

By default the system binds the services to all the available NICs. You can however, bind the services to a specific NIC using the steps described below. Note that this operation is not recommended for clustered computers. (In a clustered environment, failover will not work if the services are bound to a specific NIC.)

1. Create the sBindToInterface registry key on the computer and provide the host name or IP address of the interface to which all services should bind.
2. Stop and start the services.

(Note that the system also allows you to define the interface pairs for data transfer between any two computers. See Data Interface Pairs for more details.)

COMM SERVE COMPUTERS IN CLUSTERED ENVIRONMENTS

For CommServe computers in clustered environments, you can bind known-port services (such as CVD, EvMgrC, EvMgrS, and QSDK) to specific IP address and/or host names. Use the following steps to bind services using this feature.

1. Create the **IPsToBind.txt** file in the **<Install Directory>\Base** folder.
2. Add the IP address or the interface name associated with the NIC cards(s) that must be used.

There must be one entry per line, as shown in the following example:

```
123.45.67.895
interface1.company.com
```

3. Save the file and then stop and start the services.

Note that if the **IPsToBind.txt** file is created, at least one valid IP address must match the resolved IP address of the interface name provided or else services will not start.

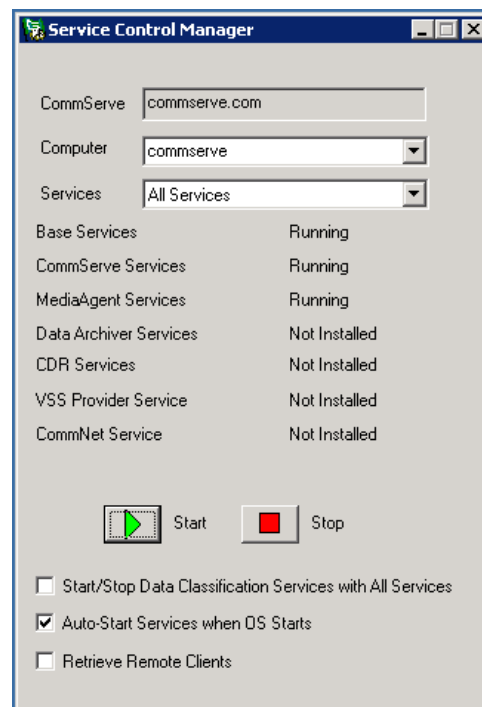
SERVICE CONTROL

SERVICE CONTROL FOR WINDOWS

The **Service Control Manager** can be used to stop and start services used by the system on Windows. Services on any Windows client computer within the CommCell can also be stopped and started remotely from another Windows client computer within the CommCell.

The **Service Control Manager** window includes the following fields:

Computer	The host computer of the services.
Services	Allows you to select either <i>All Services</i> , <i>Base Services</i> , <i>CommServe Services</i> , or <i>MediaAgent Services</i> . The <i>All Services</i> option starts (or stops) all services on the local computer, regardless of the components you have installed.
Base Services	Either stopped or running.
CommServe Services	Either stopped or running.
MediaAgent Services	Either stopped or running.
Data Archiver Services	Either stopped or running.
CDR Services	Either stopped or running.
VSS Provider Service	Either stopped or running.
CommNet Service	Either stopped or running.
Start/Stop Data Classification Services With All Services	If selected, and all services on the local computer are started (or stopped), then all Data Classification Enabler services will start (or stop) as well.
Auto-Start Services when OS Starts	If selected, all services applicable to the local system will start automatically when the system is started. If cleared, the services must be started manually.
Retrieve Remote Clients	If selected, the <i>Computer</i> field is populated with the names of all the remote Windows client computers within the CommCell. From this field you can remotely stop or start services from any selected Windows client computer within the <i>Computer</i> field. This feature is not support for Clients installed with an IP address, and Clients on Windows 64-bit computers.



If a client computer within the CommCell is running on a Windows Server 2008 Core Operating System, the **Service Control Manager** must be launched remotely from another Windows client computer within the CommCell. From the remote client computer, you will be able to start/stop services of the client.

SERVICE CONTROL ON WINDOWS CLUSTER

A clustered environment that is not a Windows cluster (VERITAS, Polyserve, etc.) requires that each physical node bind only to that node's specific IP address. Each physical node needs an IPSToBind.txt file in the Base directory. This will force the services on each node to bind to the node's IP address and not the virtual machine IP address. This is not necessary in a Windows clustered environment.

RUNNING SERVICES USING A WINDOWS USER

You can create a User (and not the local system account) to run services and operations only for the Windows File System iDataAgents and SQL Server iDataAgent. By default, services run as a local system account. The created User will run services to back up and restore files and folders regardless of ownership, permissions, encryption, or auditing settings.

The User will use several built-in groups, including Backup Operator, Administrator, and Local Administrator. These groups have the necessary permissions and user rights defined. Only a member of the Administrator group can assign users as Backup Operators.

Warning: You may be required to edit the registry. However, before you do this, back it up and ensure that you understand how to restore it if a problem occurs. For information about how to do this, view Windows Help on the "Restoring the Registry" from Microsoft Help topic in Regedit.exe or the "Restoring a Registry Key" Help topic in Regedt32.exe.

See User Accounts and Passwords: Considerations When Using a Windows User to Run Operations for more information along with the following procedures:

- View or Modify User Rights Assignments on a Workgroup or Member Server
- View or Modify User Rights Assignments on a Domain Controller
- Set up User Permissions and Rights on a Windows Workgroup or Member Server
- Set up Folder Permissions

SERVICE CONTROL FOR UNIX

The services can be stopped or started from a Unix system. However, only one instance of start/stop services at a time is allowed on the system. If you attempt more than one such instance, the appropriate error message is displayed. The following commands can be used to start and stop services:

The `-instance` option now refers to product installation instances. Such instances have an independent set of binaries, use different network ports, and may talk to different CommServes. Instances have nothing to do with virtual machines; they allow you to have two independent installations of the software on the same machine.

Command	Usage
<code>Calypso -all -instance <inst_name>[-force] start</code>	Brings up services on all configured instances (-all). The <code>-instance</code> switch can be used to start services on a specific instance only. The software will refuse to start if it detects partially installed patches. In such cases, you can either install the latest service pack or start the software with the <code>-force</code> option and use Automatic Update to push patches from the CommServe.
<code>Calypso -all -instance <inst_name> stop</code>	Stops services on all configured instances (-all). The <code>-instance</code> switch can be used to stop services on a specific instance only.
<code>Calypso -all -instance <inst_name> restart</code>	This is the same as "Stop" followed by "Start."
<code>Calypso -all -instance <inst_name> list</code>	Lists all running services on all instances or just <inst_name>.
<code>Calypso -all -instance <inst_name> status</code>	Provides information about the client installation and for all configured instances on the client. The <code>-instance</code> switch can be used to provide information for a specific instance only.
<code>Calypso -csname</code>	Displays the name of the CommServe and the instance. For a multi-instance installation, displays the name of all the affected CommServes and instances.
<code>Calypso help</code>	Displays this help message.

If services go down during a process (e.g. install, backup, etc.), the `Calypso start` command will not restart services unless the command is included in the crontab file. See Ensure Restarting of Services Using crontab for step-by-step instructions

SERVICE CONTROL FOR NETWARE

Services used by the system can be stopped or started from the NetWare Server using the Load/Unload commands, or from a remote Novell Client PC using the **NetWare Service Manager**.

The **NetWare Service Manager** window includes the following fields:

NW Servers	Allows you to select the name of the NetWare server for service control.
Services	Allows you to select either All Services, Base Services, or MediaAgent Services. The All Services option starts (or stops) all services on the local computer, regardless of the components you have installed.
Refresh Services	Allows you to refresh the selected services.

NLM Status

Displays the current status of the NetWare Loadable Module (NLM).



SERVICE CONTROL FOR CONTENT INDEXING

For information on controlling the services for Content Indexing, see Content Indexing Services.

GXADMIN TOOL

GxAdmin is a real-time CommCell administration tool used to view, monitor, and administer the various services and processes of the CommCell components on local and remote Windows computers.

This tool is available at the <Install Directory>/base folder, on Windows computers. The tool contains the following tabs:

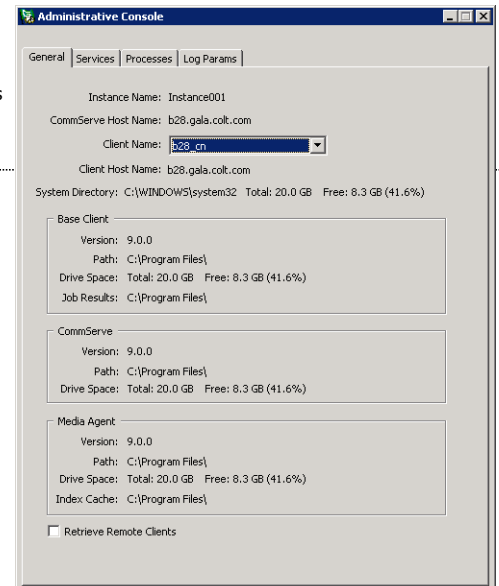
GENERAL

The general tab displays the CommCell deployment details such as Instance Name, CommServe Host Name, Client Name, and the Client Host Name. It also provides the configuration details of each CommCell component installed.

The following details are displayed:

- Software version
- Installation directory
- Total space and free space on the disk
- Job Results directory (for clients), Index Cache (for MediaAgents), and database details (for CommServe).

By default, details of the local client are displayed. You can also view the details of remote clients. See Use GxAdmin to View Remote Clients for instructions.



SERVICES

The services tab displays the list of services along with the instance name and the status of the service, for each CommCell component. The individual services can be managed. See Use GxAdmin to Start/Stop Services for step-by-step instructions.

PROCESSES

The processes tab displays the list of CommCell processes that are currently running. Process details such as start time, memory used, thread count, and handle count are displayed. The log details of the process can be stored in a dump file and used for troubleshooting purposes. See Use GxAdmin to Create Process Dump for step-by-step instructions.

LOG PARAMS

The Log Params tab displays the log parameter details such as the debug level, log file size, maximum log file version, and debug wait time, for each module. You can use the Log Params tab to configure log parameters. See Use GxAdmin to Set Log Parameters for instructions.

[Back To Top](#)

Services - How To

Topics | How To | FAQs | Related Topics

Start Services on Windows

Stop Services on Windows

Start Services on NetWare

Stop Services on NetWare

Access NetWare Service Manager from a Remote Novell Client

Start Services on Unix

Stop Services on Unix

Remotely Start or Stop Services on Windows Client Computers Within a CommCell

Access Service Control Manager from CommCell Console

Ensure Restarting of Services Using crontab

View or Modify User Rights Assignments on a Workgroup or Member Server

View or Modify User Rights Assignments on a Domain Controller

Set up User Permissions and Rights on a Windows Workgroup or Member Server

Set up Folder Permissions

Use GxAdmin to View Remote Clients

Use GxAdmin to Start/Stop Services

Use GxAdmin to Create Process Dump

Use GxAdmin to Set Log Parameters

START SERVICES ON WINDOWS

Before You Begin

All services used by the system start automatically when the appropriate computer is started or when the appropriate software is installed. If you want to manually start the services, disable the Auto-Start Services when OS Starts option from the **Service Control Manager** window (this option is enabled by default).

 To start the services on Windows:

1. Launch the **Service Control Manager** from the **Start | Programs** menu.
2. Select **All Services** from the **Services** field. Optionally, you can also select **Base Services**, **CommServe Services**, **CommNet Services**, or **MediaAgent Services**.
3. Click **Start** to restart the specific service(s). When the services are restarted successfully, the **Service Control Manager** window updates the status of the services you selected from **Stopped** to **Running**.

Optionally, you can verify which services were started by viewing them from the Windows **Services** window, available in the **Control Panel**.

4. Resume any jobs you suspended prior to stopping the services.
-

STOP SERVICES ON WINDOWS

Before You Begin

- Services used by the system must be running in order for data protection, data recovery operations, and all jobs to run properly. Generally, it is strongly recommended that you should leave all services running. Stopping these services should be avoided whenever possible.
- Use the Job Controller to verify that no jobs (data protection operations, data recovery operations, etc.) are in progress. If a job is in progress and in the Running or Waiting state, use the Job Controller to suspend or kill the job. Alternately, you can wait for the job to complete.
- Stopping either the CommServe services or the Base services will stop all operations that depend on that CommServe.
- When you stop services on a given system, the functions dependent upon the system's services will no longer be available to the rest of the CommServe.
- All services depend upon the Base services, therefore, stopping the base services stops all services.
- For the Windows 2000, Windows 2003, and Windows XP platforms, services will automatically recover if they are stopped unexpectedly. If the services stop unexpectedly, the services will attempt to restart every two minutes until they start successfully. While the Server Event Manager Service is restarting,

(either by a user restarting the service manually or by auto-recovery), the Job Manager Service and the Media and Library Manager service will also be restarted.

▶ To stop services on Windows:

1. Open the **Service Control Manager**. For more information, see Access Service Control Manager from CommCell Console.
2. Click the service you want to stop from the **Services** field.
3. By default, the **Auto-Start Services when OS Starts** option is selected, meaning that all services applicable to the local computer will start automatically when the computer is restarted.

If you want to start all services manually instead, clear this option (to disable the auto-start feature).

4. Click **Stop** to stop the specific service(s).

When the services are stopped successfully, the **Service Control Manager** window updates the **All Services** status from **Running** to **Stopped**.

Optionally, you can verify which services were stopped by viewing them from the Windows **Services** window.

START SERVICES ON NETWARE

▶ To start services on a NetWare system: **Start from Remote Novell Client PC**

1. Open the **Service Manager**. For more information, see Access Service Control Manager from CommCell Console.
2. Type in the name of the CommServe being accessed.
3. Press **Enter** to continue. This populates the NW Servers drop-down menu.
4. Select an NW Server.
5. Click **Start** to start the services. When the services are started successfully, the **Service Manager** window updates the status of the services you selected from **Stopped** to **Running**.

Start from NetWare Server

1. Run the following command from your local computer:

Load Galaxy

This should start the services.

2. Resume any jobs you suspended prior to stopping all services.
-

STOP SERVICES ON NETWARE

▶ To stop services on a NetWare system:

Stop from Remote Novell Client PC

1. Open the **Service Manager**. For more information, see Open Service Manager from Remote Novell Client PC.
2. Type in the name of the CommServe being accessed.
3. Press **Enter** to continue. This populates the NW Servers drop-down menu.
4. Select an NW Server.
5. Click **Stop** to stop the services. When the services are stopped successfully, the **Service Manager** window updates the status of the services you selected from **Running** to **Stopped**.

Stop from NetWare Server

Run the following command from your local computer:

Unload Galaxy

ACCESS NETWARE SERVICE MANAGER FROM A REMOTE NOVELL CLIENT

▶ To open the Service Manager from Remote Novell Client:

1. In the Novell Client computer, navigate to the **<install directory>\Base** folder.
2. Double-click **NWGalaxyscm.exe**.

The **NetWare Service Manager** window will be displayed.

START SERVICES ON UNIX

▶ To start services on Unix:

1. From a client computer, log on to the computer as **root**.
 2. At the command line prompt, type the **Calypso start** command.
 3. Press **ENTER**.
 4. Resume any jobs you suspended prior to stopping all services.
-

STOP SERVICES ON UNIX

▶ To stop services on Unix:

1. From a client computer, log on to the computer as **root**.
2. At the command line prompt, type the **Calypso stop** command.
3. Press **Enter**.

This should stop the services.

REMOTELY START OR STOP SERVICES ON WINDOWS CLIENT COMPUTERS WITHIN A COMMCELL

▶ To remotely start or stop services on Windows client computers within a CommCell:

1. Open the **Service Control Manager**. For more information, see Open Service Control Manager from CommCell Console.
2. Select **Retrieve Remote Clients**. The **Computer** field is automatically populated with the names of the Windows clients within the CommCell.
3. From the **Computer** field, select the client computer from which you want to stop or start the services.
4. Click **Stop** or **Start** to stop or restart the specific service(s). When the services are restarted successfully, the **Service Control Manager** window updates the status of the Base services from **Running** to **Stopped**, or from **Stopped** to **Running**.

Optionally, you can verify which the services on the remote computer that were started by viewing them from the Windows **Services** window.

ACCESS SERVICE CONTROL MANAGER FROM COMMCELL CONSOLE

Before You Begin

- To start the Service Control Manager using the CommCell Console, the CommCell Console must be accessed using a stand-alone or installed version of the CommCell Console.
- The Service Control Manager cannot be accessed from the CommCell Console when it is run as a Remote Web-Based Application.
- Another component such as a CommServe, MediaAgent or Agent software must also be installed on the computer.

▶ To open the Service Control Manager from the CommCell Console:

1. Open the CommCell Console as described in Run the CommCell Console as a Java Application.
2. From the CommCell Console, click **Tools > Service Control Manager**.

The Service Control Manager window is displayed.

ENSURE RESTARTING OF SERVICES USING CRONTAB

Before You Begin

- Please consult your operating system vendor manual for instructions on adding crontab entries.
- crontab entries must be made using the root user ID.

▶ To ensure restarting of services using the crontab file:

1. From the client computer, open the crontab file.
2. Type an entry that includes the appropriate install directory and command and that reflects how often you want to restart services. For example:

```
* 0-23 *** <software installation path>/Base/Calypso start
```

indicates that services will be checked every hour to see if a restart is necessary (which is recommended).

3. Save your file.
-

VIEW OR MODIFY USER RIGHTS ASSIGNMENTS ON A WORKGROUP OR MEMBER SERVER

▶ To view or modify user rights assignments on a Workgroup or Member Server:

1. Click **Start > Settings > Control Panel > Administrative Tools**.
 2. From **Administrative Tools**, select the local security policy and add the Service user to all the required rights (logon as service, backup, restore).
-

VIEW OR MODIFY USER RIGHTS ASSIGNMENTS ON A DOMAIN CONTROLLER

▶ To view or modify user rights assignments on a domain controller:

1. Click **Start > Settings > Control Panel > Administrative Tools**.
 2. From **Administrative Tools\Domain Controller Security Policy**, expand the tree to **Security Settings, Local Policies, and User Rights Assignment**. Add the user to all the required rights (logon as service, backup, restore).
-

SET UP USER PERMISSIONS AND RIGHTS ON A WINDOWS WORKGROUP OR MEMBER SERVER

▶ To set up user permissions and rights on a Windows Workgroup or Member Server:

1. Click **Start > Settings > Control Panel > Administrative Tools**.
 2. From **Administrative Tools**, double-click **Computer Management**.
 3. Create or prepare to manage a Windows user who will run the services.
 4. Open Computer Management by expanding **Local User and Groups** and then **Users**. Double-click or create the User who will be running the services.
 5. Right-click the User (if new), click **Properties**, and click **Member of**. Then add the Backup Operators group to the User.
 6. Change the services account to the User and re-start the services.
 7. Log off and log in as the Administrator for the policies to take effect. Sometimes you may have to restart the computer to this end.
-

SET UP FOLDER PERMISSIONS

▶ To set up folder permissions:

1. As appropriate, provide the service user with full control to the installation directory or confirm that such control is in place. The default location is `C:\Program Files\Company Name`.
 2. Right-click, select **Properties**, and then select the **Security tab** and **Add Backup Operators** (or the service user) with full control rights.
-

USE GXADMIN TO VIEW REMOTE CLIENTS

▶ To view details of clients installed in remote computers using GxAdmin tool:

1. On Windows clients, navigate to the **<install directory>\Base** folder.
2. Double-click **GxAdmin.exe**. The **GxAdmin Tool, General** tab is displayed.
3. Select the **Retrieve Remote Clients** field. The remote clients connected to the CommCell will list will be listed in the **Client Name** field.
4. Select the desired client name from the **Client Name** list.
5. The details of the CommCell components installed in the remote client are displayed.

USE GXADMIN TO START/STOP SERVICES

▶ To start/stop the CommCell services using GxAdmin tool:

1. On Windows clients, navigate to the **<install directory>\Base** folder.

2. Double-click **GxAdmin.exe**. The **GxAdmin Tool** is displayed.
 3. Select the **Services** tab. The component services and the individual services are displayed.
 4. Select the desired service, right-click and select Start/Stop/Restart as required.
-

USE GXADMIN TO CREATE PROCESS DUMP

▶ To create a process dump using GxAdmin tool:

1. On Windows clients, navigate to the **<install directory>\Base** folder.
 2. Double-click **GxAdmin.exe**. The **GxAdmin Tool** is displayed.
 3. Select the **Processes** tab. The various processes running and their details are listed.
 4. Select the desired process and right-click.
 - Select **Dump** to create a dump file containing the process details. The process dump, a `.dump` file with the filename containing the process name with the timestamp information appended, is created in `<Install Directory>\Log Files` folder.
 - Select **Kill** to kill the process.
 - Select **View Logs** to view the process log.
-

USE GXADMIN TO SET LOG PARAMETERS

▶ To set log parameters using GxAdmin tool:

1. On Windows clients, navigate to the **<install directory>\Base** folder.
 2. Double-click **GxAdmin.exe**. The **GxAdmin Tool** is displayed.
 3. Select the **Log Params** tab. The log settings for the various modules are displayed.
 4. To modify a parameter, double-click the corresponding cell and edit the value.
 5. Click **OK** to save the changes.
-

[Back to Top](#)

Audit Trail

Topics | How To

Overview

Severity Levels

Operations Recorded by Audit Trail

Related Reports

OVERVIEW

The Audit Trail feature allows you to track the operations of users who have access to the CommCell. This capability is useful if a detrimental operation was performed in the CommCell and the source of that operation needs to be determined.

Audit Trail records are retained for a specific period of time (in days) based on the severity level selected. Outlined below are the default retention timeframes for each severity level:

- Critical: Records are retained for 365 days
- High: Records are retained for 365 days
- Medium: Records are retained for 240 days
- Low: Records are retained for 120 days

You can adjust the retention timeframe based on each severity level using the Audit Trail dialog box. To access the Audit Trail dialog box, use the Control Panel from the **Tools** menu on the CommCell Console. After the retention time has expired, the data will be pruned when data aging is run. (See Data Aging for more information.)

See Configure Audit Trail Retention for step-by-step instructions on configuring Audit Trail retention.

SEVERITY LEVELS

Operations performed within the CommCell are grouped into four severity levels. Each level has pre-classified operations associated with it. These levels, as well as examples of operations that fall within them, are described in the following sections.

CRITICAL

This level records operations that will result in imminent loss of data. Some examples of operations that fall into this severity level are:

- Deleting a backup set
- Deconfiguring an Agent
- Performing an erase media operation.

When this severity level is selected for the GUI Audit Trail Report, only Severity Level Critical operations will be included.

HIGH

This level records operations that may result in loss of data. Some examples of operations that fall into this severity level are:

- Changing client encryption properties
- Changing media management configuration
- Creating a subclient (may result in data loss if no schedules are created)

When this severity level is selected for the GUI Audit Trail Report, Severity Level Critical and High operations will be included.

MEDIUM

This level records changes to the general configuration of one or more entities. Such changes may produce unintended results when operations are performed. Some examples of operations that fall into this severity level are:

- Changing the name of a storage policy
- Exporting media
- Killing a job

When this severity level is selected for the GUI Audit Trail Report, Severity Level Critical, High, and Medium operations will be included.

LOW

This level records changes to status, addition of entities, and other operations that have minimal impact on existing CommCell functions. Some examples of operations that fall into this severity level are:

- Compliance searches
- Setting container information for VaultTracker actions
- Quick library scans

When this severity level is selected for the GUI Audit Trail Report, operations for all severity levels will be included.

OPERATIONS RECORDED BY AUDIT TRAIL

The following table lists the operations that are recorded at each severity level:

SEVERITY LEVEL	OPERATION
Critical	Abort Media in VaultTracker Action
Critical	Change Client CommServe Host Name
Critical	Change Client Host Name
Critical	Change Client Name
Critical	Change SharePoint Archiver Prune Settings
Critical	Deconfigure a Storage Node in Library and Drive Config Tool
Critical	Delete a Client Group
Critical	Delete a Library
Critical	Delete a Mount Path
Critical	Delete Backup Set
Critical	Delete Client from Content Indexing Engine
Critical	Delete Content Director Legal Hold
Critical	Delete Content Director Policy
Critical	Delete Content Director Record Center
Critical	Delete Content Director Search
Critical	Delete Content Director Tag
Critical	Delete Content Index for Job
Critical	Delete Content Indexing Engine
Critical	Delete Content Indexing for Storage Policy
Critical	Delete Custom Calendar
Critical	Delete Deduplication for Storage Policy Copy
Critical	Delete Disk Media Content
Critical	Delete ERM Connector
Critical	Delete Export Location
Critical	Delete History of VaultTracker Action
Critical	Delete Iron Mountain Customer ID
Critical	Delete Media
Critical	Delete Media Container
Critical	Delete Media Contents and Move Media
Critical	Delete Replication Policy
Critical	Delete Replication Set
Critical	Delete Schedule
Critical	Delete Schedule Policy
Critical	Delete Snapshot
Critical	Delete Spare Group
Critical	Delete Storage Policy
Critical	Delete Storage Policy Copy
Critical	Delete User
Critical	Delete User group
Critical	Delete VaultTracker Policy
Critical	Deleted Filer Management
Critical	Disable Backups for Storage Policy Copy
Critical	Disallow Copy Jobs in Media
Critical	Erase Backup Data
Critical	Erase Media
Critical	Execute QScript
Critical	Export and Delete Media
Critical	Failed Login

Critical	Force Deconfigure a client
Critical	Force Deconfigure a MediaAgent
Critical	Force Deconfigure an Agent
Critical	Full Erase Media
Critical	Full Erase Media in Library
Critical	Hard Delete Client
Critical	Hard Delete iDataAgent
Critical	Job Based Pruning
Critical	Kill All Jobs
Critical	Mark Recall Done for Media in VaultTracker Action
Critical	Move Media between Libraries
Critical	Oracle RMAN Cross-Check Disabled
Critical	Oracle RMAN Cross-Check Enabled
Critical	Quick Erase Media
Critical	Quick Erase Media in Library
Critical	Recall Media
Critical	Remove Deduplication Access Path
Critical	Revert Snapshot
Critical	Update Custom Calendar
Critical	Update Storage Policy Copy Properties
High	A SCSI2 reservation release was attempted for a drive but failed.
High	Add New User
High	Add New User Group
High	Allow Export
High	Allow Recopy Data in Media
High	Allow Recopy Job
High	Change Network Password
High	Change Storage Policy Copy Data Path
High	Change Subclient Content
High	Control Services
High	Create Subclient
High	Deconfigure Instance
High	Delete Instance
High	Delete Replication Pair
High	Delete Snap Volume Unit
High	Delete Subclient
High	Delete Subclient Policy
High	Delete Workflow
High	Deleted Schedule Holiday
High	Disable Schedule Policy
High	Disallow Content Indexing for Jobs
High	Do Not Retain Job
High	Execute QScript
High	Migrate Disk Library
High	Reach Destination for Media in VaultTracker Action
High	Reassociate Bulk Subclients
High	Reassociate Individual Subclients
High	Reassociate Subset of Subclients
High	Resume Export for Media in VaultTracker Action
High	Return Media in VaultTracker Action to Source
High	Rollback History of VaultTracker Action
High	Scheduled job ran
High	Suspend Export for Media in VaultTracker Action
High	Tape Catalog Merge
High	Update Activity Control
High	Update Client Encryption Properties
High	Update Content Indexing Properties for Storage Policy
High	Update Deduplication Access Path
High	Update Instance Properties
High	Update Library Properties
High	Update Storage Policy Properties
High	Update Subclient Properties
High	Update User Group properties
High	Update VaultTracker Policy
High	User group Enable/Disable
High	Web service Failure Login
Medium	Add a Deduplication Access Path
Medium	

	Add a Mount Path
Medium	Add Blind Media
Medium	Add Custom Calendar
Medium	Add Media Barcode Pattern
Medium	Add New Media Container
Medium	Add Operation Window
Medium	Add Snap Volume Unit
Medium	Add Spare Group
Medium	Add Subclient Policy
Medium	Add Workflow
Medium	Allow Content Indexing for Jobs
Medium	Allow Copy Job
Medium	Allow Copy Jobs in Media
Medium	Change Index Cache Retention Days
Medium	Change Media Barcode Pattern
Medium	Change SAN Switch
Medium	Change Storage Policy Copy Precedence
Medium	Change Storage Policy Properties for Moving Snapshots to Backup Media.
Medium	Change Subclient Post-Command
Medium	Change Subclient Pre-Command
Medium	Change the Host for a Storage Node in Library and Drive Config Tool
Medium	Change Threshold for Drive Maintenance
Medium	Change Threshold for Library
Medium	Change Threshold for Media Expiration
Medium	Changed Filer Management
Medium	Changed Schedule Holiday
Medium	Client Configuration Policy Modified
Medium	Clone Content Director Legal Hold
Medium	Clone Content Director Policy
Medium	Clone Content Director Record Center
Medium	Clone Content Director Search
Medium	Clone Content Director Tag
Medium	Clone ERM Connector
Medium	Clone Storage Policy
Medium	Clone Subclient Policy
Medium	Configure a Storage Node in Library and Drive Config Tool
Medium	Configure the Whole Storage Node in Library and Drive Config Tool
Medium	Create Content Director Legal Hold
Medium	Create Content Director Policy
Medium	Create Content Director Record Center
Medium	Create Content Director Search
Medium	Create Content Director Tag
Medium	Create Content Indexing for Storage Policy
Medium	Create ERM Connector
Medium	Create New Backup set
Medium	Create New Instance
Medium	Create Schedule
Medium	Create Schedule Policy
Medium	Create Storage Policy
Medium	Create Storage Policy Copy
Medium	Create Subclient
Medium	Created Filer Management
Medium	Created Schedule Holiday
Medium	Delete Media Barcode Pattern
Medium	Delete Operation Window
Medium	Description modified
Medium	Disable Content Director Legal Hold
Medium	Disable Content Director Policy
Medium	Disable Content Director Record Center
Medium	Disable Content Director Search
Medium	Disable Content Director Tag
Medium	Disable Deduplication Access Path
Medium	Disable ERM Connector
Medium	Disable Schedule
Medium	Discover Media
Medium	Drive Cleaned
Medium	Drive Replaced
Medium	

	Enable Content Director Legal Hold
Medium	Enable Content Director Policy
Medium	Enable Content Director Record Center
Medium	Enable Content Director Search
Medium	Enable Content Director Tag
Medium	Enable Deduplication Access Path
Medium	Enable ERM Connector
Medium	Enable Schedule
Medium	Enable Schedule Policy
Medium	Execute QScript
Medium	Execute QScript
Medium	Export Media
Medium	Export Media from Library
Medium	Export Media from Library through VaultTracker
Medium	Export Media through VaultTracker
Medium	Kill Job
Medium	Mark Media Bad
Medium	Mark Media from Foreign CommCell Reusable
Medium	Mark Media Full
Medium	Mark Media Good
Medium	Mark Partial Full
Medium	Mark Volume Full for Storage Policy Copy
Medium	Media Reuse Allowed
Medium	Media Reuse Prevented
Medium	Migrate Media
Medium	Modify MediaAgent properties
Medium	Mount Snapshot
Medium	Move All Media to Spare Group
Medium	Move Number of Media to Spare Group
Medium	On Demand Failover for Storage Policy Copy
Medium	Pick Job for Data Verification
Medium	Pick Job for Moving Snapshots to Backup Media
Medium	Pick up Media in VaultTracker Action
Medium	Prevent Export
Medium	Rename Snap Volume Unit
Medium	Rename Spare Group
Medium	Rename Subclient
Medium	Rename Subclient Policy
Medium	Rename Workflow
Medium	Replace a Storage Node in Library and Drive Config Tool
Medium	Retain Job
Medium	Security Name Server Settings
Medium	Unmount Snapshot
Medium	Unpick Job for Moving Snapshots to Backup Media
Medium	Update Application properties
Medium	Update Backup set properties
Medium	Update Backup Set Properties
Medium	Update Client properties
Medium	Update Client properties - Client group association
Medium	Update Content Director Legal Hold
Medium	Update Content Director Policy
Medium	Update Content Director Record Center
Medium	Update Content Director Search
Medium	Update Content Director Tag
Medium	Update Deduplication Properties
Medium	Update ERM Connector
Medium	Update Export Location
Medium	Update Instance properties
Medium	Update Iron Mountain Customer ID
Medium	Update Media Container
Medium	Update Media Management Configuration Parameter
Medium	Update Media Properties
Medium	Update Operation Window
Medium	Update Schedule
Medium	Update Schedule Policy
Medium	Update Snap Volume Unit
Medium	Update Spare Group Properties
Medium	

	Update Subclient Policy
Medium	Update Subclient properties
Medium	Update User
Medium	Update User group association
Medium	Update Workflow
Medium	User Login
Medium	User Logout
Medium	Verify Media
Low	A SCSI2 reservation was released for a drive, and the reservation release was successful.
Low	Add Export Location
Low	Add Iron Mountain Customer ID
Low	Add Media Container
Low	Annotation
Low	Blind Media Full Inventory
Low	Blind Media Quick Inventory
Low	Compliance Search
Low	Download Item
Low	Dummy Operation - please replace
Low	ERM Submission
Low	Execute QScript
Low	Export Client Pass Phrase
Low	Full Library Scan
Low	Legal Hold Item
Low	Mark Drive Fixed
Low	Mark Media Exported
Low	Media Catalog
Low	Quick Library Scan
Low	Reset Client Pass Phrase
Low	Restore process
Low	ReviewSet Operation
Low	Set Container for Media in VaultTracker Action
Low	Tagging
Low	Web service User Login

RELATED REPORTS

GUI AUDIT TRAIL REPORT

The GUI Audit Trail Report provides a list of operations that were performed in the CommCell based on the selected severity level.

[Back to Top](#)

Audit Trail - How To

[Topics](#) | [How To](#)

CONFIGURE AUDIT TRAIL RETENTION

Required Capability: See Capabilities and Permitted Actions.

▶ To set the Audit Trail:

1. From the **Tools** menu in the CommCell Console, click **Control Panel**, and then select **Audit Trail**.
2. From the Audit Trail dialog box, select the desired retention time (in days) for each severity level.

The default retention times for each severity level are as follows:

- Severity Level 1: Records are retained for 365 days
 - Severity Level 2: Records are retained for 365 days
 - Severity Level 3: Records are retained for 240 days
 - Severity Level 4: Records are retained 120 days
3. Click **OK**.

Log Files

Topics | How To | Support | Related Topics

Overview

View Log Files

- View Log Files From a CommServe, SRM Server, MediaAgent, or Client
- View the Log Files of an Active Job
- View the Log Files of a Job in a Job History Window

Send Log Files

- Send Log Files from the CommCell Console
- Send Log Files from the Command Line
- Send Log Files via FTP or HTTP
- Set the Maximum Size for Email Bundles
- Send Log Files from the Workstation Backup Agent Client Console

Customize Log Files

- Setting the Maximum Size of Log Files
 - Setting the Maximum Number of Backup Log Files
 - Setting the Maximum Size of Media Manager Log Files
 - Setting the File Format for sending the Log Files
 - Enabling Passive FTP Connection
 - Setting the Timeout Value for Sending Log Files via FTP
 - Changing the Location of Log Files
-

OVERVIEW

Log files provide the processing details of operations that have occurred on your system.

The software allows you to view and send these log files from the CommCell Console stand-alone or remote web-based applications. You can also send log files from the Command Line or upload them to an existing FTP server.

The maximum default size of the log files is 5 MB. When the maximum size is reached, the file is rolled over to <filename>_1.log. You change the maximum default size of the log files by using the `NMaxLogFileSize` registry key.

Note that the dates and times of the log files pertaining to CommServe and SRM Server services are not updated until these services are stopped and restarted, even if the log files are updated in the interim. These log files are:

- CVD.log
- EvMgrS.log
- JobManager.log
- MediaManager.log
- CVMA.log


In addition to log files, there are other ways you can obtain information about conditions within the CommCell, such as from configured Alerts, or by events reported in the Event Viewer.

If necessary the Send Log Files option can be used to send the firewall configuration files.

VIEW LOG FILES

The **View Log Files** feature allows you to view log files from the CommCell Console for any of the following:

- A CommServe, SRM Server, MediaAgent, or client.
- An active job in the Job Controller.
- A job in a job history window.

 In a cluster, the log files reside on the physical computer that is the active node. If a failover has occurred, **View Log Files** will only show the logs of the current active node, and thus, only processing details of operations that occurred



after the failover; **Send Log Files** will collect *all* cluster log files from passive nodes as well, and thus, processing details of operations that occurred before the failover.

The following sections describe the methods with which you can view log files:

VIEW LOG FILES FROM A COMMSERVE, SRM SERVER, MEDIAAGENT, OR CLIENT

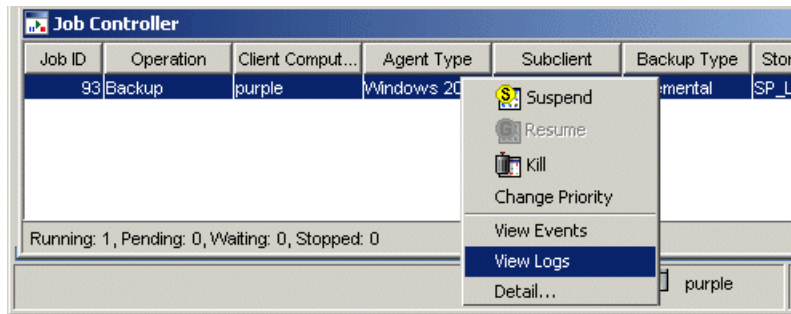
Use the **View Log Files** option to view the log files of a selected CommCell resource.

The log files that reside on a given computer may differ depending on the role of the computer in the CommCell (CommServe, SRM Server, MediaAgent, Client). A CommServe computer contains only the CommServe log files. A computer that is both a CommServe and a Client contains the log files of both entities.

For step-by-step instructions, see [View the Log Files of a CommServe, SRM Server, MediaAgent, or Client Computer](#).

VIEW THE LOG FILES OF AN ACTIVE JOB

You can view the log files of an active job in the Job Controller by using the **View Logs** option.



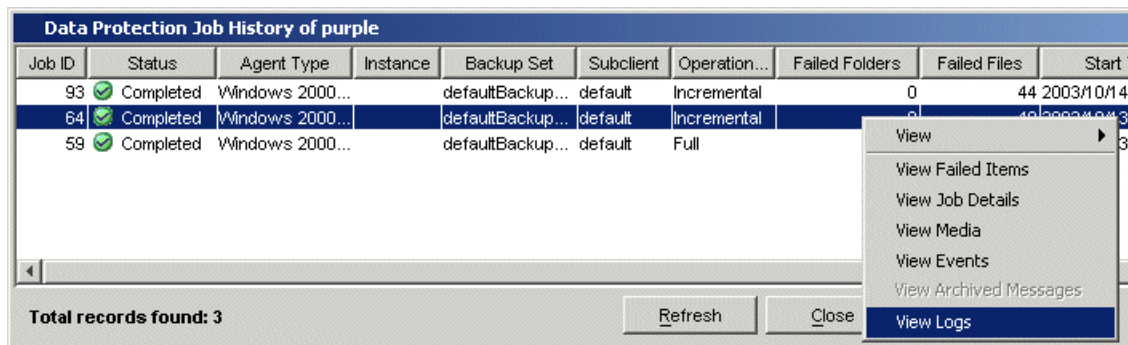
Once the **View Logs** option is selected, the log files related to the active job is displayed in the **View Log File for Job n** window. You can also send the log files by page to an email recipient by selecting the **Send Page** option in the **View Log File for Job n** window and entering the email recipient's SMTP Parameters.

For step-by-step instructions, see [View the Log Files of an Active Job](#).

For more information on the Job Management feature, specifically for active jobs, see [Job Management](#).

VIEW THE LOG FILES OF A JOB IN A JOB HISTORY WINDOW

You can view the log files of a job in a Job History window by using the **View Logs** option. Note that the following example illustrates a Data Protection Job History window.



Once the **View Logs** option is selected, the log files related to the job history is displayed in the **View Log File for Job n** window.

For step-by-step instructions, see [View the Log Files of a Job History](#).

For more information on the Job History feature, see [Job History](#).

SEND LOG FILES

The **Send Log Files** feature allows you to send or save log files by:

- Emailing the log files to one or more email recipients.

- Uploading the log files to an existing FTP server.
- Saving the log files to a specified location on the CommServe computer.

If a particular job spans into multiple log files, the logs will only be retrieved from the most current log file and the previously saved log file, e.g., `JobManager.log` and `JobManager_1.log`.



- In a cluster, the log files reside on the physical computer that is the active node. If a failover has occurred, **Send Log Files** will collect *all* cluster log files from passive nodes as well, and thus, processing details of operations that occurred while other physical computers served as the active node.
- Log files can be configured to be sent via e-mail to user groups created from within the CommCell Console as well as external domain user groups.

The following sections describe the methods with which you can send or save log files:

SEND LOG FILES FROM THE COMMCELL CONSOLE

Log files can be sent or saved from the CommCell Console using the **Send Log Files** dialog box.

You can send or save several types of log files from one or more computer(s), including:

- CommCell Information, which can include the CommServe database logs, SRM database logs, or SQL database logs.
- Computer Information, which can include either the log files for a specific job run within the CommCell, or the log files for all jobs run on the selected CommCell computer(s).
- Machine Information, which can include file system and application state logs, as well as information on commands and system failures.
- Log files created during a specified Time Range.

By default, prior to sending or saving log files, all the selected log files are automatically bundled into a `.cab` file. If you want, you can save or send these logs files in the `.zip` file format by using the `bSendLogUseZIP` registry key. For setting the file format for the log files that you want to send or save, see [Setting the File Format for sending the Log Files](#).

Before sending an email, you must set-up the email server within the CommCell Console. See [E-Mail Server Configuration](#) for more information.

For step-by-step instructions, see the following procedures:

- [Send Log Files](#)
- [Send Log Files To a Remote Computer](#)

SEND LOG FILES FROM THE COMMAND LINE

Log files can be sent from the command line by using the `sendLogFiles.exe` utility located in the `<software installation path>\Base` folder. The log files are sent to the specified recipient e-mail address or stored on a local directory on the CommServe computer in a `.cab` file (`*.cab`).

If you want, you can save or send these logs files in the `.zip` file format by using the `bSendLogUseZIP` registry key. For more information, see [Setting the File Format for sending the Log Files](#).

You can choose to send log files at the command line using one of two methods:

- Manually entering each command at the command prompt. This option is useful if you wish to use a set of commands that you might not otherwise use on a frequent basis.
- Creating an input file containing all the commands in either `.txt` or `.doc` formats. This option is useful if you routinely send log files using a set of commands that differ only slightly from one send log files operation to another.

You can also create custom commands that can collect additional information during all Send Log Files operations.

For command line usage and arguments, see [Command Line Interface - Send Log Files](#).

SEND LOG FILES VIA FTP OR HTTP

Log files can be sent to an existing FTP or HTTP server using either of the following methods:

- From the Command Line (FTP only) (see [Command Line Interface - Send Log Files](#) for step-by-step instructions).
- From the **Send Log Files** dialog box in the CommCell Console (see [Send Log Files](#) for step-by-step instructions).

To configure FTP or HTTP settings for sending log files, you can use the **Troubleshooting Settings** dialog box located in the CommCell Console's **Control Panel**. This dialog box is also accessible through the **Settings** button found in the **Send Log Files** dialog box. For step-by-step instructions, see [Configure Troubleshooting Settings](#).

SET THE MAXIMUM SIZE FOR EMAIL BUNDLES

Log file bundles may exceed the maximum allowed size for some email servers. In such cases, the software provides the capability to send the log file bundles to the designated recipient using multiple emails. If a bundle exceeds the maximum allowed size, a separate email with the remainder of the bundle will be sent to the designated recipient.

Once the recipient saves the log files to disk, the log files can be concatenated into their original form by performing the following steps:

1. From the command line, enter the following:

```
copy /B <source_directory>\<log_file_01_name> + <source_directory>\<log_file_02_name> /B c:\<concatinated_log_file_name>.CAB
```

2. Open <concatinated_log_file_name>.CAB using WinZip.

For step-by-step instructions on setting the maximum size for email bundles, see Set the Maximum Size for Email Bundles.

SEND LOG FILES FROM THE WORKSTATION BACKUP AGENT CLIENT CONSOLE

Workstation Backup clients send log files using the **Send Logs** option from the Client Console. See Send Log Files from the Workstation Backup Client Console for step-by-step instructions. By default the log files are sent to the <software Installation Path>\Log Files\WBALogs\<Client Name> folder on the CommServe computer.

The log files can also be directed to an existing FTP server. See Configure FTP Settings for Workstation Backup Clients for step-by-step instructions.

CUSTOMIZE LOG FILES

A log file can be customized to replace words of a log file with custom-defined words. The words to be replaced and their substitutes are defined in a simple text file called a dictionary file.

The ScrubLogFiles utility in the Resource Pack takes this dictionary file as input along with the input file specification and the output folder in which it is to place the modified files. For each file in the input file specification, it replaces the words defined in the dictionary file.

SETTING THE MAXIMUM SIZE OF LOG FILES

This registry key defines the maximum size of a specific log file. The size of the log file is measured in megabytes (MB). If the size of the file is greater than the value in the registry key, an additional log file is created with the name, <filename>_1.log.

To create this registry key:

1. From the **CommCell Browser**, expand **Client Computers**.
2. Right-click the <Client> in which you want to add the registry key, and then click **Properties**.
3. Click the **Registry Key Settings** tab.
4. Click **Add**.
5. On Windows in the **Name** box, type <logfile>_MaxLogFileSize. On UNIX in the **Name** box, type <logfile>_MAXLOGFILEZIE
6. In the **Location** list, type one of the following:
 - o On a Windows computer, type HKEY_LOCAL_MACHINE\Software\CommVault Systems\Galaxy\Instance<xxx>\EventManager.
 - o On a UNIX computer, type /etc/CommVaultRegistry/Galaxy/Instance<xxx>/EventManager/.properties.
7. In the **Type** list, select **REG_DWORD**.
8. In the **Value** box, enter a numeric value between 10 and 50, and then click **OK**.

The registry key appears in the list on the **Registry Key Settings** tab.

9. In the **Client Computer Properties** dialog box, click **OK**.

For more information, see the entry in Registry Keys.

SETTING THE MAXIMUM NUMBER OF BACKUP LOG FILES

This registry key defines the maximum number files that can be created for a specific backup log file.

1. From the **CommCell Browser**, expand **Client Computers**.
2. Right-click the <Client> in which you want to add the registry key, and then click **Properties**.
3. Click the **Registry Key Settings** tab.
4. Click **Add**.
5. On Windows in the **Name** box, type <logfile>_MaxLogFileBackups. On UNIX in the **Name** box, type <logfile>_MAXLOGFILEBACKUPS.
6. In the **Location** list, type one of the following:
 - o On a Windows computer, type HKEY_LOCAL_MACHINE\Software\CommVault Systems\Galaxy\Instance<xxx>\EventManager.
 - o On a UNIX computer, type /etc/CommVaultRegistry/Galaxy/Instance<xxx>/EventManager/.properties.

7. In the **Type** list, select **REG_DWORD**.
8. In the **Value** box, enter a numeric value between 10 and 50, and then click **OK**.

The registry key appears in the list on the **Registry Key Settings** tab.

9. In the **Client Computer Properties** dialog box, click **OK**.

For more information, see the entry in Registry Keys.

SETTING THE MAXIMUM SIZE OF MEDIA MANAGER LOG FILES

Use the following steps to set the maximum size of the **MediaManager** log file and the number of log files to retain

1. Navigate to **C:\Program Files\Bull Calypso\Calypso\Base** folder
2. Double-click the **SetLogParamsGUI** file.
3. Click the **CommServe** tab.
4. Under **Applications**, select the **MediaManager** checkbox and modify the following log parameters:
 - o **LogFileSize(MB)** - to set the maximum size for Media Manager log files.
 - o **LogFileMaxVer** - to set the maximum number of Media Manager log files to retain.

SETTING THE FILE FORMAT FOR SENDING THE LOG FILES

By default, prior to sending or saving log files, all the selected log files are automatically bundled into a single **.cab** file. If you want, you can send or save these log files in the **.zip** file format.

Use the following steps for setting the file format for sending and saving log files in **.zip** file format.

1. From the **CommCell Browser**, expand **Client Computers**.
2. Right-click the **<Client>** on which the CommServe resides, and then click **Properties**.
3. Click the **Registry Key Settings** tab.
4. Click **Add**.
5. In the **Name** box, type **bSendLogUseZIP**.
6. In the **Location** list, type or select **Commserve**.
7. In the **Type** list, select **REG_DWORD**.
8. In the **Value** box, type **0**.
9. The registry key appears in the list on the **Registry Key Settings** tab.
10. Click **OK**.

ENABLING PASSIVE FTP CONNECTION

If you are using FTP server to upload the log files, by default, the client connects to the Server through port 21 of the Server. However, you can enable a passive FTP connection, wherein the client first receives the port number to be used for connection from the Server and then connects to the Server using the specific port number.

Use the following steps to enable passive FTP connection:

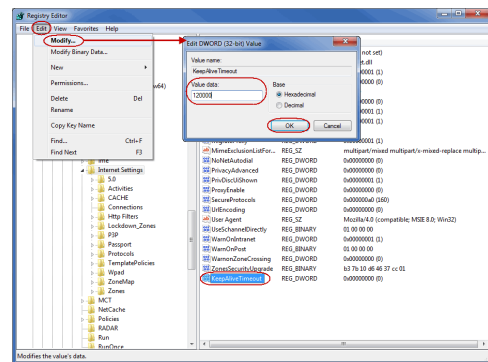
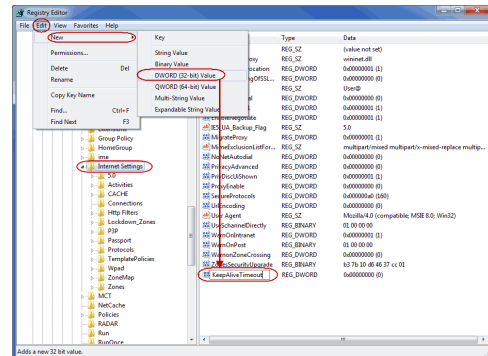
1. From the **CommCell Browser**, expand **Client Computers**.
2. Right-click the **<Client>** on which the CommServe resides, and then click **Properties**.
3. Click the **Registry Key Settings** tab.
4. Click **Add**.
5. In the **Name** box, type **nFTPPASSIVEFLAG**.
6. In the **Location** list, type or select **Commserve**.
7. In the **Type** list, select **REG_DWORD**.
8. In the **Value** box, type **1**.
9. The registry key appears in the list on the **Registry Key Settings** tab.
10. Click **OK**.

SETTING THE TIMEOUT VALUE FOR SENDING LOG FILES VIA FTP

Because sending large log files via FTP can take a long time, the operation sometimes times out. You can set the `KeepAliveTimeout` registry key to specify the timeout length in milliseconds. For more information, see the entry in Registry Keys.

To set the timeout length for FTP uploads:

1. Open Registry Editor (Regedit.exe or Regedt32.exe).
2. Expand **HKEY_CURRENT_USER > Software > Microsoft > Windows > CurrentVersion**, and then click **InternetSettings**.
3. Click the **Edit** menu, point to **New**, and then select **DWORD Value**.
4. Enter **KeepAliveTimeout** as the registry key name, and then press **ENTER**.
5. Select the **KeepAliveTimeout** registry key, click the **Edit** menu, and then select **Modify**.
The Edit DWORD Value dialog box appears.
6. In the **Value data** box, enter the amount of time, in milliseconds, that you want to wait before the upload times out.
For example, if you want the upload to time out after 2 minutes, enter 120000.
7. Click **OK** to save your settings.



CHANGING THE LOCATION OF LOG FILES

You can change the location in which log files are saved with the `dEVLOGDIR` registry key. For more information, see the entry in Registry Keys.

To change the location in which log files are saved:

1. From the **CommCell Browser**, expand **Client Computers**.
2. Right-click the **<Client>** on which the CommServe resides, and then click **Properties**.
3. Click the **Registry Key Settings** tab.
4. Click **Add**.
5. In the **Name** box, type **dEVLOGDIR**.
6. In the **Location** list, type or select **EventManager**.
7. In the **Type** list, select **STRING**.
8. In the **Value** box, type the location to which you want to save log files.

For example:

c:\log_files

9. Click **OK**.

The registry key appears in the list on the **Registry Key Settings** tab.

10. To ensure that this change takes effect, restart client services.

Back To Top

Log Files - How To

Topics | How To | Support | Related Topics

Send Log Files

Send Log Files from the Command Line

Send Log Files To a Remote Computer

Configure Time Range

Configure Troubleshooting Settings

Set the Maximum Size for Email Bundles

Send Log Files from the Workstation Backup Client Console

Configure FTP Settings for Workstation Backup Clients

View the Log Files of a CommServe, MediaAgent, or Client Computer

View the Log Files of a Job History

View the Log Files of an Active Job

SEND LOG FILES

Before you Begin

- Ensure that you have a product that can open zipped files.
- A mail server must be defined in the CommCell Console.
- Provide a valid email address or a local destination path on the CommServe to store the log files.

Required Capability: See Capabilities and Permitted Actions

▶ To send log files:

1. In the CommCell Browser, right-click the CommServe, click **All Tasks**, and then select **Send Log Files**. The **Send Log Files** window is displayed.
2. From the **General** tab, provide the following information:
 - one or more recipient email addresses (multiple email addresses separated by a comma)
 - a **Subject (Ticket Number)**
 - a **Problem Description**
3. From the **Computers** tab, choose the appropriate **Job ID** if you are sending the log files of a specific job.

If you wish to send the log files to specific computer(s), you can select and move the appropriate client computers from the **Available Computers** list to the **Selected Computers** list.
4. From the **CommCell Information** tab, select the following options, if desired:
 - **CommServe** if you wish to include the CommServe database log files.
 - **SRM Database** if you wish to include the SRM database log files.
 - **Database logs** if you wish to include the error logs for the CommServe Database Engine.
5. From the **Machine Information** tab, select the log information you wish to include, if any.
6. From the **Output** tab, select the following options:
 - If you wish to upload the log files to an existing FTP and/or HTTP location, select the **Upload to FTP Location** and/or **Upload to HTTP Server** check box. If **Upload to HTTP Server** is selected, you can define a proxy server by clicking **Proxy Settings**.
 - If you wish to send the log file information immediately, select the **Email to Recipients** box. Type the address of the recipient(s) who are to receive the log file information.

To send log files to multiple recipients, select the desired recipients in the **Available Users** field. You can then add or remove the desired recipients from the **Users to be Notified** using the appropriate arrow buttons. Note that log files can be configured to be sent via e-mail to user groups created from within the CommCell Console as well as external domain user groups.
 - To save the log files to a specific directory on the CommServe disk, select the **Save to Folder** check box. You can either type or browse the CommServe local path.



In order to save the log files to the CommServe disk, the user must have Administrative Management capability at CommServe level.

- Click **Ok**.

COMMAND LINE INTERFACE - SEND LOG FILES

Before you Begin

- Ensure that you have a product capable of opening `tar` files.
- Ensure that a mail server is defined in the CommCell Console.
- Ensure that you are running the utility from the CommServe computer when using the command line.
- Specify a valid e-mail address or local destination path on the CommServe to store the log files.

USAGE

To send log files from the command line, navigate to the `<software installation path>\Base` folder and enter the required information. You can choose to type in the commands manually at the command prompt or use an input file as described in the following sections:

USING ARGUMENTS AT THE COMMAND PROMPT:

```
sendLogFiles.exe -<argument_value>
```

USING AN INPUT FILE:

```
sendLogFiles.exe -af "<location_of_input_file>\<name_of_input_file>"
```

CREATE CUSTOM COMMANDS

Custom commands can be created by defining new commands utilizing the required arguments.

To create custom commands:

- Open the `GXCommands` table by navigating to **Start | Programs | Microsoft SQL Server 2005 | SQL Server Management Studio | Databases | CommServ**.
- In the **commandToRun** column, add the appropriate arguments to a new row in the table (see Required Arguments for a list of available arguments to include).

Note the ID number for the new command as it appears in the **ID** column.
- Open the `GXCommandOSMapping` table by navigating to **Start | Programs | Microsoft SQL Server 2005 | SQL Server Management Studio | Databases | CommServ**.
- Locate the ID number for your command in the `GXCommandid` column.
- Enter the operating system ID for your computer in the `simOSFamily` column. This information should be entered in the cell that corresponds to the command ID number. The operating system IDs supported are listed below:

- 1: Linux
- 2: Windows
- 4: HP-UX
- 5: Solaris
- 6: AIX
- 10: NetWare
- 11: Tru64
- 13: FreeBSD
- 14: Macintosh

REQUIRED ARGUMENTS:

-vm	Virtual machine <code>-vm <CommServe_name></code>
-CS	Sends log files from the CommServe.
-rm	Specifies which remote computer's log files are to be sent. Repeat the <code>-rm</code> argument to specify multiple remote computers. <code>-rm <remote_computer_name></code>

-j	Sends log files for a particular Job ID. -j <Job_ID_Number>
-w	Sends the log files from all computers associated with a particular Job ID.
-db	Sends the log files from the CommServe SQL database.
-sql	Sends the SQL error logs.
-sl	Sends the system logs.
-gu	Sends information on software updates.
-cd	Sends the crash dump.
-mc	Sends machine information.
-sc	Sends the system command output.
-gl	Sends software component logs. Must be used in conjunction with either the -cs or -rm arguments. -gl -cs OR -gl -rm
-uc	Sends user-defined command output.
-FTP	Used to send selected log files to an existing FTP server running the CommCell Console. FTP Server information can be defined or overridden using the FTPServer/FTPUser/FTPPassword command.
-n	Used to specify an email address to which notification emails regarding successful and failed FTP operations will be sent. If this option is not specified, the FTP notification email will be sent to the current notification email address in the CommServe database. A list of email addresses can be entered with comma as separator. -n <ftp_notification_mailbox@mail.com>
-r	Used to specify an email address to which the log files will be sent. A list of email addresses can be entered with comma as separator. -r <mailbox1@mail.com>
-d	The directory to which the log files will be saved. -d <full_directory_path>
-s	Used to specify a custom subject line for the email containing the log files. -s "<subject_line_text>

Example 1:

In this example, the log files for client1 are sent to mailbox1@mail.com. A custom subject line will be displayed in the e-mail messages.

```
sendLogFiles.exe -vm commserve1 -rm client1 -r mailbox1@mail.com -s "Log Files for client1"
```

Example 2:

In this example, the CommServe log files and the log files for **client1** and **client2** are stored in the **c:\logs** directory on the CommServe computer.

```
sendLogFiles.exe -vm commserve1 -rm client1 -rm client2 -d c:\logs
```

Example 3:

In this example, the input file is located in the **c:\logs** directory on the CommServe computer. An input file is created which will be executed at the command prompt using the following command:

```
sendLogFiles.exe -af "c:\logs\logs.txt"
```

The input file is formatted as follows:

```
[<CommServe_Name>]
```

```
[s]
```

```
[<subject>]
```

```
<email_address>
```

```
[j]
```

```
<job_ID_number>
```

The **-j** and **-rm** commands cannot be used together in the same send log files operation.

SEND LOG FILES TO A REMOTE COMPUTER

Required Capability: See Capabilities and Permitted Actions

▶ To send log files to a remote computer:

1. From:
 - A CommServe, MediaAgent, or client:
 1. Click **View**, and then click **Log Files**. The **Select the Log File to Open** window is displayed.
 2. Open a specific log file, either by selecting the log file name from the list or by typing the name of the log file in the field provided. (In the **Files of type** field, **Log Files (*.log)** is displayed by default.)
 3. Click **Open**. The contents of the log file are displayed in the **Log File for Job n** dialog box.
 - A specific job:
 1. Right click an active job in the Job Controller, or right-click a job in a job history window, then click **View Logs**. The contents of the log file are displayed in the **Log File for Job n** dialog box.
 2. From the **File** menu of the **Log File for Job n** dialog box, click **Send Page**.
 3. From the SMTP Parameters dialog box, type the name of an SMTP host (mail server). If you are viewing log files from a remote CommCell Console, then the SMTP host should be the same as the CommServe. If it is not the same, the operation will fail due to security issues.
 4. Click **OK**.
-

CONFIGURE TIME RANGE

Required Capability: See Capabilities and Permitted Actions

▶ To configure the time range for sending log files:

1. From the CommCell Console, right-click on the CommServe icon, click **All Tasks**, and then click **Send Log Files**. This opens the **Send Log Files** dialog box.
 2. Click the **Time Range** tab.
 3. Select the **Time** check box if you wish to include a specific number of hours or days to be included in the log files prior to the current time or date.
 4. Select the **Select Date/Time** option if you wish to choose a specific range of dates to be included in the log files. You may also select the time zone that corresponds to the dates and times selected.
 5. Click **OK**.
-

CONFIGURE TROUBLESHOOTING SETTINGS

Required Capability: See Capabilities and Permitted Actions

You can access the **Troubleshooting Settings** dialog box using either of the following:

- The CommCell Console's **Control Panel**.
- The **Settings** button in the **Send Log Files** dialog box.

▶ To configure troubleshooting settings using the **Control Panel**:

1. From the CommCell Console, right-click on the CommServe icon, click **Control Panel**, and then click **Troubleshooting Settings**. This opens the **Troubleshooting Settings** dialog box.
2. Specify the FTP or HTTP Location, User Name, and Password.
3. If you wish to receive notification emails regarding successful or failed FTP operations, you can select the **Notify User Upon FTP Completion/Failure** check box and provide the email address to which the notifications will be sent. You can also provide an email address to which log settings will be sent.
4. If you wish to restore all settings to their factory defaults, click the **Reset to Factory Settings** button.

▶ To configure troubleshooting settings using the **Send Log Files** dialog box:

1. From the CommCell Console, right-click on the CommServe icon, click **All Tasks**, and then click **Send Log Files**. This opens the **Send Log Files** dialog box.
2. Click the **Settings** button. This opens the **Troubleshooting Settings** dialog box.
3. Specify the FTP or HTTP Location, User Name, and Password.

- If you wish to receive notification emails regarding successful or failed FTP operations, you can select the **Notify User Upon FTP Completion/Failure** check box and provide the email address to which the notifications will be sent. You can also provide an email address to which log settings will be sent.
 - If you wish to restore all settings to their factory defaults, click the **Reset to Factory Settings** button.
-

SET THE MAXIMUM SIZE FOR EMAIL BUNDLES

Required Capability: See Capabilities and Permitted Actions

▶ To set the maximum size for email bundles:

- From the CommCell Console's Control Panel, select E-Mail and IIS Configuration.
 - Enter the desired maximum size limit (in megabytes) using the space provided for the **Mail server size limit (MB)**.
Log files exceeding the designated maximum size will be sent to the email recipient in multiple emails.
-

SEND LOG FILES FROM THE WORKSTATION BACKUP CLIENT CONSOLE

Use the following procedure to send the log files for review.

To send the log files:

- Launch the Workstation Backup agent from the **Start | Programs** menu.
 - Click the Help icon (?) in the toolbar, and select the **Send Logs** option.
 - The log files are sent.
-

CONFIGURE FTP SETTINGS FOR WORKSTATION BACKUP CLIENTS

Required Capability: See Capabilities and Permitted Actions

▶ To configure FTP settings to receive Workstation Backup client log files:

- Open the GxGlobalParam table in the CommServe database.
 - Add a new row with name = `SendLogsClientUseFTP` and value = `-FTPServer <servername> -FTPUser <username> -FTPPassword <password>`. For example, `-FTPServer mcrae64 -FTPUser Orange -FTPPassword Orange`.
 - Save the changes. The log files from the workstation Backup clients would be sent to the specified server.
-

VIEW THE LOG FILES OF A COMMSERVE, SRM SERVER, MEDIAAGENT, OR CLIENT COMPUTER

Required Capability: See Capabilities and Permitted Actions

▶ To view the log files of a CommServe, MediaAgent, or client computer.

- From the CommCell Browser, right-click a CommServe, MediaAgent, or client computer, click **View**, and then click **Log Files**. The **Select the Log File to Open** window displays.
 - To see a specific log file, either select the log file name from the list or type the name of the log file in the field provided. (In the **Files of type** field, **Log Files (*.log)** is displayed by default.) Click **Open**. The contents of the log file are displayed.
-

VIEW THE LOG FILES OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

▶ To view the log files of a Job History:

- From the CommCell Browser, right-click the entity whose job history you want to view, and then click to view a job history.
 - From the job history filter window select the filter options, if any, that you want to apply, and then click **OK**.
 - From the job history window, right-click the job whose log files you want to view, and then click **View Logs**.
 - The contents of the log file related to the selected job history are displayed in the **Log File for Job n** window.
-

VIEW THE LOG FILES OF AN ACTIVE JOB

Required Capability: See Capabilities and Permitted Actions

▶ To view the log files of an active job:

1. From the Job Controller of the CommCell Console, right-click a job, then click **View Logs** from the short-cut menu.
 2. The contents of the log file related to the selected job are displayed in the **Log File for Job *n*** window.
-

[Back To Top](#)

Name Management

Topics | How To | Troubleshoot

TABLE OF CONTENTS

Overview

Support

Changing the CommServe Name

Changing the Names of Clients/MediaAgents

Changing the Names of CommCell Components after a CommCell Migration

Changing the Domain Name for CommCell Components

Changing the Names from the Command line

Important Considerations

Agent Specific Considerations

OVERVIEW

It may be necessary to change the names of CommServe, MediaAgent and/or Client computers in a CommCell. The need to change the names of computers may occur in one or more of the following situations:

- When the CommServe is moved or hardware changed to provide for a better configuration.
- When a CommCell is migrated and the clients are moved to another CommServe.
- When the domain name associated with an entire CommCell or part of a CommCell is changed.
- When a Client is moved or hardware changed to provide for a better configuration.

The following sections describes the name management process in all of the above situations.

Ensure the following before you change the names of computers in the CommCell using the CommCell Console:

- Change the name of the computer in the operating system.
- Make sure that the computer is available in the network with the new name. (DNS lookup or other name resolution facilities is appropriately configured to resolve the new name of the computer.)
- Ensure that all applications running on the computer, such as SQL server, Exchange, Server, Oracle database, etc function with the new name. For the procedure to rename a computer that hosts a Stand-Alone Instance of SQL Server, see <http://msdn.microsoft.com/en-us/library/ms143799.aspx>.

Use **ping** (or other such network connectivity utilities) to verify whether the computer which has a new name, is accessible. Also ensure that the other computers in the network are accessible to the computer with the new name.

SUPPORT

Name management process is supported for all components from the CommCell Console.

Computers in Windows and Unix are supported in the clustered environment. (Netware is not supported in the clustered environment.). When performing the name change process in a clustered environment, use the CommCell Console to perform the name change.

CHANGING THE COMMSERVE NAME

CommServe name can be changed from the Control Panel in the CommCell Console. The CommServe name change process includes the following:

- Change the CommServe name
- Automatically inform all MediaAgents/Clients - clustered and non-clustered - in the CommCell of the new CommServe name.

See Change the Name of the CommServe Computer for step-by-step instructions.

Consider the following before performing the name change operation in a CommServe:

- All MediaAgents/Clients must be accessible during the CommServe name change process. If for some reason the MediaAgents/Clients were not accessible a dialog box will provide a list of MediaAgents/Clients that were unavailable during the name change operation. In such case, make sure that the MediaAgents/Clients are accessible and perform the name change operation in those MediaAgents/Clients using one of the following procedures:
 - Change the CommServe name in the multiple MediaAgents/Clients. See Change the Name of the CommServe in Multiple MediaAgents/Clients.
 - Change the CommServe name in a specific client/MediaAgents. See Change the Name of Client/MediaAgents Computers.

CHANGING THE NAMES OF CLIENTS/MEDIAAGENTS

The Client/MediaAgent name can be changed from the Client or MediaAgent Properties in the CommCell Console. See Change the Name of Client/MediaAgent

Computers. for step-by-step instructions.

When performing the name change process in a clustered environment, use the CommCell Console to perform the name change.

CHANGING THE NAMES OF COMMCELL COMPONENTS AFTER A COMMCELL MIGRATION

Use one or more of the following steps to change the appropriate names after performing CommCell Migration:

- If the Client names are changed after CommCell Migration, change the name of the appropriate Clients using the steps described in Change the Name of Client/MediaAgent Computers.
- If the Domain names are changed, provide the name of the new domain as described in Change the Domain Names for CommCell Computers.
- Make sure that the clients/MediaAgent computers that were migrated to the appropriate CommServe. See Change the Name of the CommServe in Multiple MediaAgents/Clients for step-by-step instructions.

CHANGING THE DOMAIN NAME FOR COMMCELL COMPONENTS

If there is a domain name change for one or more computers in a CommCell, provide the name of the new domain as described in Change the Domain Names for CommCell Computers.

CHANGING THE NAMES FROM THE COMMAND LINE

The CommServe, MediaAgent and Client names can be changed from the command line. This maybe useful when you install the software using the Decoupled Install and would like to change the name of the computer when the computer is registered.

The command must be executed locally, in the computer, and cannot be used to change the name of a remote computer.

Use the following steps to change the hostname or display name of a MediaAgent/Client computer as an example:

1. Navigate to the **<Software Install Directory> \Base** folder and run the following command:

CHANGING THE HOST NAME

```
SetPreImagednames.exe CCNAME -hostname newhostname oldhostname -displayname computername
```

where,

- `newhostname` and `oldhostname` are the new and old host names of the computer, which should be in the `computer.domain.company.com` format
- `computername` is the name of the computer currently displayed in the CommCell Browser

CHANGING THE CLIENT NAME DISPLAYED IN THE COMMCELL BROWSER

```
SetPreImagednames.exe CCNAME -displayname newcomputername oldcomputername
```

where,

- `newcomputername` is the new display name of the computer
- `oldcomputername` is the name of the computer currently displayed in the CommCell Browser

The command will display the "Successfully changed names" message when completed.

You can run the above commands for the CommServe and Web Server computers by replacing the `CCNAME` parameter in the command with `CSNAME` for the CommServe, or `WEBSERVER` for the Web Server.

2. Restart the Services from the Service Control Manager, see Start Services on Windows for step-by-step instructions.

Once the services are started open the CommCell Console. The new name for the computer will be displayed in the CommCell Browser.

IMPORTANT CONSIDERATIONS

- If Application Based Firewall is enabled on computer then the Name Change operation may fails. Perform the following steps if you encounter this problem:
 - Disable the Application Based Firewall by setting the `nEnableSessionBlacklist` value to 0.
 - Restart the client services from the Service Control Manager. See Service for step-by-step instructions on stopping/starting services.
 - Perform the name change operation in the computer. See Change the Name of Client/MediaAgent Computers for step-by-step instructions.
 - Enable the Application Based Firewall by setting the `nEnableSessionBlacklist` registry key to 1.
- Do not use spaces when specifying a new name for the Client.
- Schedules for the client must be recreated after changing the name of a Client computer.
- On clustered computers, the name change operation must be performed from the CommCell Console.

AGENT SPECIFIC CONSIDERATIONS

FILE ARCHIVER FOR WINDOWS/UNIX AGENTS

- If the name change operation is performed on a client that contains the File Archiver for Windows/Unix agent, services must be restarted on that client after the name change operation. This will ensure that stub recall from these clients functions correctly.

WEB SEARCH SERVER

- When the CommServe name is changed, the value in the `sINSTANCE` registry key, in the computer hosting the Web Search Server, must be changed to reflect the new CommServe name. This registry key contains the SQL database instance name in which CommServe database is stored. See `sINSTANCE` registry key for more information.
- When you change the name of a client that has the Web Search Server installed, make sure to change the URLs from the Search Server URLs tab of the **Client Properties** dialog box.

Back to Top

Name Management - How To

[Topics](#) |
 [How To](#) |
 [Troubleshoot](#)

TABLE OF CONTENTS

Change the Name of the CommServe Computer

Change the Name of CommServe in Multiple MediaAgents/Clients

Change the Name of Client/MediaAgent Computers

Change the Domain Names for CommCell Computers

SRM

Change the Data Source Name

CHANGE THE NAME OF THE COMMSERVE COMPUTER

Before changing the name of the CommServe computer, follow the steps below:

1. Perform a Disaster Recover Backup.

Verify and ensure that the Disaster Recovery Backup completes successfully. Also note down the location of the disaster recovery backup file. (For a more detailed discussion, see Phases of Disaster Recovery Backups.)

2. Ensure the following:

- Change the name of the computer in the operating system.
- Make sure that the computer is available in the network with the new name. (DNS lookup or other name resolution facilities is appropriately configured to resolve the new name of the computer.)
- Ensure that all applications running on the computer, such as SQL server, Exchange, Server, Oracle database, etc function with the new name. For the procedure to rename a computer that hosts a Stand-Alone Instance of SQL Server, see <http://msdn.microsoft.com/en-us/library/ms143799.aspx>.

Use **ping** (or other such network connectivity utilities) to verify whether the computer which has a new name, is accessible. Also ensure that the other computers in the network are accessible to the computer with the new name.

3. Specify the current CommServe name in the `hosts` file located in the `C:\Windows\System32\drivers\etc` directory. The CommServe name should be specified in the following format:

```
172.xx.xx.xx commservName commservComputer.mydomain.company.com
```

Adding the CommServe name to the `hosts` file will allow the upcoming name change operation to automatically update the system DSN with the new CommServe name.

The following procedure describes the steps involved in changing the name of the CommServe computer.

1. From the **Tools** menu in the CommCell Console, click **Control Panel**.
2. Double-click **Name Management**.
3. Select the **Update CommServe hostname on CommServe and Remote clients** option and click **Next** to continue.
4. Select the new CommServe name from the **Current CommServe Name** list.
5. Select the old CommServe name from the **Old CommServe Host Name** list and click **Finish** to continue.

The operation will change the CommServe name and will automatically inform all the MediaAgents/Clients in the CommCell of the new CommServe name. If for

some reason the MediaAgents/Clients were not accessible a dialog box will provide a list of MediaAgents/Clients that were unavailable during the name change operation. In such case, make sure that the MediaAgents/Clients are accessible and perform the name change operation in those client/MediaAgents using one of the following procedures:

- Change the Name of the CommServe in Multiple MediaAgents/Clients
- Change the Name of Client/MediaAgents Computers

CHANGE THE NAME OF COMMSERVE IN A MULTIPLE MEDIAAGENTS/CLIENTS

The following procedure describes the steps involved in changing the name of the CommServe in a multiple clients/MediaAgent computers.

1. From the **Tools** menu in the CommCell Console, click **Control Panel**.
2. Double-click **Name Management**.
3. Select the **Update CommServe for Clients post Migration or Split** option and click **Next** to continue.
4. Select the new CommServe name from the **Current CommServe Name** list.
5. Select the old CommServe name from the **Old CommServe Host Name** list and click **Next** to continue.
6. Select the names of clients in which the CommServe name should be changed from the **Available** list and use the arrow button to move them to the **Selected** list and then click **Finish**.

It is recommended that you do not select the **Update database even if clients are unreachable** option.

If the option is not selected, and the clients are not reachable, you can subsequently re-run this operation for the failed clients.

If this option is selected, and the clients are not reachable, you must manually update the clients as described in Manually Updating the CommServe or Domain name on Client/MediaAgent Computers.

The CommServe name will be changed in the selected clients.

CHANGE THE NAME OF CLIENT/MEDIAAGENT COMPUTERS

The following procedure describes the steps involved in changing the name in a specific Client/MediaAgent computers. On clustered computers, the name change must be performed from the CommCell Console.

1. Perform the name change on the computer. After changing the name, ensure the following:
 - Change the name of the computer in the operating system.
 - Make sure that the computer is available in the network with the new name. (DNS lookup or other name resolution facilities is appropriately configured to resolve the new name of the computer.)
 - Ensure that all applications running on the computer, such as SQL server, Exchange, Server, Oracle database, etc function with the new name. For the procedure to rename a computer that hosts a Stand-Alone Instance of SQL Server, see <http://msdn.microsoft.com/en-us/library/ms143799.aspx>.

Use **ping** (or other such network connectivity utilities) to verify whether the computer which has a new name, is accessible. Also ensure that the other computers in the network are accessible to the computer with the new name.
2. Open the **CommCell Console**.
3. Right-click the Client/MediaAgent in which the name was changed, and then click **Properties**.
4. From the **General** tab, click **Edit**.
5. From the Edit Client Name dialog box, modify the **Client Name** and the **Host Name**. CommServe HostName displays the full interface name of the CommServe computer used by the Client/MediaAgent to communicate with the CommServe. If you wish to change the CommServe name, type the new CommServe name in **CommServe HostName** field.

Do not use spaces when specifying a new name for the Client.

6. Click **OK** to save the information.

The name of the computer is changed.

CHANGE THE DOMAIN NAMES FOR COMMCELL COMPUTERS

The following procedure describes the steps involved in changing the domain names for the Windows and UNIX Client computers.

1. From the **Tools** menu in the CommCell Console, click **Control Panel**.
2. Double-click **Name Management**.
3. Select the **Update Domain Name** option and click **Next** to continue.

4. Select the old domain name from the **Old Domain Name** list.
5. Type the new domain name in the **New Domain Name** box and click **Next** to continue.
6. Select the names of clients in which the domain name should be changed from the **Available** list and use the arrow button to move them to the **Selected** list and then click **Finish**.

The domain name is changed in the selected clients.

CHANGE THE DATA SOURCE NAME

The following procedure describes the steps involved in changing the Data Source Name of the CommServe and SRM databases:

1. Using IE type in the following
`https://localhost/Reports[$Bull Calypso]`
2. Select **SRM** node.
3. Edit the following Data Source Names (DSNs):
 - o CommServe
 - o SRM
 - o SRMRaw
4. Select a DSN.
5. Change the old System Name to the new System Name in the **Connection String** field.
6. Re-enter the password, then click **Apply**.

The DSN will connect to the New System.

[Back To Top](#)

CommCell Migration

Basic Advanced Troubleshooting

TABLE OF CONTENTS

Overview

Migration Components

- What is Migrated
- What is Not Migrated

Prerequisites

- General Requirements
- Migration Requirements

Permanent Migration

- Export Metadata from the Source CommCell
- Import Metadata on the Destination CommCell

Temporary Migration

- Export Metadata from the Source CommCell
- Import Metadata on the Destination CommCell

View Admin Job History

Post Migration Considerations

OVERVIEW

CommCell Migration provides the facility to move Clients or MediaAgents from one CommCell to another for performing cross server restores or on a permanent basis to allow backups to continue in a new CommCell.

MIGRATION COMPONENTS

WHAT IS MIGRATED

The following components are available for migration:

1. Client computers and the Agents installed on the Client can be migrated to another CommCell. You can select the individual Agents, Backupsets, and Subclients for migration.
2. Client Group definitions are migrated but not the associations and the clients associated to the Client group.

Note that the client group definition is migrated. The actual clients within the group are not migrated unless they are selected for migration.

3. Subclient policies, schedule policies, users and user groups, media location and alerts associated with the CommCell.
4. Client configurations such as holidays, operation window, activity control, and schedules can be migrated.
5. Metadata records associated with the backup data secured by Data Protection operations from the Agents. This includes the following:
 - o History information.
 - o Information about media.
 - o Storage Policy and Storage Policy Copies associated with the subclients configured in the Client, including storage policies and storage policy copies used in the past, that contain valid data from the Client.
6. MediaAgent details, excluding the library configurations can be migrated to another CommCell. After the migration you will have to manually configure the libraries on the destination CommCell.

WHAT IS NOT MIGRATED

The following components associated with a source CommCell are not migrated:

- The data and binaries that are associated with metadata are not migrated.
- Information associated with MediaAgents such as, configured libraries, master drive pools, drive pools and drives.
- History information associated with Data Recovery operations and administration jobs.
- Firewall related configuration information.
- Events associated with jobs generated by Clients that are migrated.
- Audit trail information associated with the client

- Subclient-based Storage Policy Copy associations.
- Any associations related to the configurations i.e., non-data bearing entities associated with a client such as schedule policies, subclient policies etc. They are migrated as configuration templates.
- Reports.

PREREQUISITES

GENERAL REQUIREMENTS

- Verify that no jobs are in progress or scheduled to occur in the Clients that you wish to migrate. If jobs are scheduled, either perform the export at another time or disable all jobs for the client using the **Activity Control** tab from the **Client Properties** dialog box in the CommCell Console.
- Perform an Auxiliary Copy operation before exporting the metadata records for migration. This will ensure that all the copies associated with all storage policies are synchronized.
- It is recommended that you perform a disaster recovery backup operation prior to a migration operation.

MIGRATION REQUIREMENTS

- Ensure that compatible drives are available in the destination CommCell to restore the migrated backup data.
- The source and destination CommCells should be accessing the same version of CommServe(s).
- Make sure that you have the same SQL Server version in the source and destination CommServe. For example, if you have SQL 2008 R2 version in the source, you need to have the same version in the destination as well.
- If the SRM Server is installed in Source CommServe, make sure to install the SRM Server on destination CommServe too while performing CommCell Migration. This is because an SRM Analytics Policy is required to be associated with the migrated SRM components and there is one SRM Analytics Policy per CommCell.

PERMANENT MIGRATION

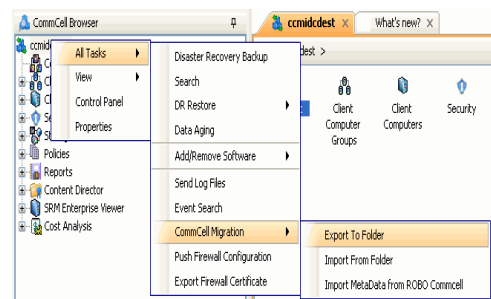
When computers are relocated or for load balancing, some clients may have to be attached to another CommCell. This process requires permanent migration of the metadata records associated with these clients. The following steps describe the process involved in migrating the metadata of an entire CommCell to another CommCell:

EXPORT METADATA FROM THE SOURCE COMMCELL

When performing CommCell Migration you will first need to export the metadata associated with the source CommCell. The export operation is performed on the source CommCell, allowing you to select entities that you wish to export from a source CommCell to the specified export location.

Follow the steps given below to export an entire CommCell:

1. From the CommCell Browser, right-click the CommServe, click **All Tasks**, click **CommCell Migration** and select **Export To Folder**.



2. From the **General** tab on the **Export Options** dialog box, provide the export location in the **Export Folder** field. Select **Use local** for a local path. Select **Use Network** for a network location. If you select a UNC path, provide the access credentials to access the export location. Click **User Name/Password** to provide the user details. Select **Use Other CS Host** to specify other CommServe along with its local path as a host for migration. Select a database from **Export entities from** list to export metadata.

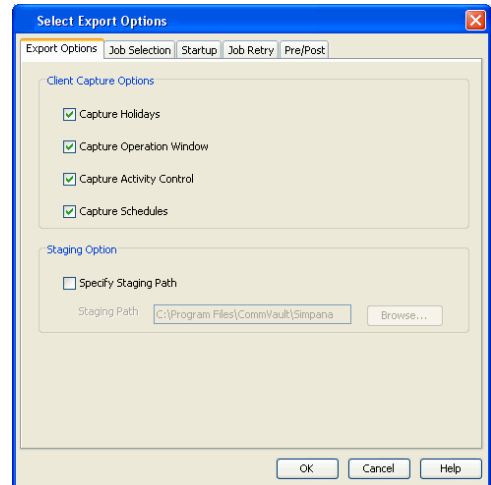
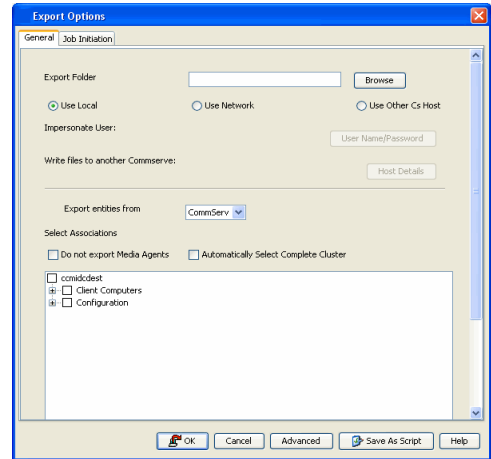
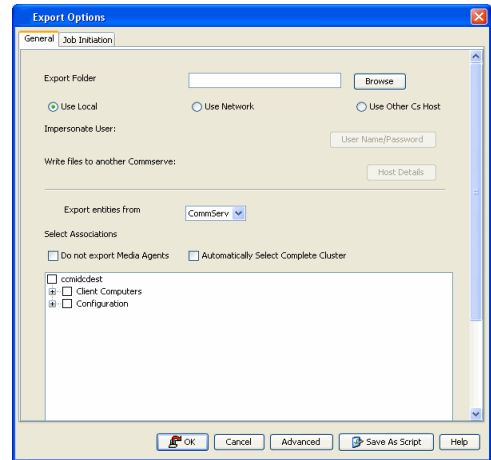
3. Select the following components for migration from **Select Associations**.
 - Client(s) that you wish to export. For a client, you can select the individual components such as Agents, Backupsets, and/or, Subclients.
 - Client Computer Groups to select a client group definition for export.
 - MediaAgent that you wish to export. If you select **Do Not Select MediaAgents** option, the MediaAgents of the selected source clients will not be migrated.
 - Desired CommCell configurations such as Subclient Policies, Schedule Policies, Users and User Groups, Alerts, and Location.

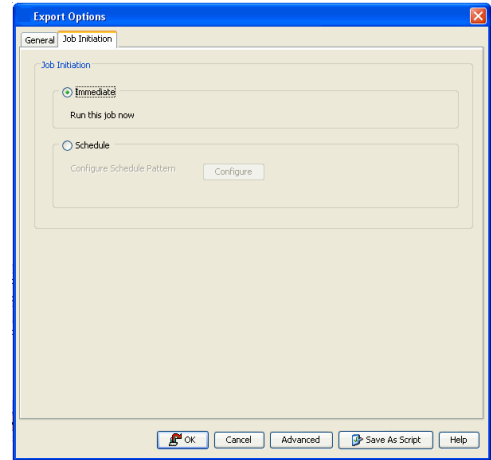


If you select **Automatically Select Complete Cluster** option, all the physical and the virtual nodes of the selected source cluster will be exported.

4. Click **Advanced** to view and select the advanced export options from **Select Export Options** dialog box.

5. From the **Job Initiation** tab on the **Export Options** dialog box, select **Immediate** run the export immediately. Alternatively, you can schedule the export job for a later time.





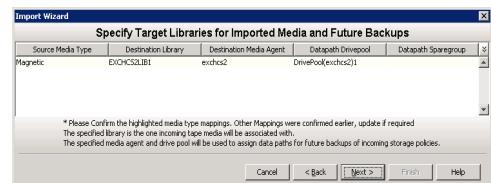
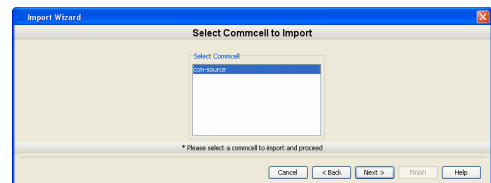
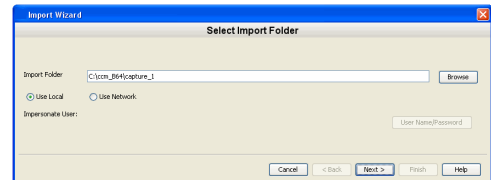
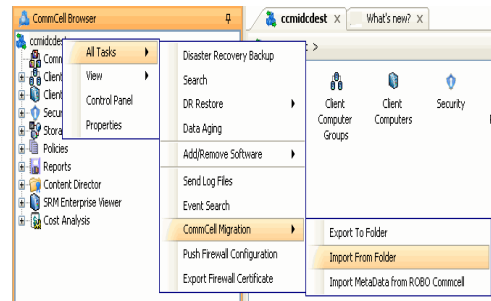
6. Click **OK** to export the metadata.

IMPORT METADATA ON THE DESTINATION COMMCELL

The metadata associated with the source CommCell can now be imported into the destination CommCell. The import will use the import entries that you have defined for the destination CommCell.

Follow the steps given below to import metadata of a source CommCell to the destination CommCell:

1. From the CommCell Browser, right-click the CommServe, click **All Tasks**, click **CommCell Migration** and select **Import From Folder**.
2. From the **Import Wizard**, provide the import location in the **Import Folder** field. Select **Use local** for a local path. Select **Use Network** for a network location. If you select a UNC path, provide the access credentials to access the import location. Click **User Name/Password** to provide the user details. Click **Next**.
3. From **Select CommCell to Import** window, select a CommCell to import and click **Next**.
4. From the **Specify Target Libraries for Imported Media and Future Backups** window, provide the media mapping options to import data from the source CommCell. Select the library, MediaAgent, drive pool, and spare group on the destination CommCell for importing data and click **Next**.



- You need to map the MediaAgent in order to associate the media. The MediaAgent should have a compatible media library to map and import the metadata from source on to the destination CommCell.
- Ensure that you copy the disk libraries to the appropriate computer specified during the import operation.
- The CV_MAGNETIC folder must have read-write access in the destination CommCell. For example, if you make copies of the CV_MAGNETIC folder using a disc, ensure that the contents are copied to a computer, so that it can be accessed

during a restore operation.

- From the **Specify Target Libraries and Mount Path Details for Imported Disk Data** window, you can view the default MediaAgent, Device Name and Mount Path on the Source CommCell for importing metadata.

The Mount Path and Library on the destination CommCell are displayed by default in this window. If you wish to change the destination mount path, click **Edit** to provide the destination Library Name and MediaAgent Name for importing metadata. Verify the mount path mapping on the **Source Mount Path Mapping** window and click **Next**.



If you are mapping the Source Mount path for the first time, the MediaAgent, Device Name, destination library and Mount Paths will appear in Blue.

- From the **Specify new Locations for Dedupe Database** window, specify the target MediaAgent and target SIDB access path on the destination CommCell for importing data and click **Next**. The SIDB needs be copied on to the destination CommCell. Otherwise, it cannot be pruned.

If you use the Global Dedup Policy as the storage policy, then the mapping path in the **Specify new Locations for Dedupe Database** window will appear in *Italics*.

For more information on SIDB/SILO configuration and mapping on the destination CommCell, see SIDB/SILO configuration.

- From the **Client Name Mapping** window, specify a new name for the client if required. If nothing is specified the old name will be used. Click **Next**.



- Migrated clients can be deconfigured from original CommServe module, before renaming the client in the migrated setup.
- If a firewall is configured for the migrated client, then you need to uninstall and reinstall the client on the destination CommCell after the migration.

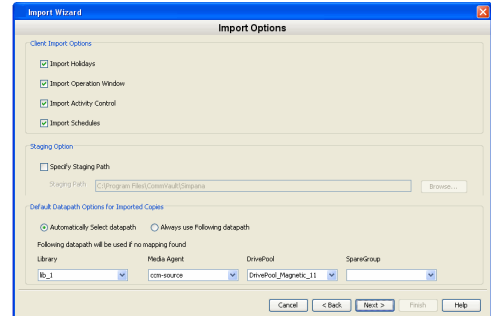
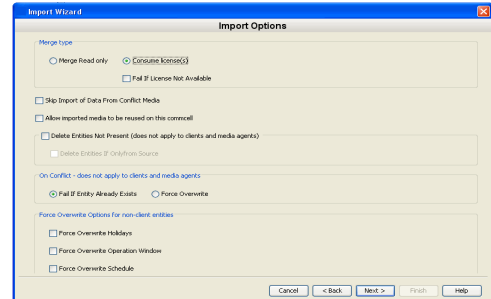
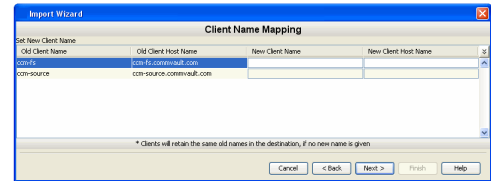
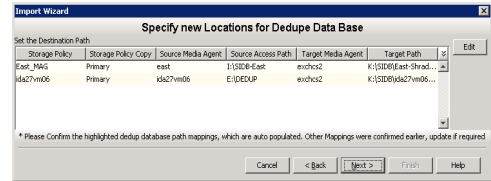
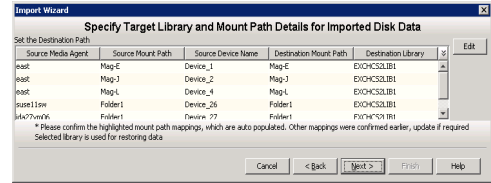
- From the **Import Options** window, select the **Consume license(s)** option to consume the license on the destination CommCell after the import is completed click **Next**.



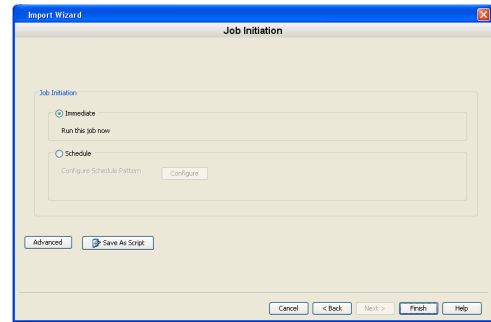
- Ensure that you have a license available on the destination CommCell.
- The destination client will be enabled once all data has been migrated. If you choose not to consume a license during this operation, the client data will be migrated, but the destination client will not be enabled.

- From the **Import Options** window, review the selected import options and click **Next**.

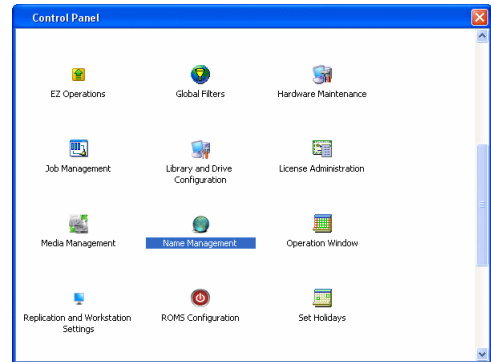
- From the **Job Initiation** window, select **Immediate** to start the import process. Alternatively, you can schedule the import job for a later time.



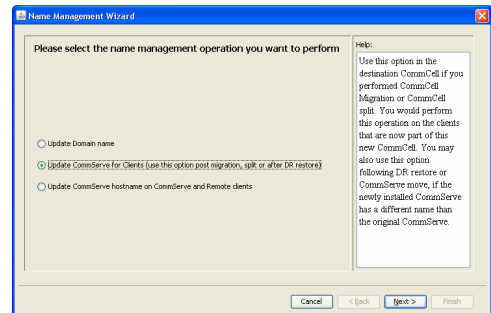
11. Click **Finish** to complete the import operation.
12. From the Control Panel, Click **Name Management Wizard** to change the CommServe Name.
You can also right click the client in the destination CommCell. From the **Client Computer Properties** dialog box, click **Name Change** to change the CommServe host name.



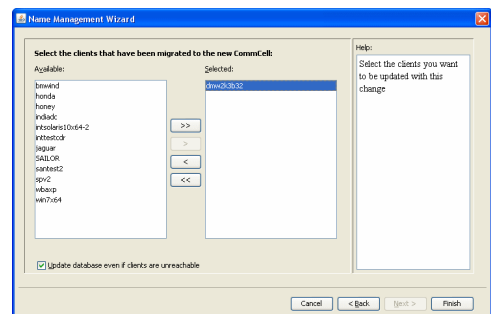
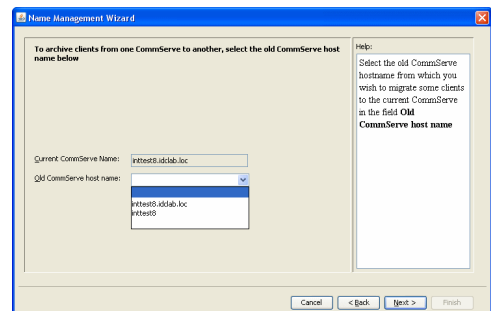
13. From the **Name Management Wizard**, select **Update CommServe for clients**. Click **Next** to Proceed.



14. Select the old CommServe hostname from which you wish to migrate the clients to the current CommServe and click **Next** to proceed.



15. Select the clients that you wish to update with this change from the list and click **Finish** to complete the migration process.



TEMPORARY MIGRATION

The following section describes the process of performing a temporary migration of a CommCell. You may need to perform a temporary migration in any of the following cases:

- To free some space on a source CommCell.
- When a copy of the Client(s) Metadata on one (source) CommCell is maintained on another CommCell. In this case, the Client continues to remain in the original CommServe, but the metadata records associated with the Client are restored to another CommCell.
- To perform maintenance operation on a source server.

The clients and configuration settings that are temporarily migrated exist in the source CommCell and destination CommCell. The properties and associations of clients and configurations in the destination CommCell exist as in the source CommCell.

EXPORT METADATA FROM THE SOURCE COMMCELL

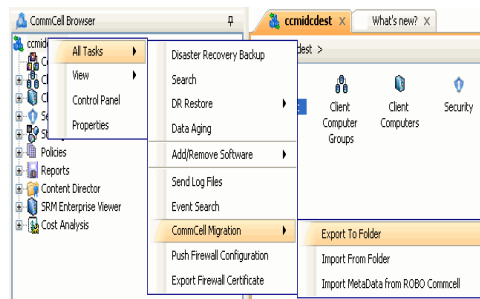
When performing CommCell Migration you will first need to export the metadata associated with the source CommCell. The export operation is performed on the source CommCell, allowing you to select entities that you wish to export from a source CommCell to the specified export location.

Follow the steps given below to temporarily export the metadata from a source CommCell on to a destination CommCell:

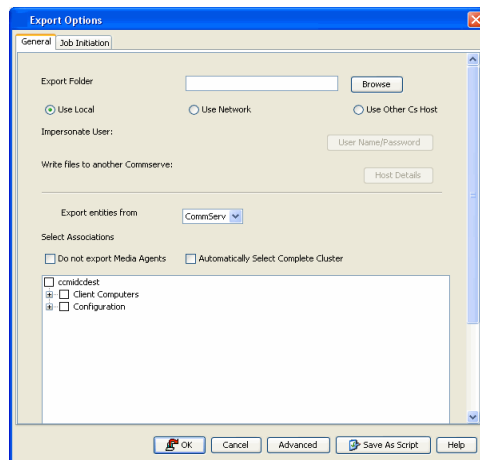
1. From the CommCell Browser, right-click the CommServe, click **All Tasks**, click **CommCell Migration** and select **Export To Folder**.



- Make sure to specify only the names of clients that you wish to temporarily migrate during the Export process.



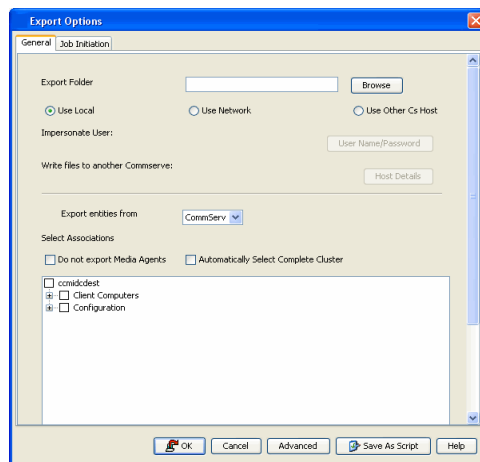
2. From the **General** tab on the **Export Options** dialog box, provide the export location in the **Export Folder** field. Select **Use local** for a local path. Select **Use Network** for a network location. If you select a UNC path, provide the access credentials to access the export location. Click **User Name/Password** to provide the user details. Select **Use Other CS Host** to specify other CommServe along with its local path as a host for migration. Select a database from **Export entities from** list to export metadata.



3. Select the following components for migration from **Select Associations**.
 - Client(s) that you wish to export. For a client, you can select the individual components such as Agents, Backupsets, and/or, Subclients.
 - Client Computer Groups to select a client group definition for export.
 - MediaAgent that you wish to export. If you select **Do Not Select MediaAgents** option, the MediaAgents of the selected source clients will not be migrated.
 - Desired CommCell configurations such as Subclient Policies, Schedule Policies, Users and User Groups, Alerts, and Location.

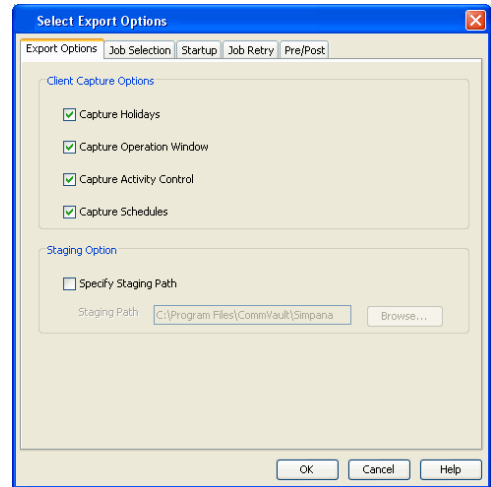


If you select **Automatically Select Complete Cluster** option, all the physical and the virtual nodes of the selected source cluster will be exported.

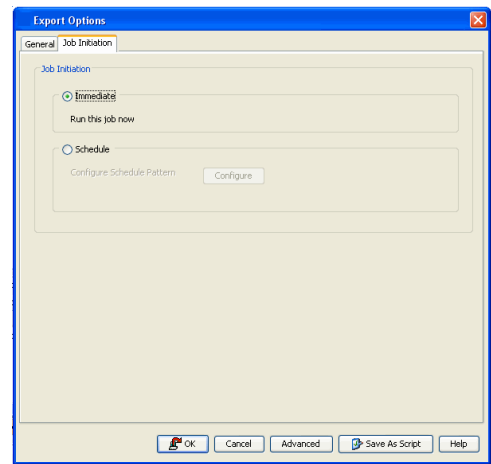


4. Click **Advanced** to view and select the advanced export options from **Select Export Options** dialog box.

- From the **Job Initiation** tab on the **Export Options** dialog box, select **Immediate** run the export immediately. Alternatively, you can schedule the export job for a later time.



- Click **OK** to export the metadata.

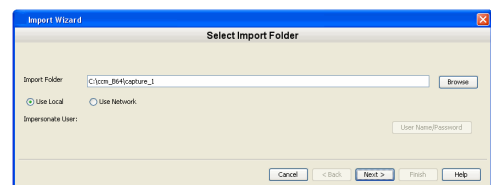
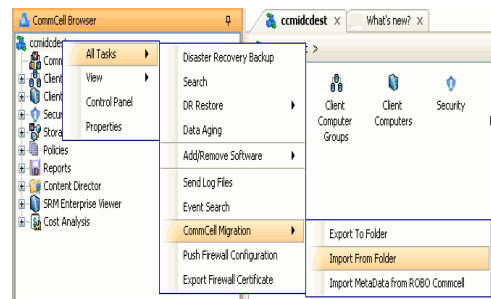


IMPORT METADATA ON THE DESTINATION COMMCELL

The metadata associated with the client in a source CommCell can now be temporarily imported on to the destination CommCell. The import will use the import entries that you have defined for the destination CommCell.

Follow the steps given below to temporarily import metadata of a source CommCell on to the destination CommCell:

- From the CommCell Browser, right-click the CommServe, click **All Tasks**, click **CommCell Migration** and select **Import From Folder**.
- From the **Import Wizard**, provide the import location in the **Import Folder** field. Select **Use local** for a local path. Select **Use Network** for a network location. If you select a UNC path, provide the access credentials to access the import location. Click **User Name/Password** to provide the user details. Click **Next**.
- From **Select CommCell to Import** window, select a CommCell to import and click **Next**.



- From the **Source Mediatype Mapping** window, provide the media mapping options to import data from the source CommCell. Select the library, MediaAgent, drive pool, and spare group on the destination CommCell for importing data and click **Next**.



- You need to map the MediaAgent in order to associate the media. The MediaAgent should have a compatible media library to map and import the metadata from source on to the destination CommCell.
- Ensure that you copy the disk libraries to the appropriate computer specified during the import operation.
- The CV_MAGNETIC folder must have read-write access in the destination CommCell. For example, if you make copies of the CV_MAGNETIC folder using a disc, ensure that the contents are copied to a computer, so that it can be accessed during a restore operation.

- From the **Source MountPath Mapping** window, you can view the default MediaAgent, Device Name and Mount Path on the Source CommCell for importing metadata.

The Mount Path and Library on the destination CommCell are displayed by default in this window. If you wish to change the destination mount path, click **Edit** to provide the destination Library Name and MediaAgent Name for importing metadata. Verify the mount path mapping on the **Source Mount Path Mapping** window and click **Next**.



If you are mapping the Source Mount path for the first time, the MediaAgent, Device Name, destination library and Mount Paths will appear in Blue.

- From the **Shared Library Device Mapping** window, click **Edit** to provide the Target MediaAgent and Device Path for importing metadata. Verify the device mapping on the **Shared Library Device Mapping** window and click **Next**.

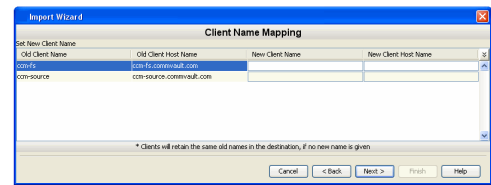
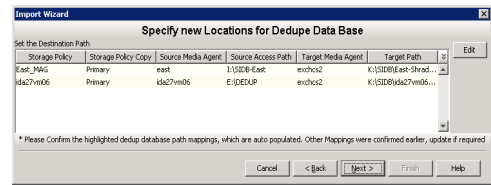
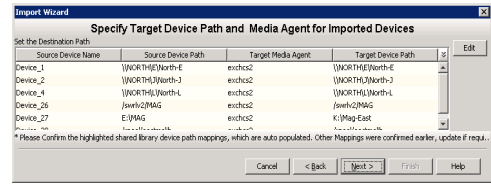
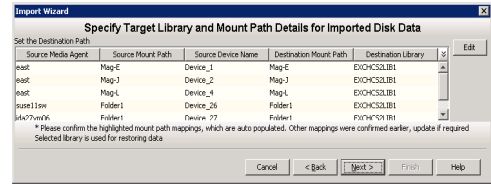
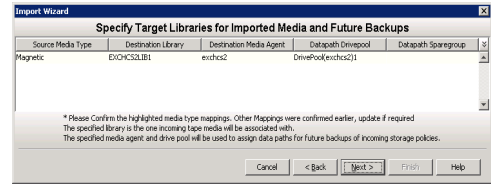
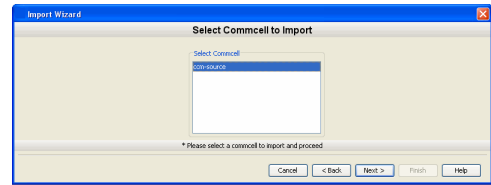
- From the **Dedupe Database Mapping** window, specify the target MediaAgent and target single instance (SIDB) access path on the destination CommCell for importing data and click **Next**.

- From the **Client Name Mapping** window, specify a new name for the client if required. If nothing is specified the old name will be used. Click **Next**.

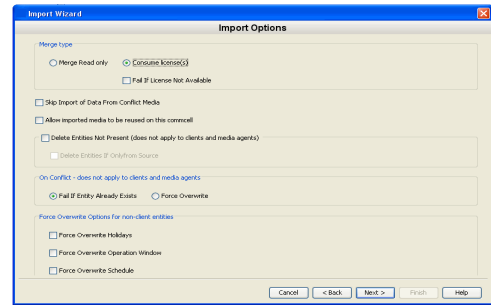


- In the case of temporary migration, it is recommended to use the old names and mapping for continuous replication from source CommCell.

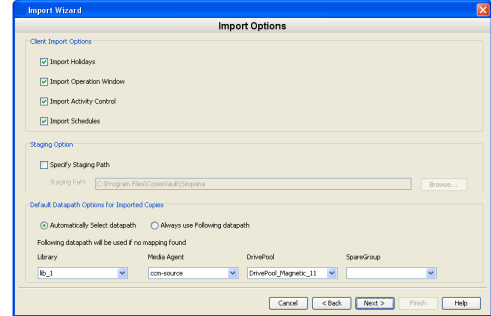
- From the **Import Options** window, review the selected import options and click **Next**.



- From the **Import Options** window for client import and datapath options, review the selected import options and click **Next**.



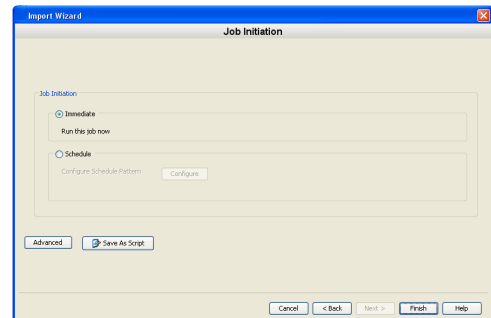
- From the **Job Initiation** window, select **Immediate** to start the import process. Alternatively, you can schedule the import job for a later time.



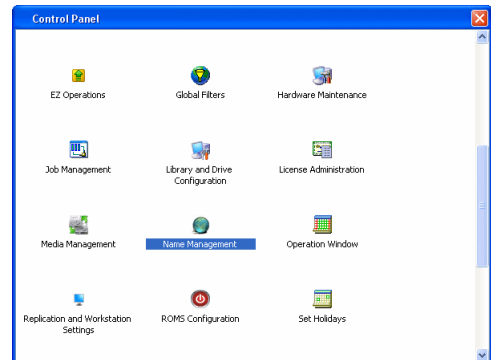
- Click **Finish** to complete the import operation.

- From the Control Panel, Click **Name Management Wizard** to change the CommServe Name.

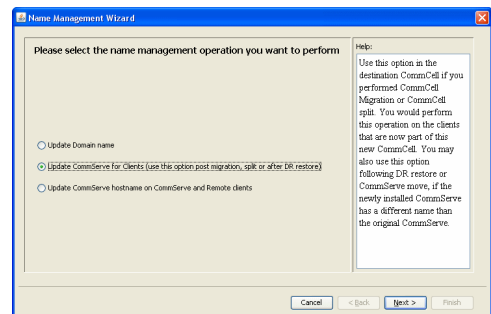
You can also right click the client in the destination CommCell. From the **Client Computer Properties** dialog box, click **Name Change** to change the CommServe host name.



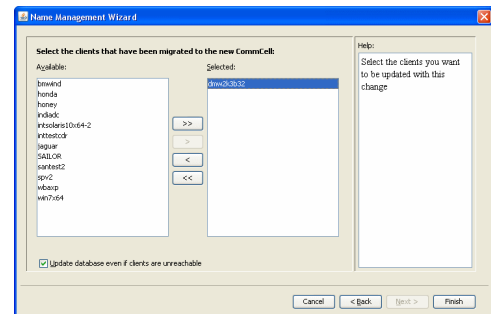
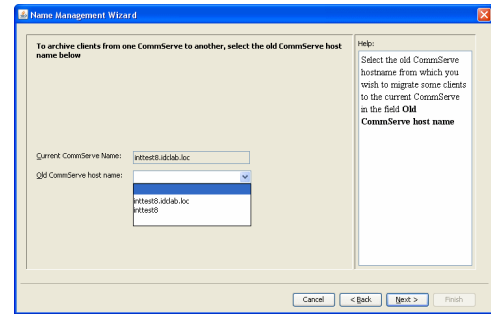
- From the **Name Management Wizard**, select **Update CommServe for clients**. Click **Next** to Proceed.



- Select the old CommServe hostname from which you wish to migrate the clients to the current CommServe and click **Next** to proceed.



16. Select the clients that you wish to update with this change from the list and click **Finish** to complete the migration process.



VIEW ADMIN JOB HISTORY

You can view the CommCell Migration job history from the Admin Job History window. Once a migration job is completed, it may be useful to view specific historical information about the job, such as the following:

- Details of the job
 - Events of the job
 - Log files of the job
1. From the CommCell Browser, right-click the CommCell whose migration history you want to view, click **View**, and then click **View Admin Job History**.
 2. For the source CommCell, select the **CommCell Export** as job type from the Admin Job History filter window to view the export history.
 3. For the destination CommCell, select the **CommCell Import** as job type from the Admin Job History filter window to view the Import history.
 4. Select the desired filter options such as time range, job status, number of jobs etc.
 5. Click **OK**.

POST MIGRATION CONSIDERATIONS

- Ensure that you check the barcodes associated with the tapes in the CommCell to make sure that there are no duplicate barcodes across all CommCells being migrated. If you find two tapes that have the same bar code, one of them needs to be changed.
- When you migrate a mount path that contains deduplicated data, the `Interval (Minutes) between disk space updates` parameter is created with a default value in minutes. This value will ascertain the time taken by MediaManager to automatically detect and update the new mount paths for deduplicated data. This in turn will determine the time to restore the data on the new target MediaAgent.
- The migrated mount paths and their corresponding migrated device controllers will be marked read only to ensure data is not corrupted. This means that no new backups can be written to the migrated mount paths and also no data can be pruned from the migrated mount paths. The migrated data is read-only and used for restore purposes. To write new backups, you need to create new local libraries with local mount paths (using a local read/write device), or add a new read/write device, device controllers and mount paths to an existing library after the migration.

To enable pruning on the mount path after a MediaAgent is permanently migrated to a new CommCell, enable read/write on the device controller pointing to the mount path. See [Modify the Access Type for Shared Disk Device](#) for step-by-step instructions.

- After a client is permanently migrated to a new CommCell, the backup for each of its subclients will automatically be converted to a full backup. This is to make sure that the metadata is disassociated from the old CommCell and recreated in the new CommCell.
- All the migrated Dedupe stores will be sealed on destination CommServe after migration.
- Auxiliary copy operation on migrated storage policies is disabled on destination CommServe after migration. To Auxiliary copy migrated data see [Enabling auxiliary copy on migrated storage policies](#).

[Back to Top](#)

Space Check

Topics | How To | Related Topics

Overview

Space Check Thresholds for the CommServe

Space Check Thresholds for the Software Installation and System Directories

Space Check for the Quick Recovery and ContinuousDataReplicator Agents

OVERVIEW

The Space Check feature monitors consumed space and free space remaining, for components which are integral to the operation of the software, and where limited space may cause operations to go into an unstable state. This monitoring includes the following:

- software installation and system directories
- disk space for the CommServe database
- all disk drives on computers with the Quick Recovery Agent or ContinuousDataReplicator installed

An event is generated in the Event Viewer when limited space and consumed space are detected for those directories. A Disk Space Low alert, if configured, will be generated if the disk space falls below the defined threshold.

If the disk space where the CommServe software is installed is less than 75MB, no new jobs will be initiated and no new phases will be started for running jobs. If the free space is less than 25MB, all the existing jobs will be killed by the system.

SPACE CHECK THRESHOLDS FOR THE COMMSERVE

DATABASE SPACE CHECK THRESHOLDS

The Database Space Check thresholds generate events and alerts if there is insufficient disk space for the CommServe Database to grow. Events are generated when the Database disk space is below the defined **Information**, **Minor**, **Major**, and **Critical** thresholds. The Disk Space Low alert, if configured, is only generated when the CommServe Database disk space falls below the defined **Critical** threshold.

The Database Space Check Interval and the Database Space Check Thresholds are configured in the System dialog box from the Control Panel. Changes to the Database Space Check Interval take effect immediately.

DATABASE SPACE CHECK INTERVAL

The Database Space Check Interval allows you to specify the frequency in which the CommServe Database Installation Directory is monitored to determine if there is insufficient disk space for the CommServe Database to grow. By default, the Database Space Check Interval is set at a one-hour frequency.

SPACE CHECK THRESHOLDS FOR THE SOFTWARE INSTALLATION AND SYSTEM DIRECTORIES

SPACE CHECK THRESHOLDS

The Space Check thresholds are configurable through the use of the registry keys for each computer within the CommCell. Use the Space Check registry keys to define the software installation and system directories' Space Check thresholds for the minimum space that should be available and the maximum space that should be consumed. If the disk free space of the directory meets the criteria defined by the Space Check registry values, an event is generated, and a Disk Space Low alert is sent, if configured.

The following directories are automatically monitored:

- Software Database Installation Directory
- Software Installation Directory
- Software Job Results Directory
- Software Temp Directory
- System Temp Directory
- Unix Var Directory
- Content Indexing Engine Directory

SPACE CHECK INTERVAL

The Space Check Interval is configurable through the use of registry keys for each computer. By default, the Space Check monitors the directories every six hours on the CommServe, once per day on the remote machines, and when services are started on any of the computers within the CommCell.

Changing the Space Check Interval will take effect when the services are restarted or at the next monitoring interval.

The following registry keys can be created for Windows, NetWare and Unix computers:

Registry Key	Purpose
bCHECK_GALAXY	Specifies if the space requirements for the software installation and system directories such as the installation directory, JobResults, or Index Cache are checked.
bCHECK_SYSTEM	Specifies if the space requirements specified for the system directories such as the %TEMP% directory for Windows computers and tmp or var directories for Unix computers are checked.
bUSE_EVENTS	Specifies if the space check events should be sent to the Event Viewer.
bCHECK_AUTOUPDATES	Specifies if the CommServe CVD will contact the configured Automatic Updates FTP site at six-hour intervals (360 minutes) to check if the CommServe Update Cache is up-to-date. If updates are missing, and the automatic update configuration is set to download the updates, the missing updates will be downloaded to the CommServe Update Cache.
nMACHINE_MAINT_INTERVAL_MINUTES	Specifies the interval (in minutes) that the system checks the following: <ul style="list-style-type: none"> • disk space for the software installation and system directories, and, for the Quick Recovery Agent and ContinuousDataReplicator, space on all volumes on the client computer • Updates available for download (CommServe only) • Service Packs available to be installed (Client or MediaAgent) • Upgrade required (Client or MediaAgent). See Updates Available to Download, Release Upgrade Required, Service Pack Required; and Disk Space Low alerts for Clients, MediaAgents, and the CommCell.
nGALAXY_MIN	Sets the threshold for the minimum space that should be available in the drive where the software is installed. An alert notification can be sent if configured in the CommCell Console. See Clients, MediaAgents and CommCell Disk Space Low alerts.
nGALAXY_MAX	Sets the threshold for the maximum space that should be consumed in the software installation directory.
nGALAXYTEMP_MIN	Sets the threshold for the minimum space that should be available in the drive where the software Temp directory resides. See Clients, MediaAgents and CommCell Disk Space Low alerts.
nGALAXYTEMP_MAX	Sets the threshold for the maximum space that should be consumed in the software Temp directory.
nSYSTEMP_MIN	Sets the threshold for the minimum space that should be available in the drive where the System Temp directory resides. See Clients, MediaAgents and CommCell Disk Space Low alerts.
nSYSTEMP_MAX	Sets the threshold for the maximum space that should be consumed in the System Temp directory.
nJOBRESULTS_MAX	Sets the threshold for the maximum space that should be consumed in the JobResults directory. This registry key is used to set alerts when space used crosses the limit specified by this key. This does not limit the actual size of job results folder.
nIDA_MIN	Sets the threshold for the minimum space that should be available in the drive where the iDataAgent directory resides. See Clients, MediaAgents and CommCell Disk Space Low alerts.
nIDA_MAX	Sets the threshold for the maximum space that should be consumed in the iDataAgent directory.
nSYSVAR_MIN	Sets the threshold for the minimum space that should be available in the var volume on a Unix computer. See Clients and MediaAgents Disk Space Low alerts.
nSYSVAR_MAX	Sets the threshold for the maximum space that should be consumed in the var volume on a Unix computer.

SPACE CHECK FOR THE QUICK RECOVERY AND CONTINUOUSDATAREPLICATOR AGENTS

For computers with either the Quick Recovery Agent or ContinuousDataReplicator installed, in addition to the monitoring already described, additional monitoring is performed, to help avoid a situation where the snapshots are deleted because maximum space on the COW cache volume or Recovery Point volume has been exceeded.

- For Windows computers, all volumes and mount points on the client computers are checked for remaining free space. For CDR, this can be useful to provide warning that the source computer is running out of disk space, which will ultimately cause replication activity to be aborted.
- For UNIX computers, /opt, /tmp, /var, and the log volume are all monitored. If you are using QSnap, the COW Cache volume is monitored as well.

SPACE CHECK THRESHOLDS

If the remaining free space on any monitored volume or mount point is less than 20% when checked, an event is generated, and a *Disk Space Low Alert* is sent by email or to a pager, if so configured. When configuring this Alert, include the <DISK SPACE INFO> Alert Token in the email/pager notification, so that meaningful data is included in the alert message. To configure an alert, see Alerts - How To.

SPACE CHECK INTERVAL

The Space Check Interval is configurable through the use of the nMACHINE_MAINT_INTERVAL_MINUTES registry key as described above. By default, Space Check checks all drives once per day, or when services are started on the client computers.

When the Space Check Interval is changed, the change will take effect when the services are restarted or at the next monitoring interval.

NOTES

- Unmounted partitions will not be checked by Space Check.
 - When the Quick Recovery Agent or CDR is installed on the virtual server of a cluster, the Space Check feature will perform these checks on the physical computer that is the active node, as well as on the virtual server.
-

[Back To Top](#)

Space Check - How To

[Topics](#) | [How To](#) | [Related Topics](#)

Set the Database Space Check Interval and the Database Space Check Thresholds

SET THE DATABASE SPACE CHECK INTERVAL AND THE DATABASE SPACE CHECK THRESHOLDS

Required Capability: See Capabilities and Permitted Actions

▶ To set the Database Space Check Interval the Thresholds for the Database Space Check:

1. From the CommCell Browser, right-click the CommServe icon, click **Control Panel**, and then double-click **System**.
2. From the System dialog box, define the appropriate frequency in hours and minutes, and define the Database Space Check threshold percentages in descending order from the **Information** severity to the **Critical** severity.
3. Click **OK**.

The Database Space Check Interval and the Database Space Check Thresholds are now set.

[Back To Top](#)

Install the CommServe and Database Engine on Separate Computers

TABLE OF CONTENTS

Overview

Setup CommServe Computer

Setup SQL Server Computer

Moving the Database

Setting up the SQL Server Account

Changing DSN Settings

Protecting the Database - Setting up the Disaster Recovery Backup

Restoring the Database

Installing Updates

Uninstalling Updates

OVERVIEW

The CommServe and the Microsoft SQL Server Database Engine can be installed on separate computers.

The following procedure describes the steps involved in building such a topology. Note that these procedures require familiarity and understanding of both the Microsoft SQL Server Database Engine and the Windows operating system.

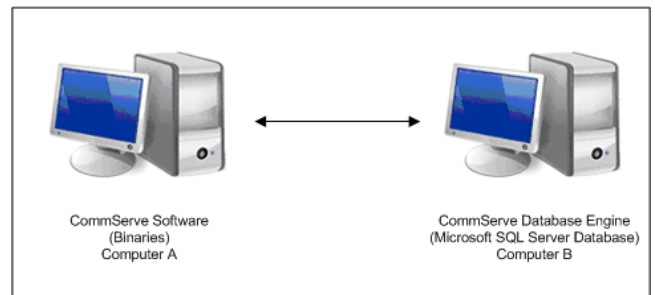
This procedure can be used when you initially install the software, or when you split an existing CommServe.

The following are not supported in this configuration:

- CommServe Name Change
- CommServe Disaster Recovery Tool (For disaster recovery procedures in this configuration, See Setting up the Disaster Recovery Backup and Restoring the Database)

The setup requires the following:

- CommServe software to be installed on CommServe and SQL Server computers. This installation will automatically install SQL Server software.
- A reliable and fast network connection between these two computers.



SETUP COMMSERVE COMPUTER

1. Install the CommServe software on the computer that will host the CommServe.
2. Verify that no jobs are in progress or scheduled to occur while setting up this configuration.
If jobs are in progress or other tasks (such as reports or updates) are scheduled, either perform this task at another time or disable all activity or disable all scheduled tasks from the CommCell Console.
3. Stop all services on the CommServe computer.

See Install the CommServe for step-by-step instructions.

To disable activity control:

1. From the CommCell Browser, right-click the **CommServe** and then click **Properties**.
2. Click **Activity Control** tab.
3. Clear **Enable All Job Activity** and **Enable Scheduler** box.
4. Click **OK**.

To stop services:

1. Click the **Start** button on the Windows task bar and then click **All Programs**.
2. Navigate to **bull | Calypso** and click **Service Control Manager**.
3. Select **All Services** in **Services**.
4. Click **Stop** to stop all services.

SETUP SQL SERVER COMPUTER

4. Install the CommServe software on the SQL Server computer. This installation will automatically install SQL Server software.

See Install the CommServe for step-by-step instructions.

See System Requirements - CommServe for more information on the SQL Server

version.

5. Stop all services on the SQL Server computer.
Note that the CommServe Services must be disabled permanently.

MOVING THE DATABASE

6. In the CommServe computer, using the **SQL Server Management Studio**, backup the **CommServ** database and create a .dmp file.

7. Copy the backup dump (.dmp) file created in **Step 4** to SQL Server Computer using any of the following method:
 - Using a physical media
 - Using a network drive that is accessible from both the Servers

8. In the SQL Server computer, using the **SQL Server Management Studio**, restore the **CommServ** database.

To stop services:

1. Click the **Start** button on the Windows task bar and then click **All Programs**.
2. Navigate to **bull | Calypso** and click **Service Control Manager**.
3. Select **All Services** in **Services**.
4. Click **Stop** to stop all services.

Perform the following steps to back up the CommServe database to a full database backup:

1. Open **Microsoft SQL Server Management Studio**.
2. Navigate to **Server Instance | Database | CommServ**.
3. Right-click the **CommServ** database, select **Tasks** and then click **Backup**. The **Back Up Database** dialog box appears.
4. In the **Database**, verify the database name.
5. In the **Backup type**, select **Full**.
6. In the **Backup Component**, select **Database** option.
7. Accept the default backup set name in the **Name**, or you can enter a different name for the backup set.
8. Specify when the **Backup set will expire**. By default **After** is selected with value **0**.
9. In the **Destination** area select **Disk** option. To select the path, click **Add**. The selected path will be displayed in the **Backup to** list.
10. To remove backup destination, select the destination path and click **Remove**.
11. Click **OK**.

Perform the following steps to restore the full database to the SQL Server computer:

1. Open **Microsoft SQL Server Management Studio**.
2. Navigate to **Server Instance | Database**.
3. Right-click **Database**, select **Restore Database**. The **Restore Database** dialog box appears.
4. On the **General** page, do the following:
 - In the **To Database**, select or type the name of a database.
 - To specify the source and location of the backup sets to restore, select **From device** option.
Click the **Browse** button, **Backup dialog box** appears.
In the **Backup media**, select one of the device type.
Click **Add** to provide the path of dump file copied in the previous step. Click **OK**.
5. On the **Options** page, do the following:
 - In the **Restore options**, choose any of the options, appropriate for your situation.
 - The **Recovery state** determines the state of the database after the restore operation.
Choose **Leave the database non-operational, and do not roll back the uncommitted transactions. Additional transaction logs can be restored. (RESTORE WITH NORECOVERY)** option.

9. Run the following query from SQL Management Studio on SQL Server Computer:

Usage:

```
exec CommServ..executeCSSetupScripts '<path>'
```

Example

```
exec CommServ..executeCSSetupScripts 'C:\Program Files\Bull  
Calypso\Calypso\'
```

Where

<path> - This is the path of CommServe Installation Directory on SQL Server Computer.

6. Click **OK**.

SETTING UP THE SQL SERVER ACCOUNT

10. On the CommServe computer, from the **Registry Editor**, edit the following values to point to SQL Server Computer:

- **sCONNECTION**
- **sDOMAIN**
- **sINSTANCE**

To open and edit the registry key:

1. From **Taskbar**, click **Start**, and then click **Run**.
2. Type **regedit**, and then click **OK**.
3. Navigate to the following key:

**HKEY_LOCAL_MACHINE\SOFTWARE\CommVault
Systems\Galaxy\Instance<xxx>\Database**

4. Edit the following values:
 - **sCONNECTION** set it to *<SQL Server computer>_commserv*
 - **sDOMAIN** set it to *<SQL Server computer>*
 - **sINSTANCE** set it to *<SQL Server computer>\BullCalypso*

CHANGING DSN SETTINGS

11. On the CommServe computer, modify the DSN Settings for the CommServe database to point to the database in the SQL Server computer.

1. Open **Control Panel | Administrative Tools | Data Sources (ODBC)**.
2. Click the **System DSN** tab.
3. Click **<CommServe computer>_commserv** and then click **Configure**.
4. Edit the following values:
 - Name** - set it to *<SQL Server computer>_commserv*
 - Server** - set it to *<SQL Server computer>\BullCalypso*
5. Click **Next**.
6. Choose the **With SQL Server authentication using a login ID and password entered by the user** option.
7. Select the **Connect to SQL Server to obtain default settings for the additional configuration options** check box and enter the login and password of the *sa* user in the SQL Server computer.
8. Click **Next** twice and then click **Finish**. (Nothing needs to be changed on these dialog boxes.)
9. Click **Test Data Source**.

The result should be **TEST COMPLETED SUCCESSFULLY**.

If not make sure SQL server on the SQL Server computer is accessible and the login information given are correct.

12. Restart the services on the CommServe computer and re-enable jobs that were disabled.

10. Click **OK**.

To start the services:

1. Click the **Start** button on the Windows task bar and then click **All Programs**.
2. Navigate to **bull | Calypso** and click **Service Control Manager**.
3. Select **All Services** in **Services**.

4. Click **Start** to start all services.

To enable activity control:

1. From the CommCell Browser, right-click the **CommServe** and then click **Properties**.
2. Click **Activity Control** tab.
3. Select **Enable All Job Activity** and **Enable Scheduler** box.
4. Click **OK**.

PROTECTING THE DATABASE - SETTING UP THE DISASTER RECOVERY BACKUP

As Disaster Recovery Backup will not work in this setup, use the following steps to protect the database:

13. Disable the Disaster Recovery Backup schedule.
14. Install the File System *iDataAgent* on the SQL Server computer.
15. Using the File System *iDataAgent*, create a subclient which includes a script in the pre-scan phase to create a **.dmp** file of the **CommServ** database. Schedule regular backups of this subclient database from file system *iDataAgent*.
Recommended schedule is a daily full backup.
16. If you want a copy of the dump in a disk library (similar to Disaster Recovery Backup) copy the dump file to another location. This can be included in the post-backup phase.

Use the following steps to disable a schedule:

1. From the CommCell Browser, right-click the **<CommServe>**, point to **View** and then click **Schedules**.
2. Select and right-click the **DR Backup Full** schedule in the right pane and click **Disable**.
3. Click **Yes** to disable the schedule.

See Getting Started - Windows File System Deployment for more information.

Use the following command line in a batch file and attach the batch file as a PreBackup Process:

```
<sql install path>\sql.exe -S <SQL ServerName> -U
sa -P <sapwd> -q "BACKUP DATABASE [CommServ] TO DISK
= 'C:\cs.dmp'"
```

This should create a dump file c:\cs.dmp.

You can choose the folder in which the .dmp file is created.

RESTORING THE DATABASE

17. If you wish to recover the database, restore the dump file using the File System *iDataAgent* on the SQL Server computer and then recover the database using the **SQL Server Management Studio**.

INSTALLING UPDATES

Use the following steps to install updates on CommServe and SQL Server computers:

Perform the following steps to install updates on SQL Server computer:

1. Services on SQL Server computer are already disabled.
2. Navigate to the **<Service Pack>** directory.
3. Execute the following command:
`InstallUpdates.exe -doNotUpdateDB -nostartsvc -silent -vm Instance001`

Perform the following steps to install updates on CommServe computer:

1. Stop all services on the CommServe computer.
2. Navigate to the **<Service Pack>** directory.
3. Execute the following command:
`InstallUpdates.exe -nostartsvc -silent -vm Instance001`
4. If `PendingDBOperation` registry key is available at the following location on CommServe computer, then delete the key.
`HKEY_LOCAL_MACHINE\SOFTWARE\CommVault Systems\Galaxy\UpdateFlags\`
5. Start all the services on the CommServe computer.

UNINSTALLING UPDATES

Use the following steps to uninstall updates on Commserve and SQL Server computers:

Perform the following steps to install updates on CommServe computer:

1. Stop all services on the CommServe computer.
2. Navigate to the `Base` directory.
3. Execute the following command:

```
Removeupdates.exe -silent -nostartsvc -vm Instance001 -undo bin
```
4. If `PendingDBOperation` registry key is available at the following location on the CommServe computer, then delete the key.

```
HKEY_LOCAL_MACHINE\SOFTWARE\CommVault Systems\Galaxy\UpdateFlags\
```
5. Start all the services on the CommServe computer.

Perform the following steps to install updates on SQL Server computer:

1. Services on SQL Server computer are already disabled.
2. Navigate to the `Base` directory.
3. Execute the following command:

```
Removeupdates.exe -silent -nostartsvc -vm Instance001 -donotupdatedb
```

SEPARATE THE COMMSERVE FROM A COMMSERVE-MEDIAAGENT COMPUTER

In some situations you may want to separate the CommServe from a MediaAgent computer, (with or without a File system iDataAgent) if they were installed together. For example, you may want to move the CommServe to a more powerful computer or such similar re-configuration needs.

The following procedure provides step-by-step instructions on how to perform this operation.

You can also use this procedure to relocate a CommServe and MediaAgent which are installed together, to two separate computers.

You will require an additional MediaAgent license to perform this operation.

SOURCE COMPUTER

- | | | |
|----|--|--|
| 1. | Copy the index cache folder (and the job results folder if the (File system iDataAgent is installed) to another location. | |
| 2. | Perform a Disaster Recover Backup.

Verify and ensure that the Disaster Recovery Backup completes successfully. Also note down the location of the disaster recovery backup file. (For a more detailed discussion, see Phases of Disaster Recovery Backups.) | See Starting a Disaster Recovery Backup for step-by-step instructions. |
| 3. | Uninstall the software from the original computer. | See Uninstalling Components for more information. |



WARNING

Do not deconfigure the libraries (tape/optical/disk libraries, etc.) when you uninstall the MediaAgent software.

ESTABLISHING THE NEW COMMSERVE COMPUTER

- | | | |
|----|---|--|
| 4. | Install only the CommServe software in the new computer. | See CommServe Deployment for information on installing the CommServe software. |
| 5. | Restore the CommServe database using the CommServe Disaster Recovery Tool. | See Restore a Disaster Recovery Backup for step-by-step instructions. |
| 6. | Change the name of the CommServe computer using the CommServe Disaster Recovery Tool. | See Change the Name of the CommServe Computer for step-by-step instructions. |
| 7. | Inform the Client and MediaAgent computers of the new CommServe name. This can be done from the <i>CommCell Console</i> . | See Informing Clients of CommServe Name Change for step-by-step instructions. |

ESTABLISHING THE NEW MEDIAAGENT COMPUTER

- | | | |
|-----|--|---|
| 8. | Install only the MediaAgent software in the old computer.
(You can also relocate the MediaAgent to another computer, if necessary.) | See MediaAgent Deployment for more information. |
| 9. | During MediaAgent installation make sure to specify the index cache to the location in which it was copied in step 1. If you are unable to do so, perform the steps described in Manually Relocate the Index Cache. | |
| 10. | Open the CommCell Console and change the MediaAgent name associated with the library.

If you have a disk library, make sure that the mount path is pointing to the appropriate location. If necessary move the mount path to the appropriate location and then change the location of the mount path. | See Changing the MediaAgent (Host) Associated with a Library for step-by-step instructions.

See Move a Mount Path for step-by-step instructions. |
| 11. | Deconfigure the original MediaAgent from the CommCell Console. | See Deconfigure a Client, MediaAgent, Agent, or Enabler for step-by-step instructions. |

ESTABLISHING THE FILE SYSTEM /DATAAGENT IN THE MEDIAAGENT COMPUTER (IF IT WAS ORIGINALLY INSTALLED)

- | | | |
|-----|--|--|
| 12. | Export the metadata records associated only with this client on the CommServe. | See Export Data from the Source CommCell for step-by-step instructions. |
| 13. | Deconfigure the Client from the CommCell Console. | See Deconfigure a Client, MediaAgent, Agent, or Enabler for step-by-step instructions. |
| 14. | Delete the Client in the CommCell Console. | See Delete a Client Computer for step-by-step instructions. |
| 15. | Import the metadata records (that was exported in step 12) associated with the client computer in the CommServe. | See Import Data on the Destination CommCell for step-by-step instructions. |
| 16. | Reinstall the file system iDataAgent on the computer. | See Deployment - Windows File System iDataAgent for more |

information.

Web Administration

TABLE OF CONTENTS

Overview

Configuring IIS for Windows Server 2008

Configuring Web Administration

Configuring the CommServe Computer

Configuring an Alternate Computer


Configuring the CommCell Console to Launch Books Online

Configuring Reports for Web Administration

Configuring an Alternate Computer for Launching Stand-Alone Add Ins

OVERVIEW

The CommCell Console software provides several configuration options for web administration. These options provide the facility to:

- Access the CommCell Console as a remote web-based application.
- Launch a downloaded copy of Books Online from the CommCell Console's  icon.

The following sections describe the various web administration options available, as well as the requirements for each configuration.

CONFIGURING IIS FOR WINDOWS SERVER 2008

Use the following steps to configure the server features and roles needed to enable IIS on a Windows Server 2008 computer:

1. Click the **Start** button, and then click **Server Manager** from the menu
2. In left pane of the **Server Manager** window, right-click **Roles**, and then click **Add roles**.
3. In the **Add Roles Wizard** window, click **Next**.
4. Select the **Web Server (IIS)** check box, and then click **Next**.
5. An overview of the Web Server role is provided. Click **Next**.
6. On the **Role Services** page, the following check boxes are automatically selected under **Common HTTP Features**:
 - Static Content
 - Default Document
 - Directory Browsing
 - HTTP Errors

Ensure to select the **HTTP Redirection** check box.
7. Under **Application Development**, select the following check boxes:
 - ASP.NET
 - ASP
 - CGI

If you are prompted to add required role services, click **Add Required Role Services**.

8. Under **Security**, select the **Basic Authentication** and **Windows Authentication** check boxes.
9. Under **Management Tools**, select the **IIS 6 Management Capability** check box. This will include the following role services:
 - IIS 6 Metabase Compatibility
 - IIS 6 WMI Compatibility
 - IIS 6 Scripting Tools
 - IIS 6 Management Console
10. Click **Next** to proceed to the confirmation page, and then click **Install**.

Once the installation completes, click **Close**.

CONFIGURING WEB ADMINISTRATION

RELATED TOPICS

CommCell Console

Provides basic information about CommCell Console.

The stand-alone CommCell Console software installation provides an option to configure the CommCell Console for web administration provided IIS is installed and running on the computer. When configured, the CommCell Console can be automatically accessed as a remote web-based application from any computer capable of communicating with the CommServe computer.

If the computer on which the stand-alone CommCell Console software is installed does not have IIS installed or was not configured for web administration during installation, you can configure web administration at a later time. This configuration can be performed on either:

- the original computer on which the stand-alone version of the CommCell Console software was installed.
- an alternate computer that is capable of communicating with the CommServe computer.

Note that the computer must have a Java-enabled web browser with the correct version of JRE installed. See System Requirements - CommCell Console as a Remote Web-Based Application for more information.

- Remote access to the CommServe may not be available for computers running outside of a firewall. To enable web access to the CommServe in this scenario, you must enable the firewall port specified in Microsoft Internet Information Service (IIS) Web Server on the CommNet Server. (By default, this port is 80.)
- The Java Web Start application may fail to launch if the Java cache contains corrupted files. To resolve this issue, open the Java Control Panel (located in the Windows Control Panel) and delete all Temporary Internet Files. Then, close and relaunch the CommCell Console.

The following sections describe each option in detail.

CONFIGURING THE COMMSERVE COMPUTER

If the CommServe computer did not have IIS installed during installation of the stand-alone CommCell Console, the CommServe computer can be configured for web administration at a later time. Once configured, the CommCell Console can then be run as a remote web-based application using the CommServe as the required IIS source.

Before you Begin:

- This procedure is not required if the CommServe computer was configured for web administration during the software installation.

▶ To configure the CommServe Computer for web administration:

1. Logon to the CommServe computer as an Administrator or a member of the Administrator's group.
2. Install the stand-alone CommCell Console software on the CommServe computer.

If IIS is already installed and running during the CommCell Console software installation, then the software installation will provide the necessary options to configure web administration. The web configuration process will be complete once the software installation completes.

The CommServe computer is now configured for web administration.

CONFIGURING AN ALTERNATE COMPUTER

If it is not desirable to use the CommServe computer as the IIS source for web administration, an alternate computer capable of communicating with the CommServe computer can be used instead. Once configured, the CommCell Console can be run as a remote web-based application using the alternate computer as the required IIS source.

For example, a CommServe computer named **green** does not have IIS installed. However, another computer in the network named **blue** does have IIS installed and the IIS services are running. The CommCell Console can then be configured to run as a remote web-based application using **blue** as the required IIS source. Once **blue** is configured, the CommCell Console can be accessed as a remote web-based application by typing the following in the web browser:

```
http://blue/<commcell_console_web_alias_name>
```

To configure the CommCell Console as a remote web-based application on a computer other than the CommServe computer, the following requirements must be met:

- The alternate computer must have IIS and the stand-alone CommCell Console software installed and running.
- The CommCell Console must be configured to use the alternate computer's IIS.

Before you Begin:

- This procedure is not required if the CommServe computer was configured for web administration during the software installation.


▶ To configure the CommServe Computer for web administration:

1. Logon to the computer as an Administrator or a member of the Administrator's group.
2. Install the stand-alone CommCell Console software on the alternate computer.

If IIS is already installed and running during the CommCell Console software installation, then the software installation will provide the necessary options to configure web administration. The web configuration process will be complete once the software installation completes.

The alternate computer is now configured for web administration.

CONFIGURING THE COMMCELL CONSOLE TO LAUNCH BOOKS ONLINE

By default, the CommCell Console's  button is configured to launch Books Online directly from the documentation web site. However, it may be necessary to access Books Online from the CommCell Console without an available internet connection. This can be achieved by downloading Books Online onto a local computer and configuring the button to launch Books Online from the downloaded copy. (See Download Books Online for more information on downloading Books Online).

The CommCell Console can be configured to launch Books Online from one of two places:

- a shared network location
- a locally hosted intranet site

Before you Begin:

- If you are configuring the CommCell Console to launch Books Online from an intranet site, the computer hosting the intranet site must have Internet Information Service (IIS) installed and enabled.
- Refer to Accessing Books Online for additional information on the available options for accessing Books Online.

▶ To configure the CommCell Console to launch Books Online:

1. From the **Tools** menu in the CommCell Console, click **Control Panel**.
2. From the **Control Panel** window, click **E-Mail & IIS Configuration**.
3. Click the IIS Server tab.
4. Click the **Use Alternate URL for Online Help** checkbox.
5. Type the desired path to the locally hosted version of Books Online to be launched from the CommCell Console.
 - If Books Online is downloaded to a local or shared drive, the path should be entered as follows:


```
<location_of_downloaded_version_of_books_online>\bull\<software_version>\books_online_1\default.htm
```
 - If Books Online is downloaded and hosted on an intranet site, the path should be entered as follows:


```
http://<iis_server_name>/bull/<software_version>/books_online_1/default.htm
```
6. Click **OK** to save the information.
7. Restart the CommCell Console.

CONFIGURING REPORTS FOR WEB ADMINISTRATION

▶ To configure reports for web administration:

1. From the **Tools** menu in the CommCell Console, click **Control Panel**.
2. From the **Control Panel** window, click **E-Mail & IIS Configuration**.
3. Click the IIS Server tab.
4. Click the **Use Alternate IIS Server for Reports** checkbox.
5. Type the name of the computer that has the Internet Information Service (IIS) installed.
6. Type the desired web alias in the **Alias** box, if it is different from the one displayed.
7. Type the non-default port number, if the default port is not suitable for your environment. Depending on the protocol, enter the port number accordingly. Refer to the following:
 - HTTP:** The default is port 80. If using this protocol, and a different port number is required: Select this option, and type a different port number.
 - HTTPS:** The default is port 443. If using this protocol, and a different port number is required: Select this option, and type a different port number.
8. Type the installation path in the **Software Installation Path on IIS Server** box or click the **Browse** button to select the path.
9. Click the **Change** button to add a login and password to access the IIS Server.
10. Click **OK** to save the information.

CONFIGURE AN ALTERNATE COMPUTER FOR LAUNCHING STAND-ALONE ADD-INS

Before you Begin:

- The alternate computer must have the CommCell Console installed and configured for web administration, as well as Internet Information Service (IIS) installed and enabled.
- This procedure can be used for launching the Outlook and Lotus Notes Add-Ins.

▶ To configure an alternate computer for Add-In Java updates:

1. From the **Tools** menu in the CommCell Console, click **Control Panel**.
2. From the **Control Panel** window, click **E-Mail & IIS Configuration**.
3. Click the IIS Server tab.
4. Click the **Use Alternate IIS Web URL for Add-in** checkbox.
5. Type the path to the alternate computer's web alias. The path should be entered as follows:

`http://<alternate_computer_iis_server_name>/<web_alias>`

The alternate computer specified in the **Use Alternate IIS Web URL for Add-in** field will also be used as the source for obtaining Java updates for Outlook and Lotus Notes Add-In clients.

6. Click **OK** to save the information.

[Back To Top](#)

CommCell Views

Topics | How To | How Do I

TABLE OF CONTENTS

Overview

Views

- CNClientInfoView
- CNMMMediaInfoView
- CommCellAdminSchedule
- CommCellAuxCopyInfo
- CommCellBackupInfo
- CommCellBkSchedule
- CommCellBkupSizeInfo
- CommCellBkScheduleInfo
- CommCellClientConfig
- CommCellClientFSFilters
- CommCellClientLevelBkpJobSummary
- CommCellClientVersion
- CommCellCompletedBkpJobsInfo
- CommCellDriveInfo
- CommCellJobController
- CommCellJobControllerCount
- CommCellLibraryInfo
- CommCellLibraryReservInfo
- CommCellLicense
- CommCellMAVersion
- CommCellMediaAgentInfo
- CommCellMediaInDrives
- CommCellMediaInfo
- CommCellPrePostCmdInfo
- CommCellRestoreInfo
- CommCellRetentionInfo
- CommCellStoragePolicy
- CommCellSubClientConfig
- CommCellUpdateInfo

OVERVIEW

CommCell Views provides a way to query information on the CommCell components directly from the SQL database.

You can use these default views, or you can create or customize the existing views to reflect the data in your organization. The views are created by querying the database. These query are by default displayed in SQL Enterprise Manager. You can also use products such as Crystal Reports, Microsoft Reporting Services and/or Microsoft Excel to format your query output.

If you modify a view or create a new view, you must reapply them after each new release.

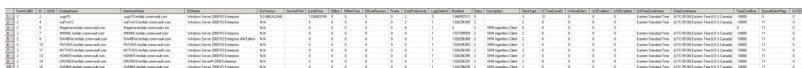
VIEWS

The following view options are available in the CommCell.

CNCLIENTINFOVIEW

The CNClientInfoView provides detailed information about each client in the CommCell.

The following image displays a sample CNClientInfoView:



Column	Description
CommCell ID	The identifier for the CommCell.
ID	The identifier for the client.
GUID	The globally unique identifier for the client.
DisplayName	The name of the client.
InterfaceName	The fully qualified name of the client.
OSName	The name of the operating system that is installed on the client.
SWVersion	The version of the software that is installed on the client.
ServicePack	The service packs that are installed.
InstallTime	The date and time on which the software was installed on the client.

Offline	Whether the client is offline. An online machine is indicated with 0. An offline machine is indicated with 1.
OfflineTime	The time at which the client went offline.
OffLineReason	The reason that the client is offline.
Priority	The priority of the job.
DataProtActivity	Whether data protection is enabled for the client.
LogDeleted	Whether the client's log has been deleted.
Modified	The date and time on which the client was last modified.
Status	The status of the client.
Description	A user-created description of the client.
ClientType	Whether the client is a secondary storage client or a primary storage client.
CCTimeZoneID	The identifier for the time zone.
IsVirtualClient	Whether the client is a virtual client.
IsCIEEnabled	Whether Content Indexing is enabled at the client level.
IsSBEnabled	Whether Snap Protection is Enabled at the client level.
StdTimeZoneName	The standard name of the time zone that is sent on the client.
TimeZoneName	The time zone that is set on the client.
TimeZoneBias	The number of seconds that the client time zone is offset from the Coordinated Universal Time (UTC).
SpecialClientFlags	An integer of bit flags for the client.
IsVSDC	Whether the client is discovered by a virtual server.

CNMMEDIAINFOVIEW

The CNMMediaInfoView provides detailed information about media in the CommCell.

The following image displays a sample CNMMediaInfoView:



Column	Description
MediaID	The unique ID generated when the media was discovered.
BarCode	The barcode label on the media.
MediaTypeID	The identifier for the media type.
CreationTime	The date and time at which the media was discovered.
NumberOfReUses	The number of times that the media can be reused.
LastExportTime	The last time that the media was moved to an outside storage location.
MediaLocationType	Whether the media
MediaLocation	The location of the media. <ul style="list-style-type: none"> If the media is inside the library, indicates whether the media is available in a storage slot or a drive. If the media is exported, indicates the outside storage location recorded by the user, when the media was exported.
retentionFlags	Whether media is flagged for retention.
retentionExpireTime	The date and time at which media with extended retention expires.
MediaFlags	An integer of bit flags for media properties.
MediaStatusReason	The reason for the current media status is set.
Attributes	The attributes associated with the media.
IsAged	Whether the media has been aged.
LibraryID	The identifier for the library in which the media is located.
LibraryName	The name of the library in which the media is located.
SpareGroupId	The identifier for the spare group to which the media belongs, if applicable.
SpareGroupName	The name of the spare group to which the media belongs, if applicable.
ExportLocationType	The type of outside storage location to which media is exported, if applicable.
ExportLocationId	The identifier for the outside storage location to which media is exported, if applicable.
ExportLocation	The outside storage location recorded by the user, when the media was exported.
ContainerId	The identifier of the physical container for the media.
ContainerName	The name of the physical container for the media.
LastRestoreTime	The last time that data was restored from the media.
LastBackupTime	The last time that data was backed up to the media.
PinMediaExpireTime	The expiration time for a pinned media.
TotalSpaceMB	The total amount of used and free space on the media in megabytes.
TotalFreeSpaceMB	The total amount of free space on the media in megabytes.
TotalCVDataSizeMB	The total amount of space that is consumed by data protections.
ArchGroupID	The identifier for the storage policy.
ArchGroupCopyId	The identifier for the storage policy copy.
GroupType	The identifier for the media group type.
MediaStatus	The status of the media.
LastWriteLibraryID	The identifier for the library that contains the last written data.
IsInMediaGroup	Whether the media is assigned.
TotalNumberOfSoftErrors	The total number of software errors reported on the media.
TotalNumberOfHardErrors	The total number of hardware errors reported on the media.
Description	User-created description of the media.
origCCCommCellId	If the client is migrated from a CommCell that is different than the local CommCell, this is the identifier for the original CommCell, from which the client migrated.

COMMCELLADMINSCCHEDULE

The CommCellAdminSchedule view provides information about scheduled administrative jobs.

The following image displays a sample CommCellAdminSchedule view:

scheduleid	scheduletask	schedtype	sp_id	sp	sp_dest_copy_id	sp_dest_copy	sp_src_copy_id	sp_src_copy
3	Administration	DR Full Backup	0	not apply	0	not apply	0	not apply
4	Administration	Data Aging	0	not apply	0	not apply	0	not apply
8	Administration	Download Updates	0	not apply	0	not apply	0	not apply
10	Administration	Install Updates	0	not apply	0	not apply	0	not apply
36	Administration	Install Updates	0	not apply	0	not apply	0	not apply
37	Administration	Install Updates	0	not apply	0	not apply	0	not apply
39	Administration	Install Updates	0	not apply	0	not apply	0	not apply
49	Administration	Install Updates	0	not apply	0	not apply	0	not apply

Column	Description
scheduleid	The unique schedule ID.
scheduletask	The type of scheduled task (administration).
schedtype	The type of schedule (e.g., disaster recovery, data aging, auxiliary copy, reports, etc.).
sp_id	The unique storage policy ID.
sp	The storage policy name.
sp_dest_copy_id	The unique ID for the destination copy.
sp_dest_copy	The destination copy.
sp_src_copy_id	The unique ID for the source copy.
sp_src_copy	The source copy.
streams	The number of streams used.
schedpattern	The scheduling pattern (One Time, Daily, Weekly, Monthly or Yearly).
schedinterval	The schedule occurrences based on the schedule pattern.
schedday	The scheduled day based on the schedule pattern.
schedtime	The scheduled start time.
schednexttime	The next scheduled time.

COMMCELLAUXCOPYINFO

The CommCellAuxCopyInfo view provides information about auxiliary copy jobs.

The following image displays a sample CommCellAuxCopyInfo view:

auxcopyjobid	storagepolicy	sourcecopyid	sourcecopy	destcopyid	destcopy	jobinitfrom	jobstatus	startdateunixsec
173	Lin_mag	9	Primary	17	copy2	Gui	Success	1178821232
205	ranger-tape1	16	primary	21	secondary	Gui	Success	1178822892
208	Lin_mag	9	Primary	17	copy2	Gui	Success	1178822965
212	formax-tape1	15	primary	22	secondary	Gui	Success	1178823350
364	Lin_mag	9	Primary	17	copy2	Schedule	Success	1178863203
*	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

Column	Description
auxcopyjobid	The Job ID of the auxiliary copy job.
storagepolicy	The name of the storage policy that was used to perform the auxiliary copy job.
sourcecopyid	The unique ID for the source copy.
sourcecopy	The storage policy copy that data was copied from during the auxiliary copy job.
destcopyid	The unique ID for the destination copy.
destcopy	The storage policy copy that data was written to during the auxiliary copy job.
jobinitfrom	Where the operation was initiated.
jobstatus	The result of the auxiliary copy job, either Success, Killed, Failed, or Failed to Start.
startdateunixsec	The start date and time of the auxiliary copy job. This time represents the number of seconds that have elapsed since 1970.
enddateunixsec	The end time of the auxiliary copy job. This time represents the number of seconds that have elapsed since 1970.
startdate	The start date and time of the auxiliary copy job.
enddate	The end date and time of the auxiliary copy job.
bytesxferred	The amount of data (in bytes) that was written to media during the auxiliary copy job.

COMMCELLBACKUPINFO

The CommCellBackupInfo view provides information about the backup jobs.

The following image displays a sample CommCellBackupInfo view:

jobid	appid	jobinitf...	clientn...	idataagent	instance	b...
360	15	Gui	sogo6	Windows 6...	DefaultI...	Mt
361	16	Gui	sogo6	Windows 6...	DefaultI...	Mt
362	17	Gui	sogo6	Windows 6...	DefaultI...	Mt
*	NULL	NULL	NULL	NULL	NULL	NULL

Column	Description
jobid	The unique Job ID of the backup job.
appid	The unique subclient ID.
jobinitfrom	Where the operation was initiated.
clientname	The client computer name.
idataagent	The iDataAgent name.
instance	The name of the instance that conducted the backup job. If the instance option is not applicable for an iDataAgent, the

	information is displayed as NULL.
backupset	The backupset name.
subclient	The subclient name.
data_sp	The storage policy name.
backuplevelint	The backup level initialization
backuplevel	The backup type that was selected. Backup types can be Full, Incremental, Differential or Synthetic Full.
incrlevel	The incremental levels for Informix and Oracle backup jobs.
jobstatusint	The job status initialization.
jobstatus	The status of the job. Job status can be Success, Killed, Failed, or Failed to Start.
jobfailedreason	The reason the backup job failed.
startdateunixsec	The UNIX start date and time of the backup job. This time represents the number of seconds that have elapsed since 1970.
enddateunixsec	The UNIX date and end time of the backup job. This time represents the number of seconds that have elapsed since 1970.
startdate	The start date and time of the backup job.
enddate	The end date and time of the backup job.
durationunixsec	The duration of UNIX seconds
duration	The length of time for the backup operation to complete.
numstreams	The number of data channels used by the storage policy to perform the backup.
numbytesuncomp	The amount of uncompressed data.
numbytescomp	The amount of compressed data.
numobjects	The number of objects that were backed up for the associated job.
isaged	The IS aged
isagedstr	The IS aged string

COMMCELLBKSCHEDULEINFO

The CommCellBkScheduleInfo view provides information about the scheduled jobs.

The following image displays a sample CommCellBkScheduleInfo view:

CommCellID	CommCellName	scheduleid	scheduleName	schedu...	schedba...	schedpa
000F73DC	warriors_cn	1436	ALL-2100-All-Fulls	Backup	Full	Daily
000F73DC	warriors_cn	1437	ALL-2100-Tue+Inc	Backup	Full	Weekly
000F73DC	warriors_cn	1438	ALL-2100-Tue+Inc	Backup	Incremental	Weekly
000F73DC	warriors_cn	1443	WIN2K3-32-210...	Backup	Full	Weekly
000F73DC	warriors_cn	1444	WIN2K3-32-210...	Backup	Differential	Weekly
000F73DC	warriors_cn	1445	SQL-2100-Tue+...	Backup	Full	Weekly
000F73DC	warriors_cn	1446	SQL-2100-Tue+...	Backup	Differential	Weekly
000F73DC	warriors_cn	1453	WIN2K3-32-210...	Backup	Full	Weekly
000F73DC	warriors_cn	1454	WIN2K3-32-210...	Backup	Differential	Weekly
000F73DC	warriors_cn	1456	WIN2K3-32-210...	Backup	Full	Weekly

Column	Description
commcellid	The unique CommCell ID.
commcellname	The CommCell name
scheduleid	The unique schedule ID.
schedulename	The schedule name.
schedulotask	The schedule task (backup)
schedulebackuptype	The scheduled backup type (Full, Incremental, Differential, or Synthetic Full).
schedulepattern	The scheduling pattern (One Time, Daily, Weekly, Monthly or Yearly).
scheduleinterval	The schedule occurrences based on the schedule pattern.
schedulebackupday	The schedule day based on the schedule pattern.
schedbackuptime	The scheduled start time.
schedulenextback	The next scheduled time.
appid	The unique subclient ID.
clientname	The client computer name.
idataagent	The iDataAgent name.
instance	The instance name.
backupset	The backupset name.
subclient	The subclient name.

COMMCELLBKSCHEDULE

The CommCellBkSchedule view provides information about the scheduled backup jobs.

The following image displays a sample CommCellBkSchedule view:

CommCellID	CommCellName	sched...	schedulePo...
FFFFFFFF	sogo6	68	schedules for s...
FFFFFFFF	sogo6	69	My Schedul...
FFFFFFFF	sogo6	134	No Templat...
NULL	NULL	NULL	NULL

Column	Description
commcellid	The unique CommCell ID.
commcellname	The CommCell name.
scheduleid	The unique schedule ID.
schedulename	The scheduled name.
scheduletask	The scheduled task (backup).
schedbackuptype	The scheduled backup type (Full, Incremental, Differential, or Synthetic Full).
schedpattern	The scheduling pattern (One Time, Daily, Weekly, Monthly or Yearly).
schedinterval	The schedule occurrences based on the schedule pattern.
schedbackupday	The schedule day based on the schedule pattern.
schedbackuptime	The scheduled start time.
schednextbackuptime	The next scheduled time.
appid	The unique subclient ID.
clientname	The client computer name.
idataagent	The iDataAgent name.
instance	The instance name.
backupset	The backupset name.
subclient	The subclient name.

COMMCELLBKUPSIZEINFO

The CommCellBKSizeInfo view provides information about the backup size.

The following image displays a sample CommCellBKSizeInfo view:

JobId	Ap...	Client	iDataAgent	Instance	BackupSet	Subclient	Data_SP
10	23	linuxfdsm64bit	Linux File System	DefaultInstance...	defaultBackupSet	subclient_DC	storage_DC
31	33	idasol1	Notes Database	idasol1 domino...	defaultBackupSet	transaction l...	NULL
27	47	ida4_FS_SRMPS	SRM Agent For ...	DefaultInstance...	defaultBackupSet	default	NULL
87	78	w2k8innova	SRM Agent For ...	defaultInstance	defaultBackupSet	default	NULL
175	81	rhel5-32bit-n2	Unix File Archiver	DefaultInstance...	Test11	Test11	Mag_Lib_8542
76	88	calvin	SRM Agent For ...	DefaultInstance...	defaultBackupSet	default	NULL

Column	Description
jobid	The unique Job ID of the backup job.
appid	The unique subclient ID.
client	The client computer.
idataagent	The iDataAgent name.
instance	The instance name.
backupset	The backupset name.
subclient	The subclient name.
data_sp	The storage policy name.
backup_type	The type of backup.
last_bkp_appsize_without_index	The last backup size of data without index.
lastbkp_indexsize	The size of index in last backup.
lastbkp_totbkpsize	the total backup size of the last backup.
lastbkp_percentchange	The change in percentage of the last backup when compared to backup of similar type before the last backup.
iscompression	the IS compressed data or not.

COMMCELLCLIENTCONFIG

The CommCellClientConfig view provides information about the client configuration. This view also contains SRM Server data.

The following image displays a sample CommCellClientConfig view

ClientId	Client	NetworkInt.	OS [Version]	Hardware	GalaxyRelease	InstallTime	UninstallTime	DeletedTime	ClientStatus	ClientBkEnable	ClientPrtEnable
1	east	east.testla.	Windows Ser...	WinX64	9.0.0BUILD084	01/23/2012 22:14:38			installed	Yes	Yes
2	north_Node	north_Node	Windows Ser...	WinX64	9.0.0BUILD084	01/23/2012 22:14:32			uninstalled	N/A	N/A
3	south_Node	south_Node	Windows Ser...	WinX64	9.0.0BUILD084	01/23/2012 23:35:38			uninstalled	N/A	N/A
4	ida36-2008-r2	ida36-2008...	Windows Ser...	WinX64	9.0.0BUILD084	01/24/2012 12:40:53			installed	Yes	Yes
5	ida31-2008-64	ida31-2008...	Windows Ser...	WinX64	9.0.0BUILD084	01/24/2012 13:09:30			installed	Yes	Yes
6	ida40-2008-r2	ida40-2008...	Windows Ser...	WinX64	9.0.0BUILD084	01/24/2012 13:37:29			installed	Yes	Yes
7	ida39mcluste...	N/A	N/A	N/A	N/A	01/24/2012 15:17:14	01/24/2012 15:17:14	Deleted	N/A	N/A	
8	ida39mcluste...	N/A	N/A	N/A	N/A	01/24/2012 15:17:16	01/24/2012 15:17:16	Deleted	N/A	N/A	
9	ida39mcluste...	N/A	N/A	N/A	N/A	01/24/2012 15:35:01	01/24/2012 15:35:01	Deleted	N/A	N/A	
10	ida35m28	ida35m28...	Windows Ser...	WinX64	9.0.0BUILD084	01/24/2012 15:50:45			installed	Yes	Yes

Column	Description
clientid	The unique client ID.
client	The client computer name.
networkinterface	The default network interface through which the client communicates and transfers data to and from MediaAgent(s).
os [version]	The client computer operating system version and vendor.
hardware	The processor platform that runs the client computer and vendor.
galaxyrelease	The version of the software component installed on the computer
installtime	The date and time on which the software was installed on the client. Format: MM/DD/YYYY HH:MM:SS
uninstalltime	The date and time on which the software was uninstalled, if applicable. Format: MM/DD/YYYY HH:MM:SS
deletedtime	The date and time on which the software was deleted, if applicable. Format: MM/DD/YYYY HH:MM:SS
clientstatus	The status of the client (installed or uninstalled).

clientbkpenable	The activity of the backup operations at the client level. The activity displays Yes if enabled and No if disabled.
clientrstenable	The activity of the restore operations at the client level. The activity displays Yes if enabled and No if disabled.

COMMCELLCLIENTFSFILTERS

The CommCellClientFSFilters view provides information about the filters that are configured for a client.

The following image displays a sample CommCellClientFSFilters view:

CommC...	CommCellNa...	appid	clientname	idataagent	backupset	subclient
FFFFFFFF	sogo19_cn	1	sogo19_cn	CommServ...	DR-Backup...	DR Subclie
FFFFFFFF	sogo19_cn	1	sogo19_cn	CommServ...	DR-Backup...	DR Subclie
FFFFFFFF	sogo19_cn	1	sogo19_cn	CommServ...	DR-Backup...	DR Subclie

Column	Description
commcellid	The unique CommCell ID.
commcellname	The CommCell name.
appid	The unique subclient ID.
clientname	The client computer name.
idataagent	The iDataAgent name.
backupset	The backupset name.
subclient	The subclient name.
subclientstatus	The status of the subclient.
content	The subclient content.
global_exclude_filter	The directories and folders to be excluded from the backup operation for the subclient.
exclude_dirs	The directories to be excluded from the backup operation for the subclient.
exclude_files	The files to be excluded from the backup operation for the subclient.
except_dirs_to_exclude	The directories to be included in the backup operation for the subclient.
except_files_to_exclude	The files to be included in the backup operation for the subclient.

COMMCELLCLIENTLEVELBKPJOBSSUMMARY

The CommCellClientLevelBkpJobsSummary view provides a summary of information about backup jobs that ran at the client level over the last 30 days.

The following image displays a sample CommCellClientLevelBkpJobsSummary view:

ClientID	ClientName	TotalJobs	Completed	CompletedWithErrors	Killed	Failed	NoRun	Dropped	Other	SchedInitiated	TotalFullAppSizeGB	To
2	k.d.s9s9s9w_cn	0	0	0	0	0	0	0	0	0	0.0000	0.1
5	sogo23_2_cn	0	0	0	0	0	0	0	0	0	0.0000	0.1

Column	Description
ClientID	The unique client ID.
ClientName	The client computer name.
TotalJobs	Total number of jobs that ran on a client over the last 30 days.
Completed	Number of jobs completed.
CompletedWithErrors	Number of jobs completed with errors.
Killed	Number of jobs killed
Failed	Number of jobs failed
NoRun	Number of jobs which failed for activity disabled or maximum instance running etc.
Dropped	Number of jobs failed to start.
Other	Number of jobs completed or failed or killed etc.
SchedInitiated	Number of Schedule Task initiated.
TotalFullAppSizeGB	Total uncompressed backup size in GB for full backup jobs.
TotalIncAppSizeGB	Total uncompressed backup size in GB for incremental backup jobs.
TotalOtherAppSizeGB	Total uncompressed backup size in GB for differential or synthetic backup jobs.
TotalAppSizeGB	Total of all backup jobs run - full/incremental/differential/synthetic jobs.
TotalFullBkpSizeGB	The total size of the full backup.
TotalIncBkpSizeGB	The total size of the incremental backup.
TotalOtherBkpSizeGB	The total size of the differential/synthetic backup.
TotalBkpSizeGB	The total size of the backup job.
ProtectedObjects	Total number of files backed up.
FailedObjects	Total number of files failed to scan or backup etc.
FailedFolders	Total number of folders failed to scan/backup etc.
StartTime	The time of the backup job started.
EndTime	The time of the backup job ended.

COMMCELLCLIENTVERSION

The CommCellClientVersion view provides information about the software version, status, and updates that are installed on the client computer.

The following image displays a sample CommCellClientVersion view:

	Name	ClientGroups	Version	AdditionalUpdates	Status
1	1touchcc	"efay"	9.0 SP6a	No	Unknown
2	1touchsvr2	"efay"	9.0 SP6a	Yes	Unknown
3	adams64	"surya"	9.0 SP6	Yes	Has Diagnostic Updates
4	animal	""	9.0	No	N/A
5	archiver2008-32_2	"Huixia"	9.0 SP5b	Yes	Has Diagnostic Updates
6	bird	"Huixia"	9.0 SP6b	Yes	Needs Update
7	bleye	""	9.0	N/A	N/A
8	cat	"surya"	9.0 SP5a	Yes	Needs Update
9	chitravm1	""	9.0 SP6	Yes	Needs Update
10	ContentStore_sapcs1	""	9.0	No	N/A

Column	Description
name	The client computer name.
clientgroups	The name of the client group to which the client computer belongs.
version	The version of the software component installed on the computer.
additionalupdates	Whether the version of the software component installed on the computer requires updates.
status	The status of the software component installed on the computer (needs update, has diagnostic updates, or unknown).

COMMCELLCOMPLETEDBKPJOBSINFO

The CommCellCompletedBkpJobsInfo view provides information about client level backup jobs.

The following image displays a sample CommCellCompletedBkpJobsInfo view:

ClientID	ClientName	TotalBkpJobs	TotalFullBkpJobs	TotalIncBkpJobs	TotalOtherBkpJobs	TotalBkpSizeGB	TotalFullBkpSizeGB	TotalIncBkpSizeGB	TotalOtherBkpSizeGB
1	kd99nl_cn	4	4	0	0	2.75	2.75	0.00	0.00
2	kd902_3_cn	1	1	0	0	1.76	1.76	0.00	0.00
3	kd90_3_cn	1	1	0	0	0.26	0.26	0.00	0.00
4	chame1_cn	1	1	0	0	2.69	2.69	0.00	0.00

Column	Description
ClientID	The unique client ID.
ClientName	The client computer name.
TotalBkpJobs	Number of backup jobs ran on a client computer.
TotalFullBkpJobs	Number of Full backup jobs ran on a client computer.
TotalIncBkpJobs	Number of Incremental backup jobs ran on a client computer.
TotalOtherBkpJobs	Number of Other backup jobs ran on a client computer.
TotalBkpSizeGb	The total size of the backup.
TotalFullBkpSizeGB	The total size of the full backup.
TotalIncBkpSizeGB	The total size of the incremental backup.
TotalOtherBkpSizeGB	The total size of the other backup.

COMMCELLDRIVEINFO

The CommCellDriveInfo view provides information about drives.

The following image displays a sample CommCellDriveInfo view:

MName	LibName	DriveName	DriveAliasName	DriveB
age.racks	Library4	Lib4_Drive3	IBM ULTRIUM-...	NO
ma018...	Library4	Lib4_Drive4	IBM ULTRIUM-...	NO
ma018...	Library4	Lib4_Drive5	IBM ULTRIUM-...	NO
ma018...	Library4	Lib4_Drive6	IBM ULTRIUM-...	NO
ma018...	Library4	Lib4_Drive7	IBM ULTRIUM-...	NO

Column	Description
maname	The media agent name.
libname	The library name
drivename	The drive name
drivealiasname	The alternative name assigned to the drive.
drivebroken	The drive broken status
cleaning reqd	The drive cleaning requirement
drivestatus	The drive status
driveofflinereason	The reason drive is offline
offlinetimestamp	The drive offline time stamp.

COMMCELLJOBCONTROLLER

The CommCellJobController view provides information about active jobs.

The following image displays a sample CommCellJobController view:

TREEFROG.COM_ntroller													
jobID	operation	clientComputer	agentType	subclient	jobType	phase	storagePolicy	mediaAgent	status	progress	errors	delayReason	description
1	95	Snap Backup	treefrog	Virtual Server	Sub06	Full	Backup	DiskLibray1	treefrog_on	Success	0		
2	97	Snap Backup	treefrog	Virtual Server	Sub07	Full	Backup	DiskLibray2	treefrog_on	Success	0		

Column	Description
jobid	The unique ID of the job.
operation	The type of operation.
clientComputer	The name of the client computer.
agentType	The agent that is performing the operation. (e.g. Windows 2000 File System)
subclient	The subclient that was protected during the operation.
jobType	The type of operation that is being conducted on data.
phase	The current phase of the operation. The number of phases varies depending on the operation.
storagePolicy	The storage policy to which the operation is being directed.
mediaAgent	The MediaAgent to which the operation is being directed.
status	The status of the operation.
progress	A status bar indicating progress. The progress bar is not visible for certain operations or for initial phases of some data protection operations.
errors	Displays any errors that have occurred during the operation.
delayReason	The description of the reason why the operation may be pending, waiting, or failing.
description	A brief description of the running job.

COMMCELLJOBCONTROLLERCOUNT

The CommCellJobControllerCount view provides information about active jobs. This view also contains SRM Server data.

The following image displays a sample CommCellJobControllerCount view:

TREEFROG.COM_ntrollerCount							
commcellid	jobtype	numofpending	numofwaiting	numofstopped	numofqueued	numofrunning	
2	Backup	0	0	1	0	0	
2	Restore	0	0	0	0	1	
*	NULL	NULL	NULL	NULL	NULL	NULL	NULL

Column	Description
commcellid	The unique ID of the CommCell.
jobtype	The type of operation.
numofpending	The number of jobs pending.
numofwaiting	The number of jobs waiting.
numofstopped	The number of jobs stopped.
numofqueued	The number of jobs queued.
numofrunning	The number of jobs running.

COMMCELLLIBRARYINFO

The CommCellLibraryInfo view provides information about library name and status details.

The following image displays a sample CommCellLibraryInfo view:

LibName	LibAliasName	LibStatus
Library2	MBU i2000 Waffle	Enable
Library4	MBU i2000 Waffle	Enable
Library4	MBU i2000 Waffle	Enable
Library4	MBU i2000 Waffle	Enable
Library4	MBU i2000 Waffle	Enable
Library4	MBU i2000 Waffle	Enable
Library4	MBU i2000 Waffle	Enable
Library4	MBU i2000 Waffle	Enable
Library4	MBU i2000 Waffle	Enable
Library4	MBU i2000 Waffle	Enable
Library4	MBU i2000 Waffle	Enable
Library4	MBU i2000 Waffle	Enable
Library4	MBU i2000 Waffle	Enable
MagLibrary5	MagLib52	Enable

Column	Description
libname	The name of the library.
libaliasname	The alternative name assigned to the library.
libstatus	The status of the the library.
libbroken	yes or no.
libstatusreason	The status reason of library.
offlinetimestamp	The offline timestamp of the library management.

COMMCELLLIBRARYRESERVINFO

The CommCellLibraryReservInfo view provides information about active jobs and their respective media and drive reservation details.

The following image displays a sample CommCellLibraryReservInfo view:

TREEFROG\COM...ryReservInfo						
jobId [reservId...]	MA [status]	libAlias [libNam...]	driveAlias [driv...]	driveMountStat...	barcode type	elapsed
	forfax [Ready]	Fornax-Mag [Ma...	/extra/F-MAG [...]		CV_MAGNETIC ...	
	forfax [Ready]	Fornax-Ranger-...	QUANTUM DLT7...	Empty [14 14 3]	N/A N/A	
	forfax [Ready]	Fornax-Ranger-...	QUANTUM DLT7...	Empty [13 8 7]	N/A N/A	
	forfax [Ready]	Fornax-Ranger-...	QUANTUM DLT7...	Empty [14 8 17]	N/A N/A	
	forfax [Ready]	Fornax-Ranger-...	QUANTUM DLT7...	Empty [9 15 5]	N/A N/A	
	forfax [Ready]	Fornax-Ranger-...	QUANTUM DLT7...	Empty [5 8 4]	N/A N/A	
	forfax [Ready]	Fornax-Ranger-...	QUANTUM DLT7...	Empty [4 2 3]	N/A N/A	

Column	Description
jobId [reservId OP]	The job reserving the resource, its unique reservation ID number, and operation (e.g., backup, restore).
MA [status]	The name of the associated MediaAgent and its status.
libAlias [libName libStatus barcodeReaderPresent]	The alternative name assigned the library, the library name, its status (e.g., online) and if there is a barcode reader.
driveAlias [driveName driveStatus]	The alternative name assigned the drive in the library, the actual drive name and its status (e.g., online).
driveMountStatus [numMount numBackup numRestore]	The number of mounts, backups, and restores for the drive.
barcode type	The barcode reader and its type.
elapsed	The elapsed time of the reservation.

COMMCELLLICENSE

The CommCellLicense view provides information about the licenses consumed in the CommCell. This view also contains SRM Server data.

The following image displays a sample CommCellLicense view:

TREEFROG\COM...ncellLicense		
client	licenseName	licenseId
abany	DataAgent for L...	22
abany	DataAgent for ...	62
apple	DataAgent for ...	1
blommingdale	DataAgent for L...	3
blommingdale	DataAgent for L...	22
bootes	DataAgent for ...	1
bootes	DataAgent for ...	73
dowers	DataAgent for L...	3
dowers	DataAgent for L...	22

Column	Description
client	The name of the client computer that consumed the license.
licenseName	The license type.
licenseId	The unique license ID used by the software.

COMMCELLMAVERSION

The CommCellMAVersion view provides information about the software component version, status, and updates that are installed on each MediaAgent.

The following image displays a sample CommCellMAVersion view:

	Name	ClientGroups	Version	AdditionalUpdates	Status
1	adams64	"surya"	9.0 SP6	Yes	Has Diagnostic Updates
2	animal	""	9.0	No	N/A
3	archiver2008-32_2	"Huixia"	9.0 SP5b	Yes	Has Diagnostic Updates
4	bird	"Huixia"	9.0 SP6b	Yes	Needs Update
5	cat	"surya"	9.0 SP5a	Yes	Needs Update
6	chitravm1	""	9.0 SP6	Yes	Needs Update
7	cork	"Fw"	9.0 SP5b	Yes	Needs Update
8	csone_2	""	9.0	No	Needs Update
9	db2redhat1	""	9.0 SP6a	Yes	Needs Update
10	db2redhat2	""	9.0 SP6b	No	Needs Update

Column	Description
name	The media agent name.
clientgroups	The name of the client group to which the MediaAgent belongs.
version	The version of the software component installed on the MediaAgent.
additionalupdates	Whether the version of the software component installed on the MediaAgent requires updates.
status	The status of the software component installed on the MediaAgent (needs update, has diagnostic updates, or unknown).

COMMCELLMEDIAAGENTINFO

The CommCellMediaAgentInfo view provides information media- related information for each client.

The following image displays a sample CommCellMediaAgentInfo view:

CHELSEA\COMM...ediaAgentInfo				
Object Explorer Details				
	MAname	MAStatus	OfflineReason	OfflineTime
▶	chelsea_cn	Enable	Ready	121855141
	ma018-1.dfw1.s...	Disable	Ready	121140965
	ma018-2.dfw1.s...	Disable	Ready	121340673
	ma018-3.dfw1.s...	Disable	Ready	121564847
	ma018-4.dfw1.s...	Disable	Ready	121140964

Column	Description
maname	The media agent name.
mastatus	The media agent status.
offlinereason	The reason media agent is Offline.
offlinetimestamp	The time media agent was offline.

COMMCELLMEDIAINDRIVES

The CommCellMediaInDrives view provides a summary of the media currently available in each drive.

The following image displays a sample CommCellMediaInDrives view:

TREEFROG\COM...ediaInDrives									
Object Explorer Details									
	LibraryName	DriveName	MediaAgent	DriveOccupied	MountStatus	BarCode	MediaAttributes	SpareGroupName	StoragePolicyName
	Formax-Ranger-STK 9710	QUANTUM DLT7000_1	formax	1	Mounted	000126	Tape Media, Assigned, Active	Default Scratch	_sharepoint_formax_tape
	Formax-Ranger-STK 9710	QUANTUM DLT7000_2	formax	1	Mounted	000069	Tape Media, Assigned, Active	Default Scratch	JODI_DA
	Formax-Ranger-STK 9710	QUANTUM DLT7000_3	formax	1	Mounted	000117	Tape Media, Assigned, Active	Default Scratch	Sylvia_TAPE
	Formax-Ranger-STK 9710	QUANTUM DLT7000_4	formax	0					
	Formax-Ranger-STK 9710	QUANTUM DLT7000_5	ranger	0					
	Formax-Ranger-STK 9710	QUANTUM DLT7000_6	ranger	0					

Column	Description
libraryname	The name of the associated library.
drivename	The name of the drive associated with the media.
mediaagent	The name of the associated MediaAgent.
driveoccupied	Indicates the number of media occupying the associated drive.
mountstatus	Indicates the number of mounts.
barcode	The barcode reader.
mediaattributes	The attributes associated with the media.
sparegroupname	Indicates the name of the associated spare group.
storagepolicyname	The name of the associated storage policy.
copyname	The name of the associated copy.
retentioninfo	Information on retention for the associated media.
runningjobs	Information on running jobs.

COMMCELLMEDIAINFO

The CommCellMediaInfo view provides a summary of media-related information.

The following image displays a sample CommCellMediaInfo view:

TREEFROG\COM...ellMediaInfo									
Object Explorer Details									
	mediaid	mediabarcodes	mediagroupid	type	format	sidename	volumeid	volumename	blocksizeKB
▶	1	000152	0	DLTape IV	N/A	A_1	1	V_1	64
	2	000124	5	DLTape IV	DLT7000	A_2	2	V_2	64
	3	000019	0	DLTape IV	N/A	A_3	3	V_3	64
	4	001212	0	DLTape IV	N/A	A_4	4	V_4	64
	5	000154	0	DLTape IV	N/A	A_5	5	V_5	64
	6	000144	0	DLTape IV	N/A	A_6	6	V_6	64
	7	000194	0	DLTape IV	N/A	A_7	7	V_7	64
	8	000045	1	DLTape IV	DLT7000	A_8	8	V_8	64

Column	Description
mediaid	The unique ID generated when the media was discovered.
mediabarcodes	The barcode label of the media.
mediagroupid	The unique ID for the media group.
type	The hardware type of the media.
format	The recording format on the media.
sidename	The unique ID generated for each side of the media.
mediaCreationTime	The date and time at which the media was discovered.
volumeid	The unique volume ID for the media.
volumename	The volume name.
blocksizeKB	The size measured in bytes of each block in the media.
totalspaceMB	The total amount of space available in the media.
usedspaceMB	The amount of used space in the media.
freespaceMB	The amount of free space available in the media.
writenum	The number of times data has been written to the media.
reusenum	The number of times the media has been re-used.
mediastatus	The status of the media. Media status can be Good, Expired, Bad, or Invalid.
volumestatus	The current status of the volume. Volume status can be Active, Full, Idle, Read Only or Bad.
volumefullreason volumefulljobid	The reason the volume is full and job marking it as full.
location	The location of the media. <ul style="list-style-type: none"> • If the media is inside the library, indicates whether the media is available in a storage slot or a drive.

	<ul style="list-style-type: none"> If the media is exported, indicates the outside storage location recorded by the user, when the media was exported.
slotname	The slot number in which the media resides.
drivename	The drive name.
exportlocation	The outside storage location of the exported media recorded by the user when the media was exported.
lastwritetimeunixsec	The most recent time at which data was protected on the media. This time represents the number of seconds that have elapsed since 1970.
rawlastwritetime (not adjusted with daylight saving)	The most recent time at which data was protected on the media, not adjusted for daylight savings time.
lastwritetime	The most recent date and time at which data was protected on the media.
drivepoolname	The drive pool name.
library	The library name.
storagepolicy	The storage policy name.
storagepolycopy	The storage policy copy name.
retentiondays	The number of days data is kept before it is pruned.
fullcycles	The number of cycles data is kept before it is pruned.
LabelErrors	The number of labeling errors that a media has encountered.
ReadWriteErrors	The number of read, write errors that a media has encountered.

COMMCELLPREPOSTCMDINFO

The CommCellPrePostCmdInfo view provides information about the backup jobs.

The following image displays a sample CommCellPrePostCmdInfo view:

TREEFROG\COMM...										
client	appType	backupSet	instance	subclientName	preScanCommand	postScanCommand	preBkpCommand	postBkpCommand	userName	
1	sogo14vm1_cn	Windows File System	Browse	DefaultInstanceName	default	c:\preScan.bat	d:\postScan.bat	c:\postBkp.bat	c:\postBkp.bat	Local System Account
	bloom	Windows File System	Browse	DefaultInstanceName	default	d:\preScan.bat	c:\postScan.bat	e:\postBkp.bat	c:\postBkp.bat	Local System Account
	serp	Windows File System	Browse	DefaultInstanceName	default	c:\preScan.bat	d:\postScan.bat	c:\postBkp.bat	c:\postBkp.bat	Local System Account
	serp	Windows File System	Browse	DefaultInstanceName	default	d:\preScan.bat	c:\postScan.bat	e:\postBkp.bat	c:\postBkp.bat	Local System Account
	bloom	Windows File System	Browse	DefaultInstanceName	default	c:\preScan.bat	d:\postScan.bat	c:\postBkp.bat	c:\postBkp.bat	Local System Account

Column	Description
client	The client computer name.
appType	The application name.
backupset	The backupset name.
instance	The instance name.
subclientName	The subclient name.
preScanCommand	The pre scan process command.
postScanCommand	The post scan process command.
preBkpCommand	The pre backup process command.
postBkpCommand	The post backup process command.
userName	The user name used to run the command.

COMMCELLRESTOREINFO

The CommCellRestoreInfo view provides information about the restore jobs.

The following image displays a sample CommCellRestoreInfo view:

TREEFROG\COMM...RestoreInfo									
jobID	destclientname	idataagent	instance	backupset	jobstatus	jobfailedreason	starttimeunixsec	endtimeunixsec	
57	plum	Windows 32-bit ...		best-small	Success		1178809077	1178809126	
61	plum	Windows 32-bit ...		best-small	PartialSuccess		1178809232	1178809321	
70	plum	Windows 32-bit ...		best-small	Success		1178810685	1178810861	
74	serpens	Notes Database	Partition_00\ho...	defaultBackupSet	Success		1178811582	1178811635	
76	bloomingdale	Notes Database	Partition_00\ho...	defaultBackupSet	Killed	Killed by cvadmin.	1178811699	1178813636	
79	prune	Active Directory		defaultBackupSet	Success		1178812080	1178812116	
96	lime	Oracle Database	rman10g1	default	Success		1178815814	1178816006	
107	prune	Active Directory		defaultBackupSet	Success		1178817039	1178817077	

Column	Description
jobID	The unique job ID of the restore job.
destclientname	The name of the client to which the data was recovered.
idataagent	The name of the iDataAgent that conducted the restore job.
instance	The instance name.
backupset	The backupset name.
jobstatus	The status of the job (Success, Killed, Failed, or Failed to Start).
jobfailedreason	The reason the restore job failed.
starttimeunixsec	The UNIX start date and time of the restore job. This time represents the number of seconds that have elapsed since 1970.
endtimeunixsec	The UNIX end date and time of the restore job. This time represents the number of seconds that have elapsed since 1970.
starttime	The date and time at which the restore job was started.
endtime	The date and time at which the restore job was completed.
duration	The length of time for the restore operation to complete.
numfiles	The number of files that were recovered.
numbytescomp	The amount of data (in compressed bytes) that was recovered.
numbytesuncomp	The amount of data (in uncompressed bytes) that was recovered.

COMMCELLRETENTIONINFO

The CommCellRetentionInfo view provides information about each Retention information.

The following image displays a sample CommCellRetention view:

CommCellID	CommCellName	SpName	CopyName	Retention
FFFFFFFF	sogo19_cn	CommServeDR(r...	Primary	60
FFFFFFFF	sogo19_cn	Magnetic-Lib(rus...	Primary	Infinite
FFFFFFFF	sogo19_cn	Magnetic-Lib(rus...	Snap-primary	Infinite
FFFFFFFF	sogo19_cn	SP-Mag-SQL-1	Priamry	Infinite

Column	Description
commcellid	The unique ID for commcell.
commcellname	The commcell name.
spname	The storage policy name.
copyname	The storage policy copy name.
retentiondays	The number of retention days.
cycles	The number of cycles.
Isdataagingenabled	The Is data aging enabled on this copy.
Ismanageddiskspaceenabled	The disk space Is managed disk space enabled.

COMMCELLSTORAGEPOLICY

The CommCellStoragePolicy view provides information about each storage policy.

The following image displays a sample CommCellStoragePolicy view:

storagepolicy	defaultcopy	hardwarecompr...	maxstreams	drivepool	library	appid	clientname	idataagent
formax_tape	tape copy1	No	1	DrivePool(formax)1	Library1	110	starscream_wss...	SharePoint :
_sharepoint_for...	tape copy1	No	1	DrivePool(formax)1	Library1	111	starscream_wss...	SharePoint :
_sharepoint_for...	tape copy1	No	1	DrivePool(formax)1	Library1	141	shadowcat_wss3.0	Windows 32
_sharepoint_for...	tape copy1	No	1	DrivePool(formax)1	Library1	143	shadowcat_wss3.0	SharePoint :
_sharepoint_for...	tape copy1	No	1	DrivePool(formax)1	Library1	144	shadowcat_wss3.0	SharePoint :
_sharepoint_for...	tape copy1	No	1	DrivePool(formax)1	Library1	204	starscream_wss...	SharePoint :
_sharepoint_for...	tape copy1	No	1	DrivePool(formax)1	Library1	266	spweb2_moss2007	SharePoint :
_sharepoint_for...	tape copy1	No	1	DrivePool(formax)1	Library1	267	spweb2_moss2007	SharePoint :

Column	Description
storagepolicy	The storage policy name.
defaultcopy	The name of the default storage policy copy associated with the storage policy.
hardwarecompress	The hardware compression status. The status displays Yes if enabled and No if disabled.
maxstreams	The maximum number of data streams established for the storage policy.
drivepool	The name of the drivepool associated with the library to which the backup data from the default copy is directed.
library	The library name.
appid	The unique subclient ID.
clientname	The client computer name.
idataagent	The iDataAgent name.
instance	The name of the instance associated with the storage policy. If the instance option is not applicable for an iDataAgent, the information is displayed as NULL.
backupset	The backupset name.
subclient	The subclient name.

COMMCELLSUBCLIENTCONFIG

The CommCellSubClientConfig view provides information about subclient configuration.

The following image displays a sample CommCellSubClientConfig view:

appid	clientid	clientname	idataagent	idataagentstatus	idagentbkenable	idagentrstenable	instance	backupset
1	2	treefrog	CommServe Man...	installed	'NULL'	'NULL'		DR-Backup5
2	2	treefrog	Windows 64-bit ...	installed	Yes	Yes		defaultBacku
3	2	treefrog	Windows 64-bit ...	installed	Yes	Yes		Indexing Ba
4	3	formax	Solaris File System	installed	Yes	Yes		defaultBacku
5	3	formax	Solaris File System	installed	Yes	Yes		Indexing Ba
6	4	ranger	Solaris File System	installed	Yes	Yes		defaultBacku
7	4	ranger	Solaris File System	installed	Yes	Yes		Indexing Ba
13	6	serpens	AIX File System	installed	Yes	Yes		defaultBacku
14	6	serpens	AIX File System	installed	Yes	Yes		Indexing Ba

Column	Description
appid	The unique subclient ID.
clientid	The unique client ID.
clientname	The client computer name.
idataagent	The iDataAgent name.
idataagentstatus	The status of the iDataAgent (installed or uninstalled).
idagentbkenable	The activity of the backup operations at the iDataAgent level. The activity displays Yes if enabled and No if disabled.
idagentrstenable	The activity of the restore operations at the iDataAgent level. The activity displays Yes if enabled and No if disabled.
instance	The name of the instance. If the instance option is not applicable for an iDataAgent, the information is displayed as NULL.
backupset	The backupset name.

subclient	The subclient name.
subclientstatus	The status of the subclient (Valid or Deleted).
schedjobpattern	The backup scheduling pattern (One Time, Daily, Weekly, Monthly or Yearly).
schedbackupday	The backup scheduled start day.
schedbackuptime	The backup scheduled start time.
schednextbackuptime	The backup next scheduled time.
data_sp	The storage policy name.
data_sp_copy	The storage policy copy name.
data_sp_copy_retendays	The number of days data is kept before it is pruned.
data_sp_copy_fullcycles	The number of cycles data is kept before it is pruned.
data_sp_schedauxcopypattern	The scheduling pattern for the auxiliary copy operation.
data_sp_schedauxcopyday	The auxiliary copy scheduled day based on the schedule pattern.
data_sp_schedauxcopytime	The scheduled start time.
data_sp_schednextauxcopytime	The next scheduled time.
data_sp_scheddestcopy	The secondary copy.
log_sp	The storage policy associated with the database transaction logs.
LastFullBkpSize(Bytes)	The size of the last full backup.
LastIncBkpSize(Bytes)	The size of the last incremental backup.
LastDiffBkpSize(Bytes)	The size of the last differential backup.

COMMCELLUPDATEINFO

The CommCellUpdateInfo view provides information about the updates installed for each component in the CommCell. This view also contains SRM Server data.

The following image displays a sample CommCellUpdateInfo view:

TREEFROG\COM...ellUpdateInfo						
clientid	client [idataage...	galaxyrelease	installedSP	installedAdditio...	missingPatch	
56	albany [Unix Bas...	7.0.0(Build67)	0	0001,0002,0003...	None	
56	albany [Linux Fil...	7.0.0(Build67)	0	0007 [007]	None	
56	albany [DB2 on ...	7.0.0(Build67)	0	None [None]	None	
55	apple [Windows ...	7.0.0(BUILD67)	0	0014,0025,0028...	None	
55	apple [Java Gui]	7.0.0(BUILD67)	0	0011,0029, [29,]	None	
12	bloomingdale [U...	7.0.0(Build67)	0	0001,0002,0003...	None	
12	bloomingdale [Li...	7.0.0(Build67)	0	0007 [007]	None	
12	bloomingdale [N...	7.0.0(Build67)	0	0001,0002,0003...	None	

Column	Description
clientid	The unique client ID.
client [idataagent]	The client and components on which the updates are installed in the CommCell.
galaxyrelease	The version of the software component installed on the computer.
installedSP	The latest service pack and latest post service pack updates installed for each component in the CommCell.
installedAdditionalPatch[latest]	After service pack installation, the current, additional update installed post service pack for each component in the CommCell.
missingPatch	After service pack installation, the service pack updates for each component that are missing (uninstalled, or not selected during the service pack installation).

[Back to Top](#)

CommCell Views - How To

- [Topics](#)
- [How To](#)
- [How Do I](#)

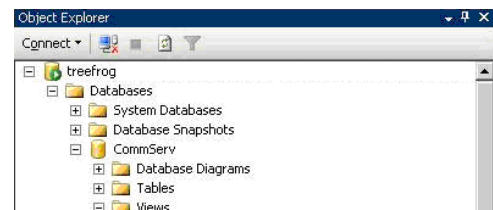
ACCESS THE COMMCELL VIEWS

This section describes the steps involved in accessing the CommCell Views using **SQL Server Management Studio**.

▶ To access the CommCell Views:

1. Select **Start | Programs | Microsoft SQL Server 2008 | SQL Server Management Studio**.

The following image displays a sample of the SQL Server Management Studio window.



2. By expanding the tree in the left pane, go to the following location: <CommServe computer name\database_instance_name> | **Databases** | **CommServ** | **Views**.

The available CommCell Views are listed in the right pane.

NOTES

- For a cluster, instead of the database instance, there will be a default or Named instance.

- dbo.CommCellAdminSchedule
- dbo.CommCellAuxCopyInfo
- dbo.CommCellBackupInfo
- dbo.CommCellBkSchedule
- dbo.CommCellBkupSizeInfo
- dbo.CommCellClientConfig
- dbo.CommCellClientFSFilters
- dbo.CommCellDriveInfo
- dbo.CommCellJobController
- dbo.CommCellJobControllerCount
- dbo.CommCellLibraryInfo
- dbo.CommCellLibraryReservInfo
- dbo.CommCellLicense
- dbo.CommCellMediaAgentInfo
- dbo.CommCellMediaInDrives
- dbo.CommCellMediaInfo
- dbo.CommCellPrePostCmdInfo
- dbo.CommCellRestoreInfo
- dbo.CommCellRetentionInfo
- dbo.CommCellStoragePolicy
- dbo.CommCellSubClientConfig
- dbo.CommCellUpdateInfo

3. To open a view, right-click the **View** and then select **Select Top 1000 Rows**.

The screenshot shows a list of database views in SQL Server Enterprise Manager. The view 'dbo.CommCellAdminSchedule' is selected, and a context menu is displayed over it. The menu options are:

- New View...
- Design
- Select Top 1000 Rows
- Edit Top 200 Rows
- Script View as
- View Dependencies
- Full-Text index
- Policies
- Facets
- Start PowerShell
- Reports
- Rename
- Delete
- Refresh
- Properties

Command Line Interface

[Topics](#) | [QCommands](#) | [Save As Script](#) | [XML Scripts](#) | [QScripts](#) | [QAPI Developers Guide](#) | [How To](#) | [Troubleshoot](#) | [Support](#) | [Related Topics](#)

Overview

Important Considerations

OVERVIEW

Command Line Interface enables you to perform several basic operations from the command line using Qcommands. The Qcommands are a set of commands that can be executed from the command line or can be integrated into your own scripts or scheduling programs. For more information, see [Command Line Interface - QCommands](#).

In addition, you can also generate scripts for specific operations from the CommCell Console using the Save As Script option. These scripts can later be executed from the command line interface using the `qoperation execute` qcommand. For more information, see [Command Line Interface - Save As Script](#).

IMPORTANT CONSIDERATIONS

GENERAL CONSIDERATIONS

- No special configuration is required to use the command line interface. The commands are integrated with the Base package, and are therefore available on all computers which have any CommServe, MediaAgent, or Agent software installed. However, it is recommended that you execute the command line operations from the CommServe.
- In order for the commands to function, the `Bull Calypso Commands Manager` service should be up and running on the CommServe. The `Bull Calypso Commands Manager` is a service that is installed with the CommServe, and is responsible for handling command line requests and forwarding them to the `Event Management Service` of the target CommServe. See [Services](#) for more information.

CAPABILITIES AND PERMITTED ACTIONS

In order to perform any of the following command line operations, the user requires Administrative Management capabilities.

- Login and logout from a command line session using `qlogin` and `qlogout` qcommands.
- Execute any of the qcommands from the command line.
- Execute the scripts generated using Save As Script option in CommCell Console.

[Back to Top](#)

Command Line Interface - How To

[Topics](#) | [QCommands](#) | [Save As Script](#) | [XML Scripts](#) | [QScripts](#) | [QAPI Developers Guide](#) | [How To](#) | [Troubleshoot](#) | [Support](#) | [Related Topics](#)

[Save a Job as a Script](#)

[Execute Scripts using qoperation execute Command](#)

[Set up the qoperation find Command](#)

SAVE A JOB AS A SCRIPT

▶ To save a job as a script:

1. From the CommCell Console, begin one of the following procedures:
 - Start a Backup
 - Browse and Restore
 - Start a Disaster Recovery Backup
 - Start a Migration Archive

- Start a Compliance Archive
 - Start an Auxiliary Copy
 - Create a QR Volume of a Subclient
 - Start Data Aging
2. For example let us consider a backup procedure. From the **Backup Options for Subclient** dialog box, select the required options that you want to execute when the script is run and click **Save As Script**.
 3. In the Save As Script dialog box select the location of the client on which you want to save the script.
 4. Enter or **Browse** to a path and name for the script file to be saved on the CommServe computer.
 5. Select **Synchronous** or **Asynchronous** execution. Some job types will always be performed asynchronously and the synchronous option will be disabled.
 - A synchronous operation exits only when the operation has completed.
 - An asynchronous operation submits the job to the CommServe and exits immediately, returning control to the calling program or script.
 6. If a script with same name exists, you can decide if the existing script must be overwritten. In addition, you can decide the extension of the save as script file.
 7. Click **OK** to save the operation as a script file.
-

EXECUTE SCRIPTS USING `qoperation execute` COMMAND

▶ To save a job as script using `qoperation execute` command:

1. From the CommCell Console, run Save a Job as Script procedure.
2. From the command prompt, navigate to the `<software installation path>\Base` folder and run the following command:

```
qoperation execute -af "D:\fsscript\fabkp.bat_1256279326.xml"
```

where:

- `qoperation execute` - Command to execute a script from command line.
- `-af` - displays the path of the `.xml` file to be executed.

The job is initiated and executed successfully.

SET UP THE `qoperation find` COMMAND

▶ To set up the `qoperation find` command:

1. From the CommCell Console, run **Save a Job as Script** from a earlier release of the software.
 2. Modify the contents of the input file of previous version, to do the following:
 - Include the form of `qoperation find` command.
 - Replace all the values for the `[options]` option with the following values: `QR_BROWSE`, `QR_NORECURSE`, `QR_NOIMAGE`, and `QR_WILDCARD`.
 - For the `[sourcepaths]` option, include the appropriate path with wildcards for backup content search purposes (e.g., `C:**\abc*.bat`)
-

[Back To Top](#)

When WAN Links Cannot Support the Full Backup Data Transfer

TABLE OF CONTENTS

Overview

Requirements

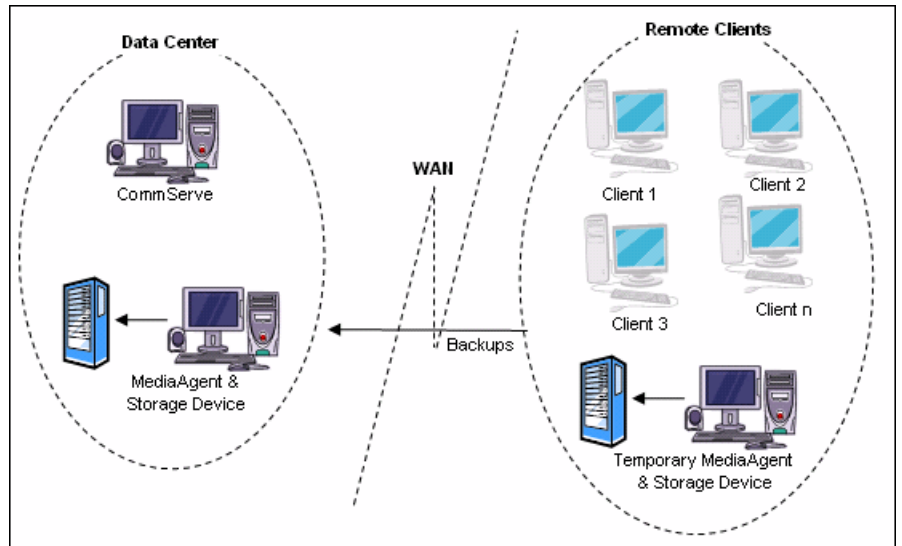
Procedure

OVERVIEW

Use the following procedure when WAN links do not have the bandwidth to transfer full backups and therefore only incremental backups can be performed on a regular basis.

Consider the following scenario:

- CommServe, MediaAgent and storage devices are located in a Data Center.
- Clients are located in remote sites across a WAN.
- The WAN can support transfer of incremental data but not full backups.



REQUIREMENTS

A `GridStore` license is required to implement this solution. (See License Administration for comprehensive information on licensing.)

PROCEDURE

Use the following procedure when WAN links do not have the bandwidth to transfer full backups and therefore only incremental backups can be performed on a regular basis.

1. Install a temporary MediaAgent at the remote site.
The MediaAgent can be installed in the Client computer or on a different computer in the remote site.
2. Attach a temporary storage device (tape or disk device) to this MediaAgent and configure the device.
This storage device must be compatible with the storage device in the Data Center.

See MediaAgent Deployment for appropriate procedures for installing the MediaAgent.

The following sections provide a discussion on the various types of libraries and how to configure them:

- Blind Libraries
- Centera Clusters
- Cloud Storage
- Direct-Attached Libraries
- Direct-Attached Shared Libraries
- Disk Libraries
- HDS Data Retention Utility (DRU)
- IP Libraries (Like libraries attached to ACSLS Server)
- NAS Libraries
- Optical Libraries
- PnP (Plug and Play) Disk Libraries
- Removable Disk Drives

- SAN-Attached Libraries
 - Stand-Alone Drives
 - Virtual Tape Libraries
3. Add a data path (using the temporary MediaAgent and Storage Device) to the Storage Policy Copy (which uses the MediaAgent and Storage Device in the Data Center as the default data path) that will eventually be used to backup the clients from the remote site on a regular basis.

If you have configured the temporary MediaAgent on a different computer in the remote site, set this data path as a high priority data path in the subclient.

See the following procedures for step-by-step instructions:
 - Add a Data Path to a Storage Policy Copy
 - Configure Data Paths for Subclients
 4. Perform an initial full backup using the data path associated with the temporary MediaAgent and storage device.

See Full Backups - How To for step-by-step instructions.
 5. Ship the media containing the data associated with the full backup to the Data Center.

In the Data Center import the media into the MediaAgent/library which will be used to backup the clients from the remote site on a regular basis.

In the case of a disk device, the disk library can be migrated to the MediaAgent located in the Data Center.

See the following procedures for step-by-step instructions:
 - Import Media
 - Migrate a Disk Library
 6. Delete the remote data path from the storage policy copy.

If necessary, the remote MediaAgent and storage device can also be deconfigured.

See the following procedures for step-by-step instructions:
 - Delete a Data Path from a Storage Policy Copy
 - De-Configure a MediaAgent
 - Deconfigure Libraries
 7. Add a data path for the MediaAgent, Storage Device in the Data Center, to a Storage Policy if it is not already available.

See Add a Data Path to a Storage Policy Copy for step-by-step instructions.
 8. Schedule regular incremental backups to go across the WAN from the remote client to the Data Center.

See Incremental Backups - How To for step-by-step instructions.
 9. Schedule regular Synthetic Full backups to read the data from the full backup as well as the incremental backup located at the Data Center.

Optionally an inline copy can be used to separate the full and incremental backup to a different Media type. (However note that using an inline copy is not mandatory.)

See the following procedures for step-by-step instructions:
 - Synthetic Full Backups
 - Enable an Inline Copy

Grandfather-Father-Son (GFS) Tape Rotation

Topics | Related Topics

Overview

OVERVIEW

This is a very common scheme used as a hierarchical data retention strategy.

For example, three sets of backups, such as weekly, monthly and yearly are defined. You can vary this frequency to suit the requirements of your environment. The weekly or Son backups are rotated on a weekly basis with one graduating to Father status each month. The monthly or Father backups are rotated on a yearly basis with one graduating to Grandfather status each year. One or more of the graduated backups is removed from the site for disaster recovery and archival purposes.

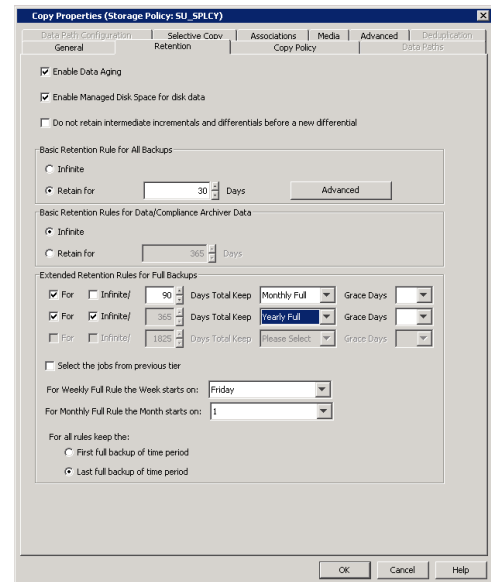
There are two ways in which this can be accomplished:

Method 1 - Using Selective Copies (See Selective Copy for detailed information)

- Perform incremental backups daily and full backup weekly to the primary copy (Retention can be set to 30 days)
- Create a selective copy for the monthly full backups (Retention can be set to 365 days)
- Create another selective copy for the yearly full backups (Retention can be set to infinite)

Method 2 - Using Extended Retention Rules on the Primary Copy (See Extended Retention Rules for detailed information.)

- Set the basic retention rules on the primary copy to 30 days
- In addition set extended retention rules for monthly full backups to 365 days and yearly full backups as infinite as shown in the sample image.



Method 1 creates separate copies of data which may be useful for off-site storage requirements.

Method 2 carves out a graded retention from a single copy.

In reality, a combination of both these methods may be required. For example, only one selective copy may be created and extended retention established in this selective copy.

In addition, you can manually retain specific jobs for a longer period (in addition to the retention period specified in the copy) if there is a necessity to retain specific jobs. See Retain a Job for more information.

Back to Top