

# CommNet Features - Table of Contents

---

## TABLE OF CONTENTS

### OVERVIEW

CommNet Server

CommNet Browser

CommNet Explorer

### SYSTEM REQUIREMENTS

CommNet Server

CommNet Browser

CommNet Explorer

### INSTALLATION

CommNet Server

- Install the CommNet Server
- Install the CommNet Server SNMP Enabler
- Install Software from the CommCell Console

CommNet Browser

- Install the CommNet Browser
- Install the CommNet Browser - Macintosh
- Install Software from the CommCell Console

### ADMINISTRATION

User Administration and Security

Web Administration

License Administration

Clustering

Alerts and Monitoring

Cost Analysis

Dashboard

Scheduling

Reports

Summaries

CommCells

Storage Resources

Libraries

MediaAgents

Cell-Client Groups

CommNet Clients

Client Computer Groups

Disaster Recovery

### OTHER

Data Collection

Firewall

Global Filters

Data Interface Pairs

SLA

Log Files

---

# Overview - CommNet

---

Overview

Software Components

- CommNet™ Server
- CommNet™ Browser
- CommNet™ Explorer

Summaries

Reports

Other Features

Concepts

---

## OVERVIEW

The CommNet™ management tool has been designed to manage and administer the CommCell Groups efficiently and in a timely manner in order to minimize administration costs. Additionally, you can analyze concise summaries and comprehensive reports showing various aspects of secondary and primary storage in order to resolve problems proactively rather than reactively. The software also provides features such as remote administration capabilities, alert mechanisms, user administration, job and resource management, and scheduling. All of these features are discussed in detail in the following sections.

---

## SOFTWARE COMPONENTS

---

### COMMNET™ SERVER

The CommNet™ Server monitors the CommCell® group that are registered in the CommNet Server. It also gathers vital information from all the cells based on the frequency established in the Data Collection Policy. It also serves the CommNet Browser which is the user interface. Microsoft SQL Server is used to store all the data gathered from cells.

- **Time Zone:** All the reports and summaries in the system will automatically take into consideration the time zone of a specific cell and adjust the time accordingly. For example, reports generated concurrently for two cells in the Eastern time and Pacific time will automatically display the local time of these Cells.

The CommNet Server is the coordinator and administrator of the CommNet domain. It allows you to configure, schedule and administer various activities.

The CommNet Server gathers data from the CommCells that are registered in a CommNet domain and maintains a database containing information collected from the various Cells. This is performed using the CommNet Server Service which runs the CommNet Server.

The CommNet Server can either be installed on the computer which has the CommServe software installed or on a totally independent computer. If the CommNet Server is installed on the CommServe computer, the CommNet Server database is also created on the same Microsoft SQL Server instance used by the CommCell.

To protect the CommNet Server database against disasters, such as computer failure, application failure, etc. it is recommended that you have a Disaster Recovery strategy in place.

---

### COMMNET™ BROWSER

The CommNet Browser provides a user-friendly interface to administer and generate summaries and reports on the CommNet domain. The user interface is specifically designed to help a system administrator isolate problems and drill-down to the root cause of the problem without having to generate multiple reports. CommNet Browser can also be accessed using a web-browser.

See CommNet Browser for a comprehensive list of features provided in the CommNet Browser.

---

### COMMNET™ EXPLORER

CommNet Explorer provides a way to query information on the CommNet components directly from the SQL database. You can use the views provided with CommNet Explorer or customize them to reflect the data in any manner appropriate to your organization.

See CommNet Explorer for more information.

---

## SUMMARIES

The software provides summaries for all entities in the CommNet domain; from a comprehensive CommCell® summaries to more detailed Client, Media Agent and Library summaries. Summaries provide information at a glance about the primary and secondary storage wherever applicable, and include vital troubleshooting information crucial to any administrator.

The software gathers critical information from the CommCell® group at specified frequencies, allowing you to view:

- Up-to-date status of any entity within a Cell.
- Detailed data protection activity and storage distribution.
- Comprehensive, historical trending information.

For addition information, see Summaries.

---

## REPORTS

The software contains various reports that help you to manage your CommNet™ domain. Some of the important reports are described below:

### DATA PROTECTION COVERAGE

Data Protection reports can help you to understand the whether or not a particular client has data protection coverage on a given day, week, month, or year. The coverage report also displays the status of the coverage on a copy basis to determine if the coverage is from a primary or an auxiliary copy. In addition, you can also view valuable trending analysis such as job success rate, media consumption and primary and secondary storage growth.

The software provides flexibility in defining the Data Protection Windows for the CommCell® group for reporting purposes. You can use these customized reports to fine tune various parameters of a CommCell configuration in order to meet the data protection window. A Window Utilization report is also provided, which can be used to determine the Clients, iDataAgents, and Data Protection operations that are not meeting the specified window within a specified amount of time.

### WINDOW UTILIZATION

Data Protection Window Utilization Report can help you determine how well the data protection window is being utilized in the CommCell® groups. This report provides a summary of data protection operations relative to the data protection window specified in the CommCell group, including the number of jobs completing outside the window.

### DATA RECOVERY COVERAGE

Data Recovery reports can help you to understand the details of the recovery operations performed in the CommCell groups, including information on the restore destination and the job successes associated with the recovery operations.

### MEDIA MANAGEMENT PERFORMANCE

Media Management related information, such as MediaAgent, library and drive performance are provided in a concise manner in various Media Management reports. The software also generates performance reports for a given MediaAgent, library and drive, to help analyze media management aspects such as throughput, data size transferred, number of data protection operations handled, and library and drive usage times.

### PREDICTION CAPABILITIES

The software provides the capability to predict the following, by looking at past consumption and usage:

- Data growth for each CommCell® group as well as the sub clients in a given CommCell® configuration.
- Media Prediction to forecast media usage (for tape/optical libraries) and capacity usage (for magnetic libraries) in each individual CommCell group.

### SLA

SLA is a scale to measure how well the data protections operations are performed in a CommCell® group. This is determined based on the short-term and long-term coverage. In order to customize the calculation based on your specific environment, facility to define the weights for several aspects in the short-term and long-term coverage and an acceptable SLA is also provided.

### PRIMARY STORAGE AND MEDIA BASED COSTING

Media based costing mechanism provides the facility to determine the cost associated with hosting an application and its protected data, based on the type of media in which the data resides. This feature includes the facility to define cost categories and the media associated with each cost category, and billable entities, such as departments within a company.

A comprehensive Billable Charge Back report can be generated to view the cost, related expense, storage size, and ranking information for all vital primary

and secondary storage entities. The report can be generated for clients or billable entities.

The costing model can be defined centrally and automatically distributed to all CommCell<sup>®</sup> group within the CommNet<sup>™</sup> domain.

---

## **LOAD**

Load information refers to the job activity status for the CommCell<sup>®</sup> groups, which includes their peak load status, the range of time with the largest amount of job activity. Users can use this report to quickly determine better data protection job schedule solutions so that the network is not overloaded at specific times. This report is extremely useful for troubleshooting network issues.

For addition information, see Reports.

---

## **OTHER FEATURES**

There are a host of other features designed to help you manage and administer your CommCell<sup>®</sup> group. Some of the major features are described below:

---

### **INSTALLATION**

The CommNet software installation is a component of the CommServe software installation removing the need for the separate installation. When installing the CommServe software, you have the option to install the CommNet software components, which includes the CommNet Server, CommNet Browser, and CommNet Explorer. Additionally, during the installation of the CommServe software, the CommNet Agent is automatically installed. The CommNet Agent no longer requires an independent install on the CommServe computer. Note that the automatic installation of the CommNet Agent does not signify that the CommServe must be registered with a CommNet Server for reporting purposes.

During installation of the CommNet Server software, you must specify the CommCell with which the CommNet Server will be associated. When installed, the CommNet Server appears as a client computer in its associated CommServe's CommCell Console. This does not register the CommCell with the CommNet Server, 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 automatic updates as well as the following:

- Licensing: The CommNet software licenses are now administered from its associated CommCell License Administration utility. The following CommNet licenses are now License Types on the CommServe Computer:
  - CommNet Server
  - CommNet Agent
  - CommNet Explorer
  - CommNet Advanced Reporting
- CommNet Books Online: CommNet Books Online documentation is merged with the CommServe software documentation to make it easier for you to quickly find desired topics in one location.

If another CommNet Server is installed in this environment, it cannot be associated with the CommCell that is already associated with a CommNet Server. It must be associated with another CommCell for deployment and license purposes.

---

### **REMOTE ADMINISTRATION**

Ability to launch multiple CommCell<sup>®</sup> Consoles to remotely administer and monitor individual cells.

In addition, to provide additional monitoring capability, the Event Viewer and Job Controller associated with the CommCell group are displayed in the CommNet<sup>™</sup> Browser.

---

### **ALERTS**

Alert mechanism provides the capability to notify users of critical conditions using E-mail, Pager and SNMP traps. This feature also provides the mechanism to escalate the conditions if it has not been addressed for a specified amount of time or if the condition worsens.

---

### **USER ADMINISTRATION**

The software supports a very flexible user security scheme that can be customized to provide access to only the designated administrators for a given Cell.

---

### **SCHEDULING**

Scheduling provides the facility to run tasks such as reports and summaries on a consistent basis. Further, scheduling also provides the capability to send critical organizational information to multiple users at multiple times and intervals in easy to use formats to specified recipients.

---

### **JOBS AND RESOURCES**

Jobs and Resources is a CommCell<sup>®</sup> task in the CommNet<sup>™</sup> Browser. It allows users to troubleshoot their environment and control CommCell<sup>®</sup> jobs and manage its resources. For more information, see CommCell<sup>®</sup> Jobs and Resources.

## CONCEPTS

You must acquaint yourself with the following concepts before using the software:

- About Data Protection Windows
  - About Coverage Qualifier Windows
  - About Activity Qualifier Windows
  - About Daily Administration Activity Monitoring Windows
  - Diagram of Weekday Windows
  - Diagram of Weekend Windows
  - About the SLA
- 

## KEYWORDS

media usage.

---

[Back to Top](#)

# CommNet Server

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

---

Overview

Data Encryption

---

## OVERVIEW

The CommNet Server is the coordinator and administrator of the CommNet domain. The CommNet Server allows you to configure, schedule and administer the various activities in the CommNet domain.

The CommNet Server gathers data from the CommCells that are registered in a CommNet domain and maintains a database containing information collected from the various Cells. This is performed using the CommNet Server Service which runs the CommNet Server.

The CommNet Server must be installed on the computer which has the CommServe software installed. The CommNet Server database is also created on the same Microsoft SQL Server instance used by the CommCell.

To protect the CommNet Server database against disasters, such as computer failure, application failure, etc. it is recommended that you have a Disaster Recovery strategy in place.

---

## DATA ENCRYPTION

The CommNet environment software supports data encryption for transmission over non-secure networks. The data is always encrypted using the same algorithm, Blowfish with 128-bit keys. The entire process, which is always enabled, is completely transparent to users. Data is encrypted on the CommNet Agent and decrypted on the CommNet Server.

A license is not required for this feature.

---

# CommNet Browser

Topics | How To | Troubleshoot | Related Topics

---

## Overview

- Automatic Updates

## CommNet Browser Components

- Saving, Printing, and Emailing CommNet Browser Components

## Running the CommNet Browser as a Stand-Alone Application

## Running the CommNet Browser as a Remote Web-Based Application

## CommNet Browser Options

## CommNet Browser CommCell Status Icons

## User Preferences

## Comments

## VaultTracker Action Monitor

## Additional CommNet Browser Features

- Flags
  - Obtaining Information About Job Errors
- 

## OVERVIEW

The CommNet Browser is the graphical user interface that allows you to administer and generate summaries and reports on the CommNet domain. The CommNet Browser provides the capability to quickly identify, isolate, and drill-down to the root cause of problems without having to generate multiple reports.

The CommNet Browser can be run in two ways:

- As a stand-alone application, which can be installed directly onto any computer running a supported platform that can communicate with the CommNet Server.

For comprehensive information on supported platforms, see [System Requirements - CommNet Browser as a Stand-Alone Application](#).

- As a remote web-based application, which allows you to access the CommNet Browser via any computer running a supported platform with a Java-enabled web browser.

For comprehensive information on supported platforms, see [System Requirements - CommNet Browser as a Remote Web-Based Application](#).

---

## AUTOMATIC UPDATES

When you login to the CommNet Browser, the CommNet Server verifies whether the CommNet Browser is up-to-date. If there has been an update to the Browser interface since the last login session, you will be notified by a prompt indicating that an update is available and ready for install. If you opt to install the update immediately, you will be required to restart the CommNet Browser. Additionally, CommNet Browser updates can be retrieved manually by selecting the **Check for Updates** option in the browser's **Setup** menu. This is useful if you do not log out of your CommNet Browser for a long period of time. If updates are available, you will be notified by a prompt indicating that an update is available and ready for install; updates are applied automatically upon exiting the CommNet Browser, and visible upon the next login.

---

## COMMNET BROWSER COMPONENTS

The CommNet Browser contains several components:

---

### COMMNET TREE

The CommNet Tree, located in the left pane of the CommNet Browser, presents the CommNet domain's components, as well as the administrative and operational tasks associated with them, in a hierarchical tree structure.

If a particular component is not reachable or not operational, this is indicated by the addition of a red circle with an "x" in the component's icon. If an object has been uninstalled, the icon is dimmed.

---

### COMMNET DASHBOARD

---



The CommNet Dashboard window, which is accessible by clicking the **CommCell** node in the CommNet Tree, can be customized to display select reports by default. These settings can be made using the **Customize Dashboard** tab in the **Browser Options** dialog box. (See *Customize the CommNet Dashboard* for step-by-step instructions.)

---

## MAIN WINDOW

The main window, located in the right pane of the CommNet Browser, presents information about the component selected in the CommNet Tree.

When the main window is maximized in the CommNet Browser, any additional windows opened are displayed on top of the existing window. Conversely, if the window is not maximized, then any additional windows are cascaded or tiled. The **Previous/Next** buttons can be used to navigate between all open windows.

When you click a different node in the CommNet Tree, any open window from the previous node are closed unless you click the **Keep Visible** button for that window.

---

## MENU BAR

Displays menu choices appropriate to the currently selected node in the CommNet Tree. Not every task can be accessed from the Menu Bar; some are accessible only by right-clicking a particular item in the CommNet Tree.

---

## STANDARD TOOL BAR

Provides an alternate means of accessing certain functionalities available from the Menu Bar. This bar can be toggled on/off from **View | Toolbars** in the Menu Bar.

---

## STATUS BAR

Located at the bottom of the CommNet Browser, this displays the current status of the connection to the CommNet Server (connected or disconnected, the login, and the language in use. This can be toggled on/off from **View** in the Menu Bar. Current connection status is indicated as:

- Green when a connection is established
- Yellow when the CommNet Browser is trying to re-establish a lost connection
- Red when a connection is lost.

The CommNet Browser tries to re-establish lost connections with the CommNet Server using the same user name and password provided during login.

---












## TASKS

Tasks associated with a selected node are available in three ways; as a right-click option on the node itself, which often contains the most items; in the **Tasks** window displayed at the lower right hand corner of the Browser; from **Tasks** in the Menu Bar. This window can be expanded or collapsed.

---

## USER BUTTONS

Several common user buttons in the CommNet Browser are outlined in the following table:

 <b>Browser Toggle</b>	Switches the display of the CommNet Tree and Users Task pane on or off. Part of the Standard Tool Bar, which can be toggled on or off from <b>View</b> in the Menu Bar.
 <b>Previous/Next</b>	Pages the display through multiple open windows, such as reports.
 <b>Update</b>	Updates the currently displayed summary. This only appears when updates have been received from a CommCell.
 <b>Keep Visible</b>	Prevents a window from being closed when you select a different node.
 <b>Save</b>	If available, saves the currently active Browser window, report content, or summary as a PDF file.
 <b>Print</b>	If available, prints the currently active Browser window, report, or summary.
 <b>Export</b>	Exports the currently active Browser window, report, or summary in Microsoft Excel format.
 <b>Email</b>	If available, packages the currently active Browser window in .pdf or .xls format and attaches the report to a new email message.
 <b>Schedule</b>	Opens New Schedule wizard to create a schedule based on the current report or summary. See <i>Create a Schedule</i> .
 <b>Pause</b>	Pauses updates to the current window.
 <b>Play</b>	Resumes updates to the current window.

## SAVING, PRINTING, AND EMAILING COMMNET BROWSER COMPONENTS

Most CommNet Browser components can be saved to a local or network disk, printed to a file or printer, and emailed to one or more email recipients. These capabilities are useful if you wish to share reports, alerts, summaries, details, and other informational entities about the CommNet.

If a particular browser component does not support a save, print, or email operation, the corresponding icon for that operation will be disabled.

### **Saving Browser Components**

CommNet Browser components can be saved to a local disk or network share in .pdf format. Below are some of the most commonly saved components:

- From the Alerts node in the CommNet Tree, click the **Save** icon to launch the additional save options. See Save Options - Alerts.
- From the Billing Entity node in the CommNet Tree, click the **Save** icon to launch the additional save options. See Save Options - Billing.
- From the Cost Category node in the CommNet Tree, click the **Save** icon to launch the additional save options. See Save Options - Cost Categories.
- From the Schedule node in the CommNet Tree, click the **Save** icon to launch the additional save options. See Save Options - Schedule.

See Save Options.

### **Printing Browser Components**

CommNet Browser components can be printed to a file or printer. Below are some of the most commonly printed components:

- From the Alerts node in the CommNet Tree, click the **Print** icon to launch the additional print options. See Print Options - Alerts.
- From the Billing Entity node in the CommNet Tree, click the **Print** icon to launch the additional print options. See Print Options - Billing.
- From the Cost Category node in the CommNet Tree, click the **Print** icon to launch the additional print options. See Print Options - Cost Categories.
- From the Schedule node in the CommNet Tree, click the **Print** icon to launch the additional print options. See Print Options - Schedule.

See Print Options.

Save and Print options are not available on CommNet Browsers running on Macintosh computers.

### **Emailing Browser Components**

CommNet Browser components can also be emailed to one or more recipients.

When clicked, the email icon will launch the **Email Report** dialog box, which provides the facility to create a new email message and select a file format in which the Browser component will be attached (.pdf or .xls).

Note that you must configure the sender address and mail server settings prior to using the email function. This can be done using the **Configuration** tab in the CommNet Server's **Properties** dialog box.

See the following for step-by-step instructions:

- Define the Mail Server
- Defining the Sender's Address
- Define the Port for the SMTP Server
- Email a CommNet Browser Component

---

## **RUNNING THE COMMNET BROWSER AS A STAND-ALONE APPLICATION**

The stand-alone version of the CommNet Browser can be run either locally from the CommNet Server computer, or remotely on a client. The CommNet Browser is automatically installed during the CommNet Server installation.

Note that the following features are not available when using the CommNet Browser on a Macintosh:

- Remote Administration of CommCells
- The remote web-based version using a browser
- Save
- Print
- Copy Chart
- Export is available only on version 10.3 and later of Mac OS X.

For step-by-step instructions on running the CommNet Browser as a stand-alone application, see:

- Run the CommNet Browser as a Stand-Alone Application - Windows
- Run the CommNet Browser as a Stand-Alone Application - Macintosh

---

## **RUNNING THE COMMNET BROWSER AS A REMOTE WEB-BASED APPLICATION**

Once the CommNet Browser software is installed on the CommNet Server computer, you can access the CommNet Browser remotely from any computer using Java Web Start. Thus, the CommNet Browser stand-alone application does not need to be installed on a remote computer that has a Java enabled Web

browser. The web-based version of the CommNet Browser has the same appearance and functionality as the installable CommNet Browser stand-alone application.

When accessing the CommNet Browser remotely for the first time, Java Web Start provides you with the option of creating Desktop and Start menu icons for the CommNet Browser. If you choose to create these icons, you will be able to remotely access the CommNet Browser directly from the Desktop or Start menu without having to enter the CommNet Server name and alias in the Web browser each time. You also retain the option of continuing to remotely access the CommNet Browser via a Web browser if desired.

If you choose not to create these shortcuts, you must launch a Web browser and enter the CommNet Server name and alias each time you wish to remotely access the CommNet Browser.

Note that the IIS Server must be configured for accessing the CommNet Browser using Java Web Start. See Set Up IIS Server for Web Administration for more information.

For step-by-step instructions on running the CommNet Browser from a remote computer, see:

- Run the CommNet Browser as a Remote Web-Based Application - Windows
- Run the CommNet Browser as a Remote Web-Based Application - Linux
- Setting Up the IIS Server for Web Administration

## COMMNET BROWSER OPTIONS

The **Browser Options** dialog box allows users to:

- Enable/disable timeout session, and specify the period of inactivity before timeout. Enabling this option will help reduce the load on the server or machine where the browser is installed. The default idle time is set at 2 hours.
- Enable/disable browser update popup messages. By default, update popup messages are displayed upon any change to a **CommCell**, or **Cell-Client Group**. Users have the option to disable these popup messages.
- Enable/disable the display of chart point labels in a diagonal format. Enabling this option increases the number of entities viewable in a single page (when printed).
- Select the browser's date format. By default, the date format will follow that of the operating system where the browser is installed. Users can select another date format for the browser and reports.
- Select the CommCell and CommNet default tasks. By default, CommCell and CommNet Dashboards are displayed in the browser when the nodes are selected. Users can also select the summary option to display the corresponding summaries when the CommCell and CommNet nodes are selected.
- Customize the Dashboard views. For more information, see Customize the CommNet Dashboard.


To set or modify the Browser Options, select **Setup | Browser Preferences** from the CommNet Browser's file menu.

See Browser Options for more information.

## COMMNET BROWSER COMMCELL STATUS ICONS

The CommNet Tree icons representing a CommCell signify the current status of the CommCell. For more information, see following table.

Icon	Description	Where Applicable
	CommCell has been recently synchronized, and is currently available.	<ul style="list-style-type: none"> <li>• CommCell nodes on the CommNet Browser CommNet Tree</li> <li>• CommCell Summary for CommCell nodes and Cell-Client Group nodes in the CommNet Browser CommNet Tree</li> </ul>
	CommCell has been recently synchronized, and is not currently available.	<ul style="list-style-type: none"> <li>• CommCell nodes on the CommNet Browser CommNet Tree</li> <li>• CommCell Summary for CommCell nodes and Cell-Client Group nodes in the CommNet Browser CommNet Tree</li> </ul>
	CommCell has not been synchronized since registration, and is currently available.	<ul style="list-style-type: none"> <li>• CommCell nodes on the CommNet Browser CommNet Tree</li> <li>• CommCell Summary for CommCell nodes and Cell-Client Group nodes in the CommNet Browser CommNet Tree</li> </ul>
	CommCell has not been synchronized since registration, and is not currently available.	<ul style="list-style-type: none"> <li>• CommCell nodes on the CommNet Browser CommNet Tree</li> <li>• CommCell Summary for CommCell nodes and Cell-Client Group nodes in the CommNet Browser CommNet Tree</li> </ul>
	CommCell has not been synchronized for more than a week, and is currently available. (Only applicable to CommCells with the current version of the CommServe software.)	<ul style="list-style-type: none"> <li>• CommCell nodes on the CommNet Browser CommNet Tree</li> <li>• CommCell Summary for CommCell nodes and Cell-Client Group nodes in the CommNet Browser CommNet Tree</li> </ul>
	CommCell has not been synchronized for more than a week, and is not currently available.	<ul style="list-style-type: none"> <li>• CommCell nodes on the CommNet Browser CommNet</li> </ul>

	(Only applicable to CommCells with the current version of the CommServe software.)	Tree <ul style="list-style-type: none"> <li>CommCell Summary for CommCell nodes and Cell-Client Group nodes in the CommNet Browser CommNet Tree</li> </ul>
	One or more CommCell(s) is not reachable or has never been synchronized.	CommNet node in the CommNet Browser CommNet Tree

## USER PREFERENCES

Each user can establish several CommNet Browser preferences which are applied at each login. These preferences, which are explained below, are established when disconnecting from the CommNet Browser using **File | Disconnect** and selecting to save User Preferences in the displayed prompt.

### LOGIN PREFERENCES

The following options can be set in the **Login** dialog box, accessed from **File | Login**:

- **LAN:** Select when the network connectivity between the CommNet Browser and CommNet Server is reliable.
- **WAN:** Select when the network connectivity between the CommNet Browser and CommNet Server may have intermittent failures and hence less reliable.
- **Locale:** Language and region are selectable for the list.
- **Apply User Preferences:** When you log out, a prompt asks if you want to save your user preferences. At each subsequent login, you can specify whether or not to use your saved preferences. Note that to save user options, you must generate the report before exiting the browser for the changes to take effect.

### SESSION PREFERENCES

The **User Preferences** dialog box displays the preferences established during the previous login session, including:

- a list of open windows.
- the state of the CommNet Tree from a previous session.
- the selected Window Style.
- the size of the CommNet Browser window.

### REPORT PREFERENCES

If you chose to save your user preferences at the end of your last login session, the CommNet Browser retains the report filter options that were selected during that session. This allows you to quickly generate routinely used reports during each login without the need to re-enter the filter criteria. You can choose whether or not to use these preferences when prompted during login.

### WINDOW STYLES

The CommNet Browser has been designed to integrate as smoothly as possible with your work environment. To change the style of the CommNet Browser, from the Menu Bar, select **View**, then **Style**, then select one of the following styles:

- **Metal:** resembling a Java application environment.
- **Windows:** resembling a Windows application environment.

### CELL SYNCHRONIZATION

The CommNet server retains the last synchronized cell information as part of user preferences, which is useful for those who regularly synchronize cells. For more information, see Synchronize Cells.

## COMMENTS

### OVERVIEW

The software provides several facilities to create or edit comments for many CommNet entities. These comments can include a description of the entity itself, special notes for users of the entity, or any other details about the entity that may be of use.

Comments will be automatically pushed to the selected entity once they are saved provided no changes were made to the comment by the entity's user since the last cell synchronization. If an entity's comment was changed after the last cell synchronization, the CommNet user will receive a pop-up message stating that the original comment had been modified. Once the next cell synchronization is complete, the CommNet user may then proceed to make the desired changes to the comment. (See Synchronize Cells for step-by-step instructions on manually synchronizing a cell.)

Note that when a comment is edited for a specific entity, the existing comment is automatically overwritten once the comment is saved. As such, it is recommended that any new comments added be appended to the existing comments. Doing so preserves the history of the comments created throughout the entity's use for future reference.

The following sections describe the areas in which comments can be created or edited.

### THE COMMENT EDITOR WINDOW

The Comment Editor window provides the facility to view and edit comments for a CommCell's CommServe, client computers, and storage resources.

Comments can be edited by any user with access to the entity selected.

See Add or Edit Comments using the Comment Editor Window for step-by-step instructions.

#### **ADDING COMMENTS TO A SPECIFIC ENTITY**

In addition to the Comment Editor, comments can also be added or edited by right-clicking on the chosen entity and selecting **Add Comment**. As with the Comment Editor, the **Add Comment** dialog box displays the original comment, if one exists, and provides space to type a new comment.

See Add or Edit Comments for a Specific Entity for step-by-step instructions.

#### **ADDING COMMENTS TO SUMMARIES**

Comments can be added or edited for select summaries. The following summaries provide the facility to add or edit comments:

- CommCell Summary
- Client Summary
- MediaAgent Summary
- Library Summary (Tape, Stand-Alone, and Disk)
- Data Protection Detail Report

Each summary provides a comment editor field in the **General** section. In addition to providing space to add or edit a comment, an option to **Include Comment in Save/Print/Export/Email** is provided.

See Add or Edit Comments in Summaries for step-by-step instructions.

## **VAULTTRACKER ACTION MONITOR**

The VaultTracker Actions Monitor provides the facility to view information about any VaultTracker actions existing throughout each CommCell.

Included in the VaultTracker Actions Monitor are:

- Information on the total number of VaultTracker actions occurring in each CommCell (including total actions and their status).
- Specific details about each individual action in a list format (including the action type, initiator, source, destination, etc.). This list can be sorted by column, which provides a way to view actions with similar characteristics together.

When an action is double-clicked, the action's details are displayed. This dialog box provides a more comprehensive look at the characteristics of the action, media barcode, state, current location and more.

When the VaultTracker Action Monitor is opened, all VaultTracker actions are immediately refreshed and will continue to refresh every two minutes for as long as the VaultTracker Action Monitor is open. When the VaultTracker Action Monitor is not open, VaultTracker actions are refreshed every 20 minutes by default. You can change this interval using the Cell Data Collection Policy dialog box. See Data Collection for more information on configuring data collection.

The VaultTracker Actions Monitor is accessible by selecting the **VaultTracker Action Monitor** node in the selected CommCell's **Task List**.

For a comprehensive look at all the VaultTracker operations occurring in one or more CommCells, the VaultTracker report can be generated. You can also view comprehensive information on media throughout multiple CommCells by generating the Media Information report. Both reports are accessible under the **Reports | Media Management** node in the CommNet Tree.


## **ADDITIONAL COMMNET BROWSER FEATURES**

The CommNet Browser provides several additional features useful in administering the CommNet domain:

### **TOOL TIPS**

Relevant additional information is provided as tool tips in all charts and tables.

### **FLAGS**

The Job and Resource Views also provide a **Flags** column, which is located on the left-hand side of the window. The **Flags** column displays a  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.

If neither of the above scenarios are present, the **Flags** column will remain empty.

---

## HYPERLINKS

Failures, such as CommCells that are not reachable or storage resources that are not operational, are displayed with a hyperlink to more detailed information about the particular failure.

### OBTAINING INFORMATION ABOUT JOB ERRORS

If a job in the CommCell has not completed successfully, the **Job Details** dialog box for that job will provide a hyperlinked **Error Code** which links 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.

Note the following when obtaining troubleshooting articles using error codes:

- Error Codes can be obtained by double-clicking the failed job in a report.
- The Error Code field will only contain a code if a job has not completed successfully.

See View Troubleshooting Article(s) Available from the Customer Support Website for step-by-step instructions.

---

## UPDATES

When an update is received from a CommCell, the CommNet Browser changes the following to inform you that an update has arrived:

- The text for the CommCell turns bold in the CommNet Tree.

When a node in the tree is selected, a pop-up message appears with an option to refresh the selected node and all corresponding windows. The pop-up messages are optional and can be disabled in the CommNet **Browser Options** dialog box.

- If a Summary is displayed in the right side pane, the Update icon and a corresponding yellow box is displayed at the top of the window informing you that an update is available.

Clicking this icon (or pressing the **F5** key) will update the most recent information on the specific summary, but will not update the entire node.

---

## REGISTER/UNREGISTER MESSAGES

As CommCells are registered/unregistered, a pop-up message will be displayed.

---

## VERSION

Select **About** from the **Help** menu to display the version number and update information of the software installed on the computer.

---

## COMMNET BROWSER AND FIREWALLS

See Firewall Requirements.

---

## COMMNET BROWSER AND COPY CHART

When viewing a report in the CommNet Browser, you can copy any chart to the clipboard in `.bmp` format by right-clicking the chart and selecting **Copy Chart**. This allows you to easily copy a chart into other applications. Note that the **Copy Charts** function is not compatible with Microsoft WordPad.

Back to Top

---

# CommNet Views

Topics | How To

## TABLE OF CONTENTS

### Overview

#### Views

CNEAppTypeView  
 CNEBKpJobsView  
 CNEChargeBackView  
 CNEClientInfoView  
 CNEJobsSummaryView  
 CNESCSchedPolicyAssoc  
 CNESubClientContentView  
 CNESubClientInfoView  
 CNESummaryView  
 CNETimeZoneDates

## OVERVIEW

The views in CommNet provide a way to query information on the CommCell components directly from the SQL database. These views are provided in addition to the CommNet Browser Report Selection feature.

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 CommNet.

### CNEAPPTYPEVIEW

The CNEAppTypeView provides an overview for the Agent Count and the amount of data backed up with each Agent for last 3 months.

The following image displays a sample CNEAppTypeView view:

WinFSCount	SolarisFSCount	OracleDBCCount	SQLDBCCount	ExchangeCount	WinFSSize	SolarisFSSize	OracleDBSize	SQLDBSize	ExchangeSize
499	2	1	7	0	0.00000...	0.0000000000...	0.0000000000...	0.00000000...	0.0000000000...

COLUMN	DESCRIPTION
WinFSCount	Total number of windows File System Agents installed.
SolarisFSCount	Total number of Solaris File System Agents installed.
OracleDBCCount	Total number of Oracle Database Agents installed.
SQLDBCCount	Total number of SQL Database Agents installed.
ExchangeCount	Total number of Exchange Agents installed.
WinFSSize	Total amount of Windows File System data backed up in last 3 months.
Solaris FSSize	Total amount of Solaris File System data backed up in last 3 months.
OracleDBSize	Total amount of Oracle Database data backed up in last 3 months.
SQLDBSize	Total amount of SQL Database data backed up in last 3 months.
ExchangeSize	Total amount of Exchange data backed up in last 3 months.

### CNEBKPJOBVIEW

The CNEBKpJobsView provides detailed information on each job.

The following image displays a sample CNEBKpJobsView view:

ChidID	CommCellName	Pruned	TimeStart	TimeEnd	UnCompBytes	Client...	ClientName	AppType...	AppType	Inst...	
1	1004019	md7zhhw	1	2009-11-20 02:05:30.000	2009-11-21 07:42:42.000	0	2	md7zhhw	33	Win FS	1
2	1004019	md7zhhw	1	2009-11-21 02:07:57.000	2009-11-21 07:42:43.000	0	2	md7zhhw	33	Win FS	1
3	1004019	md7zhhw	1	2009-11-29 02:05:15.000	2009-11-29 02:05:15.000	0	2	md7zhhw	33	Win FS	1
4	1004019	md7zhhw	1	2009-12-14 02:04:53.000	2009-12-14 14:48:45.000	0	2	md7zhhw	33	Win FS	1
5	1004019	md7zhhw	1	2009-12-17 02:04:25.000	2009-12-17 02:04:25.000	0	2	md7zhhw	33	Win FS	1
6	1004019	md7zhhw	1	2009-12-18 02:05:19.000	2009-12-18 02:05:19.000	0	2	md7zhhw	33	Win FS	1
7	1004019	md7zhhw	0	2010-01-09 02:03:10.000	2010-01-13 10:51:15.000	102364852318	2	md7zhhw	33	Win FS	1

COLUMN	DESCRIPTION
CommCellName	CommCell name.
Pruned	Yes or No.
TimeStart	Start Time of backup job.
TimeEnd	End Time of backup job.
UnCompBytes	Application Size.
ClientID	Client computer.
ClientName	The client computer name.
AppTypeID	The unique ID of the Application.
AppType	Application name.
InstanceID	The unique ID of the Instance.
InstanceName	The Instance name.
BKSetID	The unique ID of backupset.
BKSetName	Backupset name.
SubClientID	The unique ID of Subclient.
SubClientName	Subclient name.
BKLevel	Full, Increment ,Diff, etc.
StatusID	Completed, Failed, Killed.
StatusName	Completed, Failed, Killed.
OpTypeID	Backup, Restore, Recover, Auxiliary copy, etc.
OpTypeName	Backup, Restore, Recover, Auxiliary copy, etc.
CommCellID	The unique ID of the CommCell.
JobID	The unique Job ID of the backup job.
WriteTime	The amount of time to write data on media.
NumOFObjcts	The number of backup job objects.
Data_SPID	Data Storage Policy.
Data_SPNAME	Data Storage Policy name.
LOG_SPID	Log Storage Policy.
LOG_SPNAME	Log Storage Policy name.
DIFF_SPID	Differential Storage Policy.
DIFF_SPName	Differential Storage Policy name.
ScanFileFailure	The number of files failed to scan.
ScanFolderFailures	The number of folders failed to scan.
BackupFileFailures	The number of files failed to backup.
BackupFolderFailures	The number of folders failed to backup.

### CNECHARGEBACKVIEW

The CNEChargeBackView provides detailed information on each job for costing purposes.

The following image displays a sample CNEChargeBackView view:

CommCellName	Pruned	TimeStart	TimeEnd	UnCompBytes	ClientID	ClientName	AppTypeID
1 NA - admpu007m	0	2009-10-24 05:20:47.000	2009-10-24 07:06:21.000	29092405439	5	admpu012m	43
2 NA - admpu007m	0	2009-10-24 05:20:47.000	2009-10-24 07:06:21.000	2165723	5	admpu012m	43
3 NA - admpu007m	0	2009-12-12 01:26:45.000	2009-12-12 03:46:35.000	2165723	5	admpu012m	43
4 NA - admpu007m	0	2010-02-06 04:05:06.000	2010-02-06 04:21:05.000	2165723	5	admpu012m	43
5 NA - admpu007m	1	2010-02-05 21:08:48.000	2010-02-05 23:55:51.000	2165499	6	admpu009m	43
6 NA - admpu007m	1	2010-02-06 04:04:56.000	2010-02-06 04:38:31.000	100314965758	6	admpu009m	43

COLUMN	DESCRIPTION
CommCellName	CommCell name.
Pruned	Yes or No.
TimeStart	The time started for backup job.
TimeEnd	The time end for backup job.
UnComBytes	Backup Size.
ClientID	Client computer.
ClientName	The client computer name.
AppTypeID	The unique ID for Application.
AppType	Application name.
InstanceID	Instance.
InstanceName	The Instance name.
BKSetID	Backup set.
BKSetName	The backupset name..
SubClientID	The Subclient.
SubClientName	The Subclient name.



StatusID	Completed, Failed, Killed.
StatusName	Completed, Failed, Killed.
CommCellID	The unique ID for CommCell.
JobID	The unique Job ID of the backup job.
AuxCopyJobID	The Auxiliary copy job ID.
AttemptNumber	The job attempt number.
PhaseName	The job phase.
SPID	Storage Policy.
SPNAME	Storage Policy name.
SPCopyID	Storage Policy copy.
SPCopyName	Storage Policy copy name.
UnitCost	Unit Cost Per MB.

### CNECLIENTINFOVIEW

The CNEClientInfoView provides detailed information on client information.

The following image displays a sample CNEClientInfoView view:

	CommCellNumber	CommCellName	ClientID	ClientName	InterfaceName	OSName	Version	DeC
1	1004019	md7zhtw	2	md7zhtw	md7zhtw	Windows Server (R) 2008 Enterprise	9.0.0	0
2	1004019	md7zhtw	14	techshare	techshare	Windows Server 2003 x64	9.0.0	0
3	1004019	md7zhtw	16	SQL1	SQL1	Windows Server 2003	9.0.0	0
4	1004019	md7zhtw	17	SQL2	SQL2	Windows Server 2003	9.0.0	0
5	1004019	md7zhtw	21	celebrity	celebrity	Windows Server 2003	9.0.0	0
6	1004019	md7zhtw	22	kystal-web	kystal-web	Windows Server 2003	9.0.0	0
7	1004019	md7zhtw	56	harold1	harold1	Windows 2000	9.0.0	0

COLUMN	DESCRIPTION
CommCellName	CommCell name.
CommCellNumber	CommCell number
ClientID	Client computer.
ClientName	The client computer name.
Interfacename	Interface name.
OSName	The client operating system name.
Version	The version number.
DeConfigured	Weather the client is de-configured or not.
TotalbkJobs	Number of total jobs.
PrunedJobs	Number of pruned jobs.

### CNEJOBSSUMMARYVIEW

The CNEJobsSummaryView provides an overview for data protection and data recovery jobs.

The following image displays a sample CNEJobsSummaryView view:

	CommCellNumber	CommCellName	ClientID	ClientName	InterfaceName	OSName	Version	DeC
1	1004019	md7zhtw	2	md7zhtw	md7zhtw	Windows Server (R) 2008 Enterprise	9.0.0	0
2	1004019	md7zhtw	14	techshare	techshare	Windows Server 2003 x64	9.0.0	0
3	1004019	md7zhtw	16	SQL1	SQL1	Windows Server 2003	9.0.0	0
4	1004019	md7zhtw	17	SQL2	SQL2	Windows Server 2003	9.0.0	0
5	1004019	md7zhtw	21	celebrity	celebrity	Windows Server 2003	9.0.0	0
6	1004019	md7zhtw	22	kystal-web	kystal-web	Windows Server 2003	9.0.0	0
7	1004019	md7zhtw	56	harold1	harold1	Windows 2000	9.0.0	0

COLUMN	DESCRIPTION
DPJobCount	Number of Data Protection Jobs.
DPScsessHobCount	Number of Completed Data Protection Jobs.
DPFailedorKilledJobCount	Number of Failed or Killed Data Protection Jobs.
DPPrimaryDataSize	Total Data on the primary copy.
DRJobCount	Number of Data Recovery Jobs.
DRSuccessJobCount	Number of Completed Data Protection Jobs.
DRFailedorKilledJobCount	Number of Failed or Killed Data Protection Jobs.

### CNESSCHEDPOLICYASSOC

The CNESSchedPolicyAssoc view provides detailed information on Schedule Policies the Subclient is associated with.

The following image displays a sample CNESSchedPolicyAssoc view:

ChildID	CommCellName	ClientID	ClientName	AppTypeID	AppTypeName	InstanceID	InstanceName	BackupSetID	BackupsetName
1	1004019	md7zhtw	2	md7zhtw	33	Win FS	1	3	defaultBackupSet
2	1004019	md7zhtw	2	md7zhtw	33	Win FS	1	1978	SIL0_BackupSet_SP_B_Primary
3	1004019	md7zhtw	2	md7zhtw	33	Win FS	1	1978	SIL0_BackupSet_SP_B_Primary
4	1004019	md7zhtw	2	md7zhtw	33	Win FS	1	1979	SIL0_BackupSet_SP_C_Primary
5	1004019	md7zhtw	2	md7zhtw	33	Win FS	1	1979	SIL0_BackupSet_SP_C_Primary
6	1004019	md7zhtw	2	md7zhtw	33	Win FS	1	1980	SIL0_BackupSet_SP_D_Primary
7	1004019	md7zhtw	2	md7zhtw	33	Win FS	1	1980	SIL0_BackupSet_SP_D_Primary

COLUMN	DESCRIPTION
ChildID	The unique ID for CommCell.
CommCellName	CommCell name.
ClientID	Client computer.
ClientName	The client computer name.
AppTypeID	The unique ID for Application.
AppType	Application name.
InstanceID	Instance.
InstanceName	The Instance name.
BKSetID	Backupset.
BKSetName	The backupset name.
SubClientID	The Subclient.
SubClientName	The Subclient name.
SchedPolicyID	The Schedule Policy ID.
SchedPolicyName	The Schedule Policy name.
BackupType	Full, Increment, Diff, etc.
BackupTypeStr	Full, Increment, Diff, etc.
AssocLevel	Client Level, Agent Level, etc.
AssocLevelStr	Full, Increment, Diff, etc.
SchedulePattern	One Time, Daily, Weekly, Monthly or Yearly.
TimeZone	Schedule TimeZone.

### CNESUBCLIENTCONTENTVIEW

The CNESubClientContentView provides an information on data path entries to the contents of a subclient.

The following image displays a sample CNESubClientContentView view:

ChildID	SubClientID	Content	
1	1004019	2	C:\Test1
2	1004019	2407	\
3	1004019	2408	\
4	1004019	1346	\
5	1004019	1569	\
6	1004019	1570	X:\Depts
7	1004019	1590	X:\Depts\CISER

COLUMN	DESCRIPTION
ChildID	The unique ID for CommCell.
SubClientID	The unique ID of Subclient.
Content	Data path entry to the contents of a subclient.

### CNESUBCLIENTINFOVIEW

The CNESubClientInfoView provides detailed information on subclient information.

The following image displays a sample CNESubClientInfoView view:

ChildID	ChildName	ClientID	ClientName	AppTypeID	AppTypeName	InstanceID	InstanceName	BackupSetID	BackupSetName	SubClientID
1	1004019	md7zhtw	39	bigblack-box	11	Windows 2000 File System	1	82	defaultBackupSet	121
2	1004019	md7zhtw	39	bigblack-box	11	Windows 2000 File System	1	82	defaultBackupSet	123
3	1004019	md7zhtw	26	picruiser	11	Windows 2000 File System	1	53	defaultBackupSet	60
4	1004019	md7zhtw	26	picruiser	11	Windows 2000 File System	1	53	defaultBackupSet	82
5	1004019	md7zhtw	49	delorean	11	Windows 2000 File System	1	102	defaultBackupSet	151
6	1004019	md7zhtw	49	delorean	11	Windows 2000 File System	1	102	defaultBackupSet	153
7	1004019	md7zhtw	56	harold1	11	Windows 2000 File System	1	116	defaultBackupSet	172

COLUMN	DESCRIPTION
ChildID	The unique ID for CommCell.
ChildName	The unique name for CommCell.
ClientID	Client computer.
ClientName	The client computer name.
AppTypeID	The unique ID for Application.
AppTypeName	Application name.
InstanceID	The unique ID of the Instance.
InstanceName	The Instance name.
BackupSetID	The unique ID of backupset.

BackupSetName	Backupset name.
SubClientID	The unique ID of Subclient.
SubClientName	Subclient name.
Created	Subclient created.
Modified	Modified data protection activity.
NextFullBackup	Time of the next Full Backup
NextIncrBackup	Time of the next Increment Backup
NextDiffBackup	Time of the next Differential Backup
SPName	Storage Policy name.
Scheduled	Provides subclient data protection schedules.
Deleted	Provides subclient data protection deleted time.
Encryption	Provides data encryption for a selected content.
DataProtActivity	Data Protection Activity of a Subclient.

## CNESUMMARYVIEW

The CNESummaryView provides an overview of the entities (Client, iDataAgent and Libraries) count present.

The following image displays a sample CNESummaryView view:

NumCommCells	NumClients	NumAgents	NumSubClients	NumMediaAgents	NumLibraries	NumDrives	NumLicenses
1	614	628	814	28	12	39	139

COLUMN	DESCRIPTION
NumCommCells	Total number of CommCells registered
NumClients	Total number of Clients
NumAgents	Total number of Agents
NumSubClients	Total number of SubClients
NumMediaAgents	Total number of MediaAgents
NumLibraries	Total number of Libraries
NumDrives	Total number of Drives
NumLicenses	Total number of Licenses

## CNETIMEZONEDATES

The CNETimeZoneDates view provides information on time zones. This is populated when the service starts for +10 and -10 years in the CommNet Database.

The following image displays a sample CNETimeZoneDates view:

ChildID	CommCellName	Year	TimeZoneName	TimeZoneStdName	DSTFlag	Bias	STDBias	STDDate	DSTBias	DSTDate	
1	1004019	md7zhtw	2000	(GMT+08:00) Taipei	Taipei Standard Time	0	28800	0	1970-01-01 00:00:00.0000	0	1970-01-
2	1004019	md7zhtw	2001	(GMT+08:00) Taipei	Taipei Standard Time	0	28800	0	1970-01-01 00:00:00.0000	0	1970-01-
3	1004019	md7zhtw	2002	(GMT+08:00) Taipei	Taipei Standard Time	0	28800	0	1970-01-01 00:00:00.0000	0	1970-01-
4	1004019	md7zhtw	2003	(GMT+08:00) Taipei	Taipei Standard Time	0	28800	0	1970-01-01 00:00:00.0000	0	1970-01-
5	1004019	md7zhtw	2004	(GMT+08:00) Taipei	Taipei Standard Time	0	28800	0	1970-01-01 00:00:00.0000	0	1970-01-
6	1004019	md7zhtw	2005	(GMT+08:00) Taipei	Taipei Standard Time	0	28800	0	1970-01-01 00:00:00.0000	0	1970-01-
7	1004019	md7zhtw	2006	(GMT+08:00) Taipei	Taipei Standard Time	0	28800	0	1970-01-01 00:00:00.0000	0	1970-01-

COLUMN	DESCRIPTION
ChildID	The unique ID for CommCell.
CommCellName	CommCell name.
Year	Year.
TimeZoneName	TimeZone name.
TimeZoneStdName	TimeZone standard name.
DSTFlag	Day Light Saving Flag is set or not.
Bias	Difference with GMT ( For Eastern Time Zone (GMT-05).
STDBias	Standard Bias.
STDDate	Standard date.
DSTBias	Day Light Saving Bias is set or not.
DSTDate	Day Light Saving Date is set or not.

Back to Top

# System Requirements - CommNet Server

The following requirements are for the CommNet Server:

## OPERATING SYSTEM

See CommServe - Operating System support

## 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

In addition to CommServe - Hard Disk requirements, the following are required for CommNet Server:

Solid-state-disk (SSD)

800 MB of local disk space for CommNet Server database and log file growth

300 MB of local disk space for the Microsoft SQL application and database (Microsoft SQL Server is embedded in the CommNet Server software installation)

1GB of local disk space for the CommNet Server database growth

926 MB of temp space required for install or upgrade (where the temp folder resides).

In time, you may need to provide additional space (several GB) to allow for growth in the CommNet Server metadata. The size of the metadata depends on the number of Cells (CommCells) in your enterprise. The CommNet Server software does not require that the free disk space be available on a single drive.

For optimum CommNet Server performance, see CommCell Scalability Guide - Scalability Guidelines for CommServe.

## MEMORY

16 GB RAM minimum

Virtual memory should be set to twice the amount of available physical memory

## PROCESSOR

See CommServe - Processor support

## DATABASE ENGINE

CommNet Server must be installed on Microsoft SQL Server 2008 (Enterprise Edition). CommNet installations are not supported on any other Microsoft SQL Server versions. See **Database Engine** under System Requirements - CommServe - Enterprise Version for more information.

## PERIPHERALS

DVD-ROM drive

Network Interface Card

## MISCELLANEOUS

These requirements are in addition to the requirements of the CommServe software.

---

### IIS

Microsoft Internet Information Services (IIS) Web Server version 4.0 and above.

IIS is required in the CommNet Server computer (or an alternate computer configured for web administration) to provide the following:

- Remote administration capability using the CommNet Browser as a Remote Web-Based Application
- View reports from a remote computer
- Launch the Books Online from the CommNet Browser

If the CommNet Browser software is installed on a computer running IIS version 7.0 or 7.5, the following software components must also be installed and configured along with all default components on the computer:

- ASP

- ASP.NET
- IIS 6 Management Capability

---

## JRE

In a clustered environment, Java™ Runtime Environment (JRE) 1.7.0\_17 must be installed on the passive node manually; it is automatically installed on the active node, if not already installed.

---

## NETWORK

The CommNet Server computer requires IPv4 to obtain permanent licenses.

If a CommNet Server has both IPv4 and IPv6 sockets enabled, the CommNet Browser 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 in the Browser's target:

```
-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 CommNet Browser as a stand-alone application only. If you are running the CommNet Browser as a remote web-based application, you will always obtain an IPv4 address.

For additional information on supported Internet Protocols, refer to the Network Requirements for the Common Technology Engine software.

## NOTES ON COMMNET SERVER INSTALLATION

The CommNet Server should not reside on a Microsoft Exchange Server or a computer with an Oracle database. Installation of the CommNet Server software on a Microsoft Exchange Server or a computer with an Oracle database may reduce system performance below acceptable levels.

See CommServe - Database Engine and Notes on CommServe Installation for more information.

## 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

# System Requirements - CommNet Browser as a Stand-Alone Application

[Stand Alone Application](#)
[Remote Web Based Application](#)

The following requirements are for the CommNet Browser as a Stand-Alone Application:

<b>OPERATING SYSTEM</b>		<b>PROCESSOR</b>
<b>LINUX</b>	<b>RED HAT ENTERPRISE LINUX AS/ES</b>	
	Red Hat Enterprise Linux AS/ES 4.0 with glibc 2.3.x	Intel Pentium or x64 processors
	<b>RED HAT ENTERPRISE LINUX/CENTOS</b>	
	Red Hat Enterprise Linux/CentOS 5 Advanced Platform with glibc 2.5.x	Intel Pentium or x64 processors
<b>MAC OS X SERVER</b>	Mac OS X v10.4.2	Apple Macintosh computer that supports any of the operating systems identified in this table
	Mac OS X v10.4.1	Apple Macintosh computer that supports any of the operating systems identified in this table
	Mac OS X v10.4.0	Apple Macintosh computer that supports any of the operating systems identified in this table
	Mac OS X v10.3.9	Apple Macintosh computer that supports any of the operating systems identified in this table
	Mac OS X v10.3.8	Apple Macintosh computer that supports any of the operating systems identified in this table
	Mac OS X v10.3.7	Apple Macintosh computer that supports any of the operating systems identified in this table
	Mac OS X v10.3.6	Apple Macintosh computer that supports any of the operating systems identified in this table
	Mac OS X v10.3.5	Apple Macintosh computer that supports any of the operating systems identified in this table
	Mac OS X v10.3.4	Apple Macintosh computer that supports any of the operating systems identified in this table
	Mac OS X v10.3.3	Apple Macintosh computer that supports any of the operating systems identified in this table
	Mac OS X 10.3.2	Apple Macintosh computer that supports any of the operating systems identified in this table
	Mac OS X 10.3.1	Apple Macintosh computer that supports any of the operating systems identified in this table
	Mac OS X 10.3.0	Apple Macintosh computer that supports any of the operating systems identified in this table
	Mac OS X 10.2.8	Apple Macintosh computer that supports any of the operating systems identified in this table
<b>WINDOWS</b>	<b>WINDOWS 8</b>	
	Microsoft Windows 8 Editions	All Windows-compatible processors supported
	<b>WINDOWS 7</b>	
	Microsoft Windows 7 32-bit and x64 Editions	All Windows-compatible processors supported
	<b>WINDOWS 2008</b>	
	Microsoft Windows Server 2008 32-bit and x64 Editions*	All Windows-compatible processors supported
	*Core Editions not supported	
	<b>WINDOWS VISTA</b>	
	Microsoft Windows Vista 32-bit and x64 Editions	All Windows-compatible processors supported

**WINDOWS 2003**

Microsoft Windows Server 2003 32-bit and x64 Editions* with a minimum of Service Pack 1	All Windows-compatible processors supported
---	---

**WINDOWS XP**

Microsoft Windows XP Professional 32-bit Editions with a minimum of Service Pack 3	All Windows-compatible processors supported
--	---

**MEMORY**

512 MB RAM minimum required; 1 GB RAM recommended  
Virtual memory should be set to twice the amount of available physical memory

**DISPLAY**

The graphical icons in the CommNet Browser cannot be displayed in VGA mode. This affects the appearance of the Browser's toolbar and the CommNet Browser tree. Also, some table of contents are not displayed correctly.

**MISCELLANEOUS****NETWORK**

TCP/IP Services configured on the computer.

**INTERNET EXPLORER**

Microsoft Internet Explorer (IE) version 8.0, 9.0

Internet Protocol versions 4 (IPv4) or 6 (IPv6)

**MICROSOFT VISUAL C++**

Microsoft Visual C++ 2008 Redistributable Package is automatically installed. Note that Visual C++ 2008 Redistributable Package can co-exist with other versions of this software.

**NOTES ON COMMNET INSTALLATION****JRE**

Java™ Runtime Environment (JRE) SE v1.7.x or higher is recommended.

For computers running an Intel Itanium-based operating system, J2SDK1.4 64-bit is required.

For computers running a non-Intel Itanium-based operating system, JRE 1.7.x versions are supported.

If a JRE version lower than 1.7.x is available, or no version is available at all, you will be prompted to install JRE version 1.7.x

If a JRE version 1.7.x or higher is available, the install program will use the existing software.

On Macintosh operating systems, JRE software version 1.6.x must be installed prior to installing the CommNet Browser software.

On Linux operating systems, JRE software version 1.6.x must be installed prior to installing the CommNet Browser software.

If a CommNet Server has both IPv4 and IPv6 sockets enabled, the CommNet Browser 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 in the Browser's target:

```
-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 CommNet Browser as a stand-alone application only. If you are running the CommNet Browser as a remote web-based application, you will always obtain an IPv4 address.

For additional information on supported Internet Protocols, refer to the Network Requirements for the Common Technology Engine software.

**IIS**

IIS is required in the CommNet Server computer (or an alternate computer configured for web administration) to provide the following:

- Remote administration capability using the CommNet Browser as a Remote Web-Based Application
- View reports from a remote computer
- Launch the Books Online from the CommNet Browser

See Web Administration for more information on configuring web administration.

If the CommNet Browser software is installed on a computer running IIS version 7.0 or 7.5, the following software components must also be installed and configured along with all default components on the computer:

- ASP
- ASP.NET
- IIS 6 Management Capability

**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



# System Requirements - CommNet Browser as a Remote Web-Based Application

[Stand Alone Application](#)[Remote Web Based Application](#)

The following requirements are for the CommNet Browser as a Remote Web-Based Application:

## SUPPORTED WEB BROWSERS

### LINUX

Mozilla 1.x

Netscape 6.2

### WINDOWS

Microsoft Internet Explorer (IE) versions 5.01, 6.0, 7.0, 8.0

## OPERATING SYSTEM

The CommNet Console as a Remote Web-Based Application is supported on any operating system running a supported Java-enabled web browser.

## MISCELLANEOUS

### IIS

If the CommNet Browser software is installed on a computer running IIS version 7.0 or 7.5, the following software components must also be installed and configured along with all default components on the computer:

- ASP
- ASP.NET
- IIS 6 Management Capability

### JRE

Java<sup>®</sup>,<sub>ç</sub> Runtime Environment (JRE) 1.7.0\_17 or higher recommended.

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

If the above version is not available, the Browser will automatically download the latest version from the appropriate Sun website.

In some environments, it might be necessary to configure the System Settings so that **netscape** is recognized as an executable command. This can be done by adding the installation path of Netscape to the System PATH variable as follows:

```
export $PATH=$PATH:<netscape_installation_path>
```

IIS is required in the CommNet Server computer (or an alternate computer configured for web administration) to provide the following:

- Remote administration capability using the CommNet Browser as a Remote Web-Based Application
- View reports from a remote computer
- Launch the Books Online from the CommNet Browser

See Web Administration for more information on configuring web administration.

Java plug-in is not supported on Microsoft Windows Server 2008 x64 editions. To run CommNet Browser as a Remote Web-Based Application, you need to install 32-bit JRE on 64-bit machines.

## 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

# Install the CommNet Server

## TABLE OF CONTENTS

### Install Requirements

#### Before You Begin

#### Install Procedure

- Getting Started
- Cluster Selection
- Select Components for Installation
- Set Up Microsoft SQL Server Instance
- Set User Names and Passwords
- Configure the CommCell® Console for Web-Based Administration
- Install Remaining Cluster Nodes
- Setup Complete

#### Post-Install Considerations

## INSTALL REQUIREMENTS

CommNet is now merged with the Calypso software. When installing the CommNet software, by default, the CommServe components are automatically installed. Furthermore, this registers the CommNet Server with the CommServe computer for data collection and reporting services.

The following procedure describes the steps involved in installing the CommServe and CommNet Server for both cluster and non-cluster environment. The CommNet Server software must be installed before installing the CommNet Browser and SNMP Enabler.

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

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

Review the following Install Requirements before installing the software:

---

### GENERAL

- Ensure that you have an available license for CommNet Server.
- You have the appropriate Software Installation Disc.
- If the CommNet components communicate across firewalls, ensure that the corresponding ports are allowed connections through the firewalls.
- 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 the installation.
- 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.

---

### CLUSTER SPECIFIC

- The CommNet Server 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. Note that in the clustered environment the CommNet Server software cannot be installed on the physical node of a cluster.
- 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 client as local Administrator or as a member of the Administrators 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

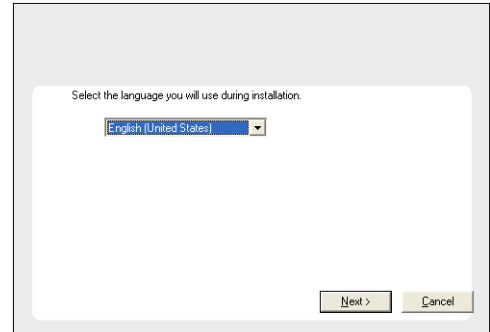
- Place the Software Installation Disc for the Windows platform into the disc drive.  
After a few seconds, the installation program is launched.

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**

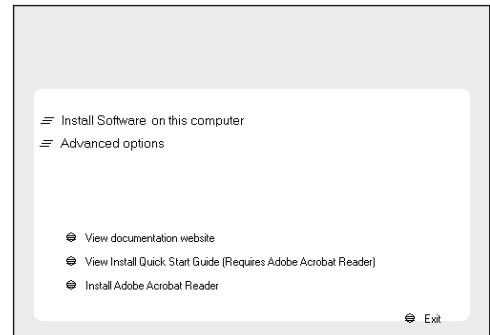
- If you are installing on Windows Server Core editions, mount to Software Installation Disc through command line, go to the **AMD64** folder and run **Setup.exe**.
- Choose the language you want to use during installation. Click the down arrow and select the desired language from the drop-down list,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

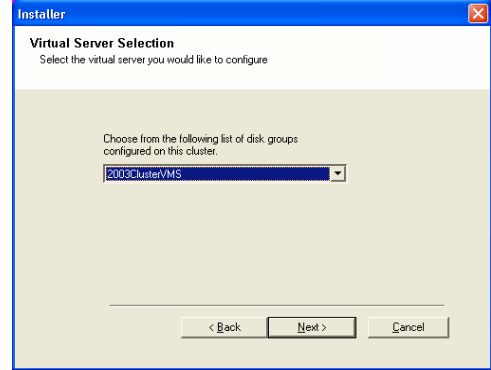
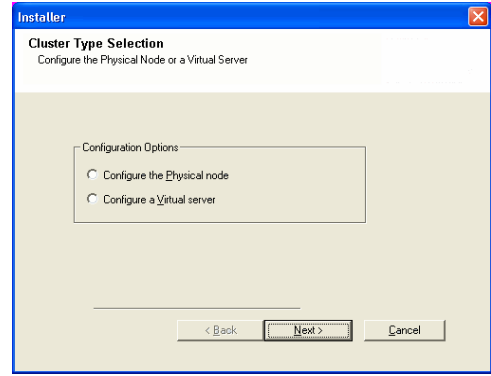


**CLUSTER SELECTION**

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.

6. 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 CommNet Server, expand the following `Common Technology Engine` folder, `CommServe Modules` and `CommNet` folder. Then select the following:

- `CommNet Server`

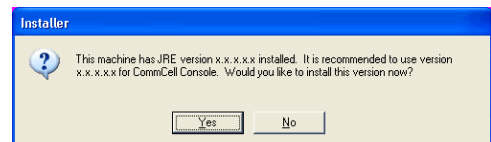
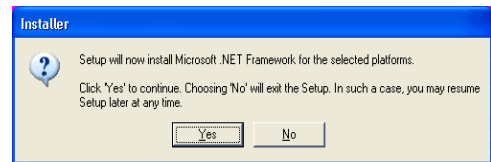
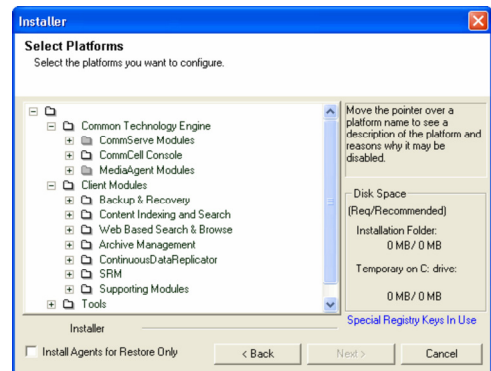
The `CommServe`, `CommCell Console` and `CommNet Browser` will be selected by default. `CommServe` are located in the `CommCell Module` folder. `CommNet Explorer` is located in the `CommNet` folder. `CommCell Console` and `CommNet Browser` are located in `CommCell Console` folder.

8. 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.

9. 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.



## SET UP MICROSOFT SQL SERVER INSTANCE

10. Specify the SQL Server System Administrator password.

### NOTES

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

Click **Next** to continue.

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

12. Enter the Installation Path for the Database Engine.

### NOTES

- This is the location where you want to setup the Microsoft SQL Server System databases.

Click **Browse** to change directories.

Click **Next** to continue.

The install program installs the database instance.

13. 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.

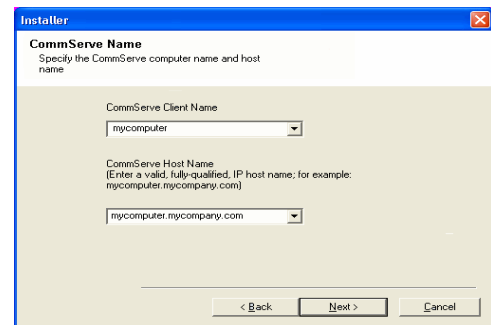
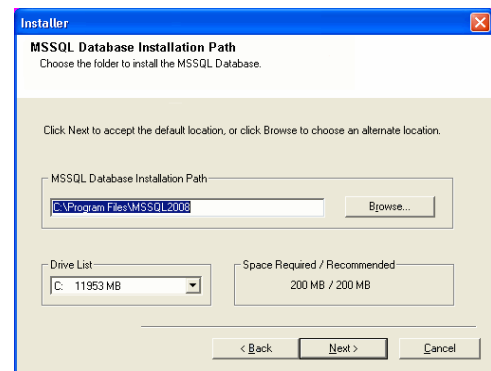
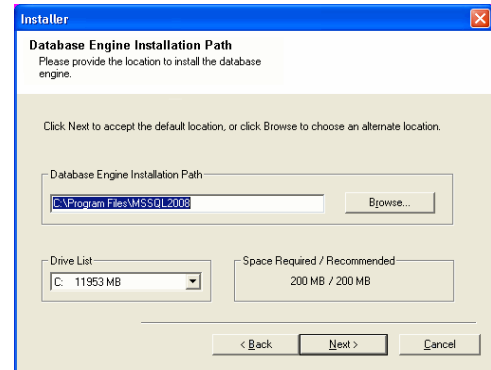
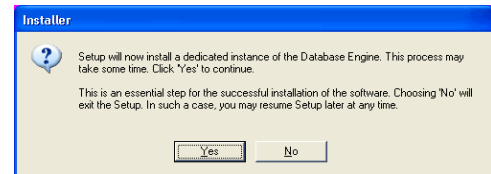
14. Enter the **CommServe Client Name** and the **CommServe Host Name**.

### NOTES

- The CommServe client name is the name of the computer. This field is automatically populated.
- The CommServe host name is the TCP/IP network interface name of the CommServe computer. This field is automatically populated.
- Do not use the following characters in the CommServe client name or the CommServe host name:  
`\ | ` ~ ! @ # $ % ^ & * ( ) + = < > / ? , [ ] { } ; : ; ""`

Click **Next** to continue.

15. Select **Add programs to the Windows Firewall Exclusion List**, if you wish to add



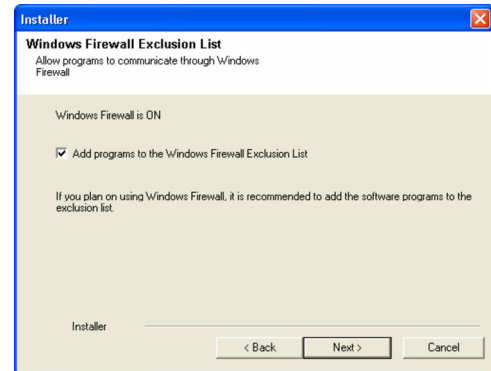
CommCell programs and services to the Windows Firewall Exclusion List.

**NOTES:**

- If Windows Firewall is enabled on the computer, this option is selected by default and must be enabled to proceed with the installation.
- If Windows Firewall is disabled on the computer, you can select this option to add the programs and services to enabled CommCell operations across the firewall, if the firewall is enabled at a later time.

You can either select this option during install or add the programs and services after installation. For adding the programs and services after installation, see [Configure Windows Firewall to Allow CommCell Communication](#).

Click **Next** to continue.



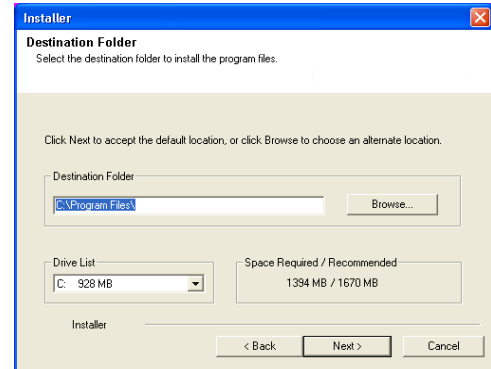
16. Specify the location where you want to install the software.

**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 has already been installed, this screen may not be displayed if the installer can use the same install location as previously used.

Click **Browse** to change directories.

Click **Next** to continue.



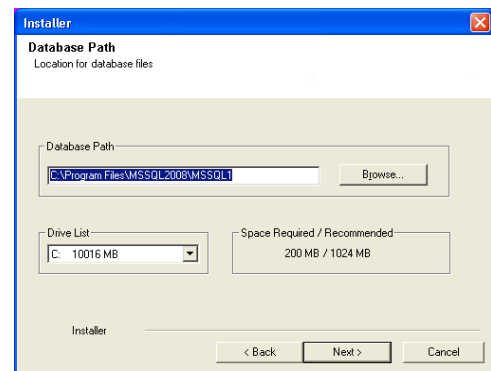
17. Specify the location of the database.

**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.

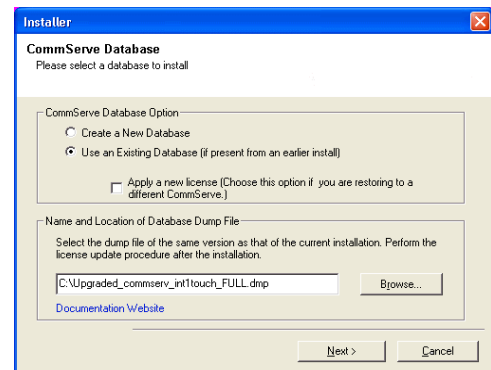
Click **Next** to continue.



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

**NOTES**

- This screen may look different from the example shown.

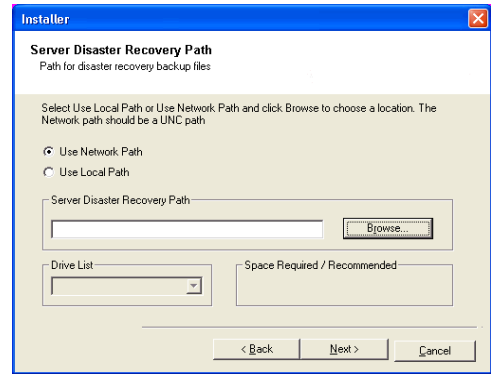


19. Enter the network or local path where Disaster Recovery Backup files should be stored.

**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.



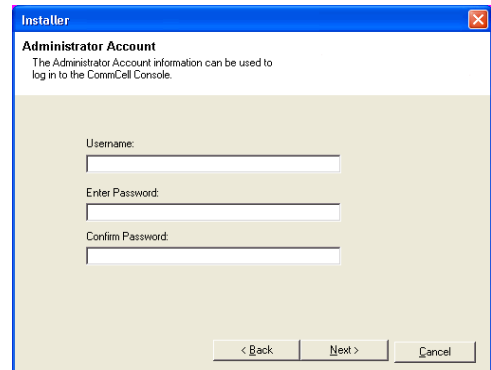
## SET USER NAMES AND PASSWORDS

20. 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.

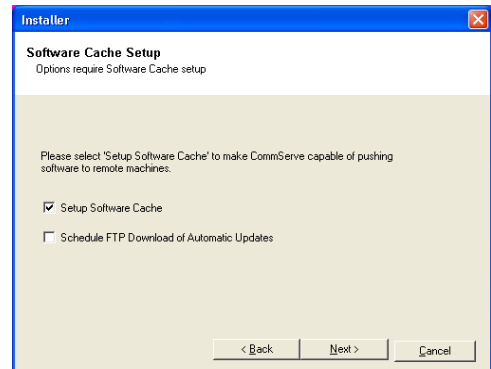
Click **Next** to continue.



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** to continue.

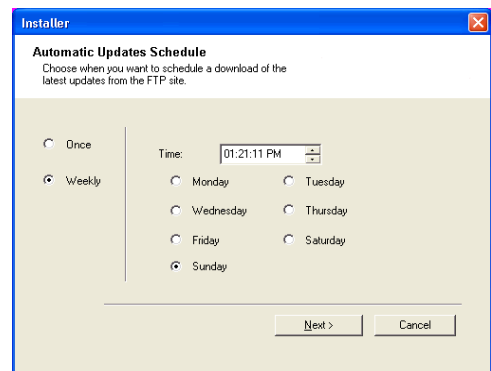


22. Schedule to download the latest software updates from the FTP site.

### 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.



23. 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.

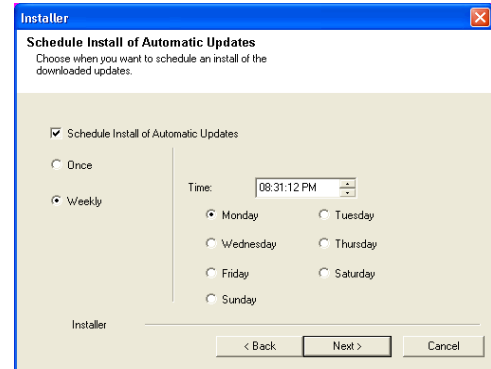
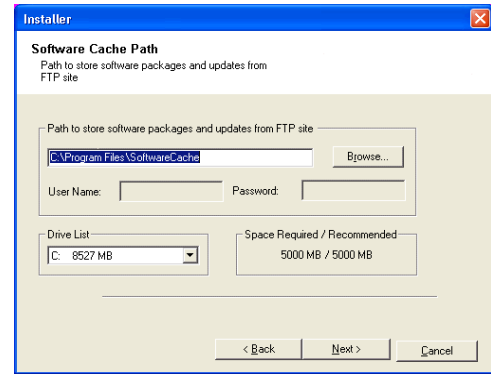
Click **Next** to continue.

24. 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.



## CONFIGURE THE COMMCELL® CONSOLE FOR WEB-BASED ADMINISTRATION

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

#### NOTES

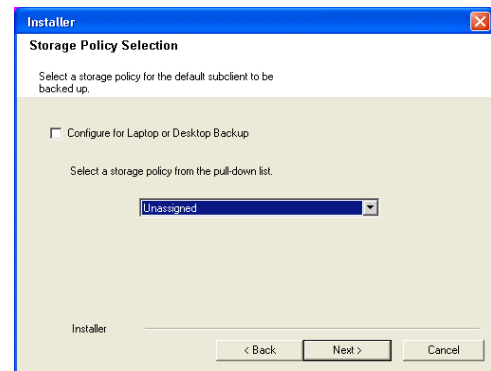
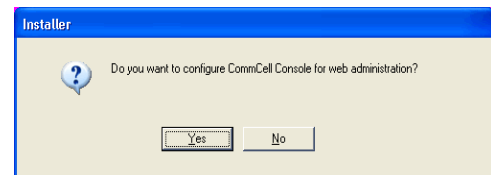
- The Internet Information Server (IIS) must be installed on this computer in order to configure for web administration.
- Configuring this computer for web administration allows you to:
  - Access the CommCell Console and Books Online from a remote computer using a Web browser.
  - View CommCell reports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

26. Select the storage policy through which you want to back up/archive the agent.

#### NOTES

- A storage policy directs backup data to a media library.
- If desired, you can change your storage policy selection at any time after you have installed the client software.
- This screen may appear more than once, if you have selected multiple agents for installation. You will be prompted to configure the storage policy association for each of the selected agents.

Click **Next** to continue.



## 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.

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

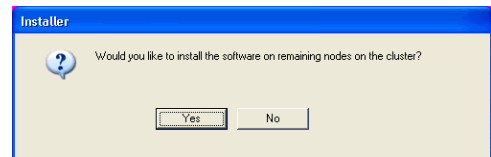


28. Select cluster nodes from the **Preferred Nodes** list and click the arrow button to move them to the **Selected Nodes** list.

**NOTES**

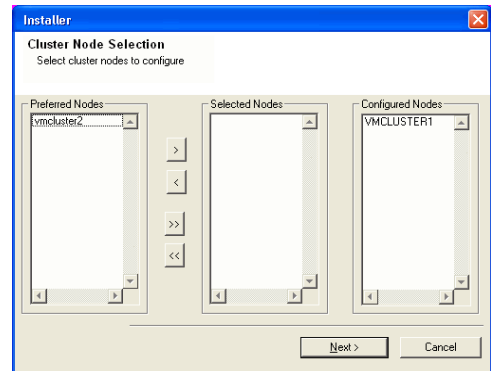
- The list of **Preferred Nodes** displays all the nodes found in the cluster; from this list you should only select cluster nodes configured to host this cluster group server.
- Do not select nodes that already have multiple instances installed. For more information, see Multi Instancing.

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



29. 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.



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

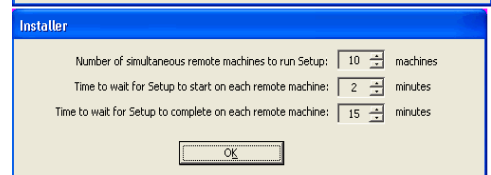
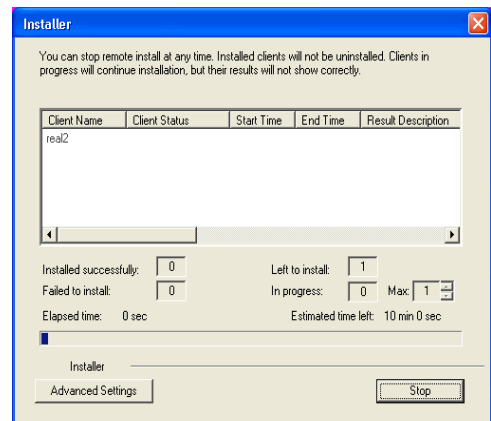
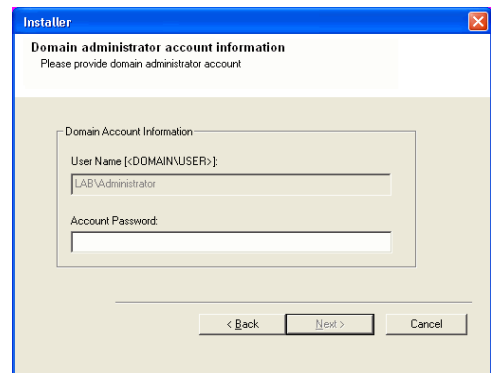
Click **Stop** to prevent installation to any nodes after the current ones complete.

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.

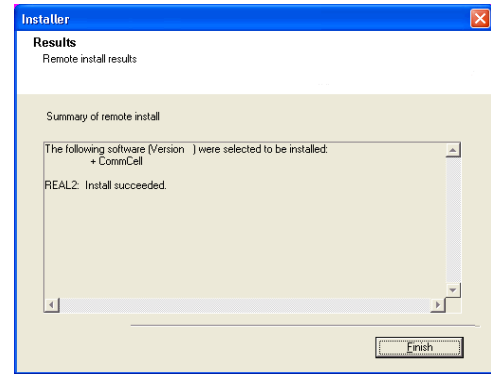


31. Read the summary for remote installation to verify that all selected nodes were installed successfully.

**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

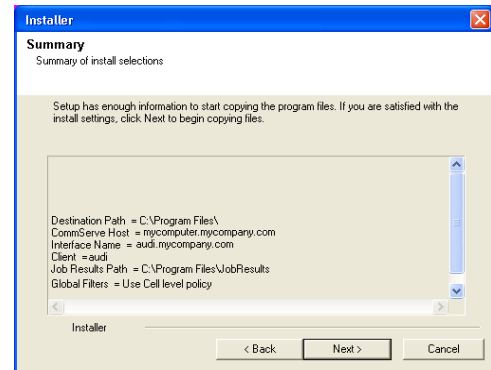
32. Verify the summary of selected options.

### 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.

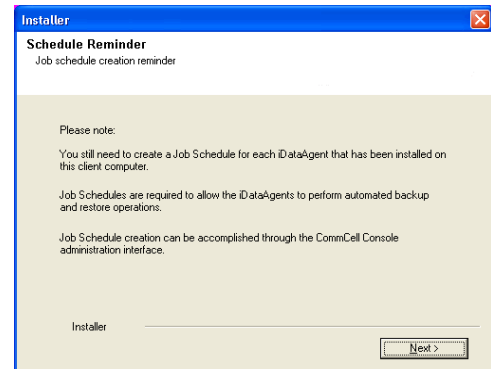
The install program now starts copying the software to the computer. This step may take several minutes to complete.



33. Click **Next** to continue.

### NOTES

- Schedules help ensure that the data protection operations for the Agent are automatically performed on a regular basis without user intervention. For more information, see Scheduling.



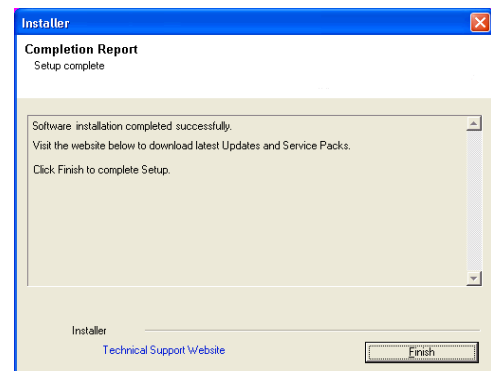
34. Setup displays the successfully installed components.

### 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.



## 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 CommNet Browser.

[Back to Top](#)

# Install the CommNet Server SNMP Enabler

## TABLE OF CONTENTS

### Install Requirements

#### Before You Begin

#### Install Procedure

- Getting Started
- Cluster Selection
- Select Components for Installation
- Configuration of Other Installation Options
- SNMP Trap Configuration
- Verify Summary of Install Options
- Install Remaining Cluster Nodes
- Setup Complete

#### Post-Install Considerations

## INSTALL REQUIREMENTS

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

The CommNet Server SNMP Enabler software must be installed on the CommNet Server computer.

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

Review the following Install Requirements before installing the software:

---

### GENERAL

- Review Install Considerations before installing the software.
- Verify that SNMP Services for Windows are running on the CommNet Server computer.
- Obtain a valid license for the CommNet SNMP Enabler software.
- SNMP Version 1 (SNMPv1) is the currently supported SNMP protocol.

---

### CLUSTER SPECIFIC

- In a clustered environment, the CommNet Server 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.

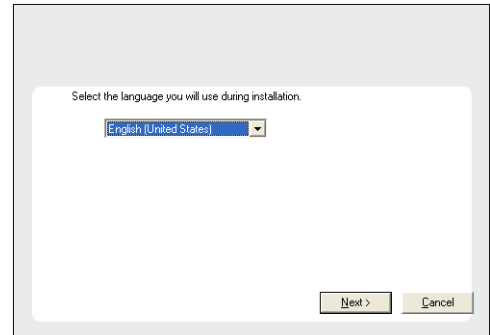
If the installation program does not launch automatically:

- 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**.

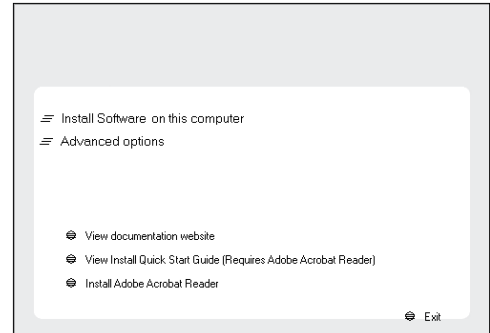
- Choose the language you want to use during installation. Click the down arrow and select the desired language from the drop-down list, and click **Next** to continue.



- 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.

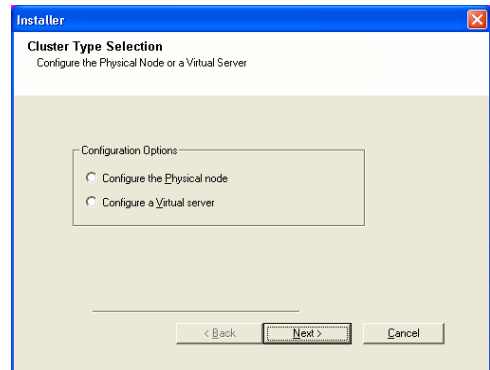


**CLUSTER SELECTION**

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

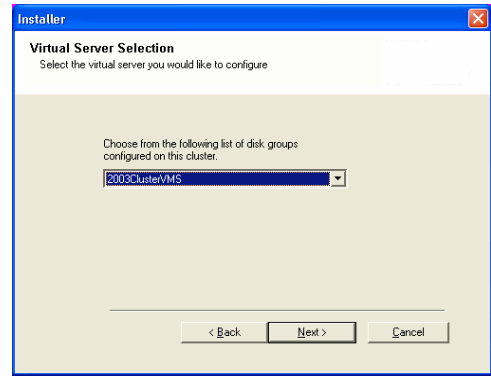
- Select **Configure a Virtual Server**.

Click **Next** to continue.



- 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.

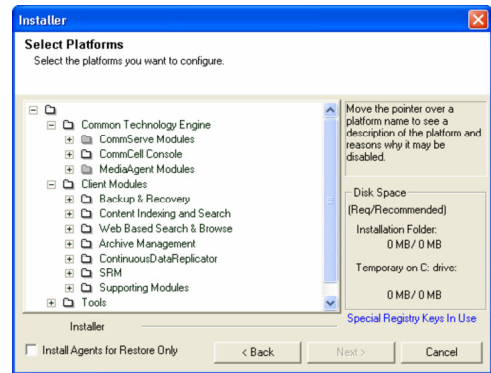
### NOTES

- 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 CommNet SNMP Enabler, expand the following `Common Technology Engine` folder, `CommServe Modules` and `CommNet` folder. Then select the following:

- `CommNet SNMP Enabler`

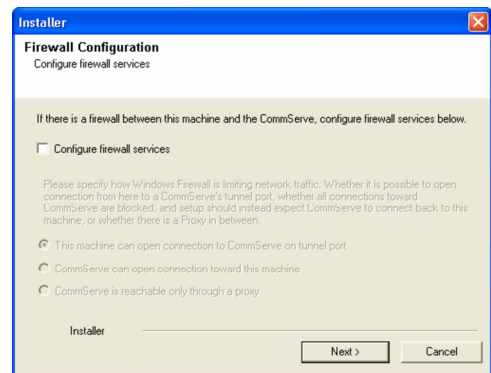


## CONFIGURATION OF OTHER INSTALLATION OPTIONS

8. If this computer and the CommServe is separated by a firewall, select the **Configure firewall services** option and then click **Next** to continue.

For firewall options and configuration instructions, see [Firewall Configuration and continue with the installation.](#)

If firewall configuration is not required, click **Next** to continue.



9. Enter the fully qualified domain name of the CommServe Host Name. This should be TCP/IP network name. e.g., `computer.company.com`.

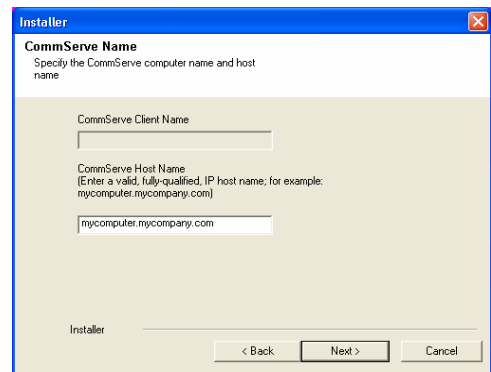
### NOTES

- The CommServe client name is the name of the computer. This field is automatically populated.
- Do not use space and the following characters when specifying a new name for the CommServe Host Name:

`|\`~!@#$$%^&*()+=<>/?,[\]\{\};:;'"`

- If a computer has already been installed, this screen will not be displayed; instead the installer will use the same Server Name as previously specified.
- If you do not specify the CommServe Host Name, a window will be prompted to continue in decouple mode. Click **Yes** to continue to Decoupled Install. Click **No** to specify a CommServe Name and continue with the installation.

Click **Next** to continue.



10. Select **Add programs to the Windows Firewall Exclusion List**, if you wish to add

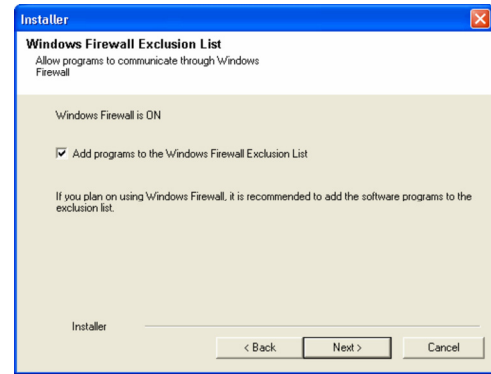
CommCell programs and services to the Windows Firewall Exclusion List.

**NOTES:**

- If Windows Firewall is enabled on the computer, this option is selected by default and must be enabled to proceed with the installation.
- If Windows Firewall is disabled on the computer, you can select this option to add the programs and services to enabled CommCell operations across the firewall, if the firewall is enabled at a later time.

You can either select this option during install or add the programs and services after installation. For adding the programs and services after installation, see Configure Windows Firewall to Allow CommCell Communication.

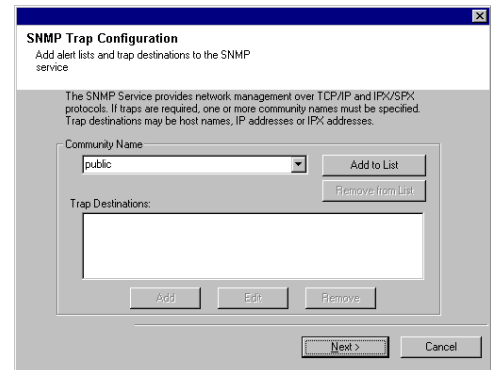
Click **Next** to continue.



## SNMP TRAP CONFIGURATION

11. 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

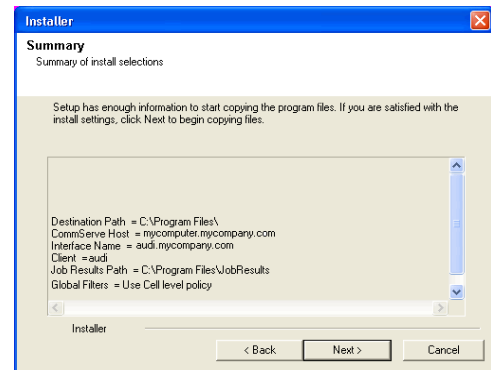
12. Verify the summary of selected options.

**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.

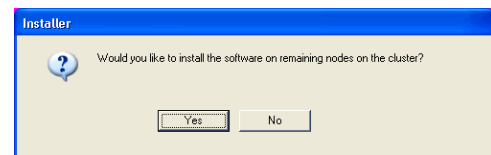
The install program now starts copying the software to the computer. This step may take several minutes to complete.



## INSTALL REMAINING CLUSTER NODES

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

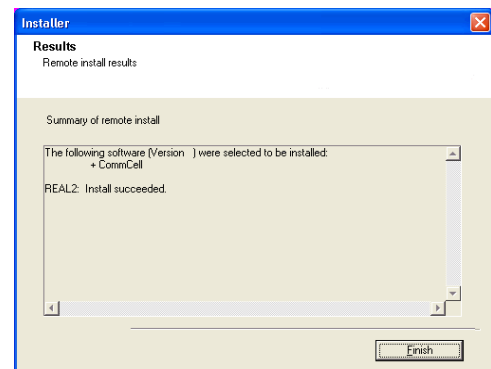
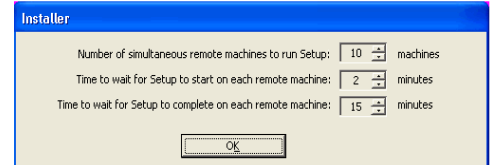
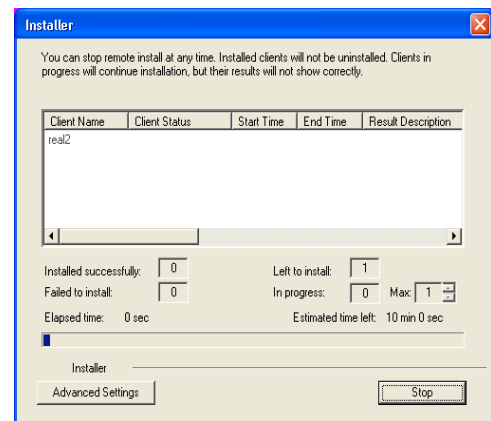
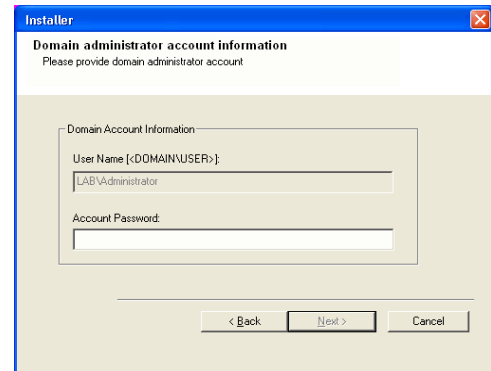
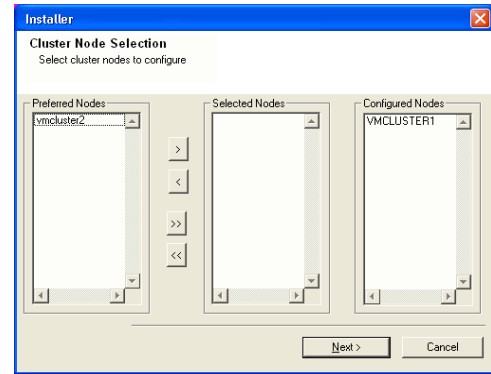
- If, during the remote install of a cluster node, setup fails to complete or is interrupted, you must perform a local install on that node. When you do, the install begins from where it left off, or from the beginning if necessary. For procedures, see *Manually Installing the Software on a Passive Node*.

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

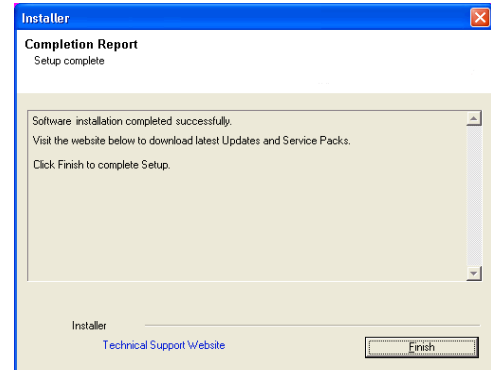
18. Setup displays the successfully installed components.

### NOTES

- The **Setup Complete** message displayed on your screen will reflect the components you installed, and may look different from the example shown.
- If **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.



## POST-INSTALL CONSIDERATIONS

Review Install Considerations after installing the software.

# Install Software from the CommCell Console (Remote Install)

Basic | **Advanced**

## TABLE OF CONTENTS

### Overview

What can be Installed  
What cannot be Installed

### Prerequisites

Space Requirement  
Firewall and Network Port Requirement  
User Permissions  
General

### Configuration

Configure the CommServe Cache Directory  
Configure Download Software

### Install Software

### View Job Details

### Verify Installation on Clients

## OVERVIEW

Agents and package distribution can now be installed - both scheduled and on-demand - from the CommCell Console. With the CommCell Console-based install capability, software can now be quickly and efficiently rolled out in large data centers and distributed WAN environments.

## WHAT CAN BE INSTALLED

Computers inside a domain, outside a domain or in multiple domains that are not yet part of the CommCell, can be selected for installation.

To see which agents are supported for Install Software from the CommCell Console, see Installation - Support.

Note that following agents are supported along with the list of agents listed in the Installation - Support.

- MediaAgent

## WHAT CANNOT BE INSTALLED

- Install Software from the CommCell Console does not support the installation of 64-bit binaries to UNIX clients.  
When you try to install software from the CommCell Console on 64-bit UNIX clients, only 32-bit binaries will be installed.
- Install Software from the CommCell Console is not supported for the following:
  - CommServe
  - CommNet Server
  - SRM Server
  - Web Search Server
  - Cluster Environment

## PREREQUISITES

### SPACE REQUIREMENT

- On the CommServe you must have adequate space in the CommServe cache directory to host the following:
  - Software Installation Discs
  - Latest Service Pack

The total amount of space can be estimated by adding the size of each of the Software Installation Discs and the latest Service Pack that you plan to host.

- On client computers you will need the temporary disk space to install the software. See System Requirement for more information on temporary space requirement.

### FIREWALL AND NETWORK PORT REQUIREMENT

Prior to installing software from CommCell Console, make sure to configure your Calypso firewall environment. For information on all available firewall scenarios, see Firewall.

To install software from CommCell Console, the following ports need to be opened:

- If you have firewall enabled on the CommServe, ensure that the client computer is able to reach the CommServe using port **8400**. This port must be open towards the CommServe to receive incoming connections from the client.

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.

- For Unix client computers, you must enable SSH (Secure Shell) and open port **22**.

In addition, if you have Solaris 11 client computers, make sure to do the following:

1. Run the following command to stop SSH on the Solaris 11 client:

```
svcadm disable ssh
```

2. Open the `/etc/ssh/sshd_config` file and add the following line at the end of the file:

```
Ciphers 3des-cbc
```

If you already have other ciphers declared, add `3des-cbc` at the end of the list after a comma (',').

3. Run the following command to start SSH.

```
svcadm enable ssh
```

- For Windows client computers, you must open the following ports:

- **445** port (SMB)
- Windows Management Instrumentation (WMI) port
- **135** port for Distributed Component Object Model (DCOM)

If you are using legacy Windows computers (Windows NT and below), you may also need to open port **139**.

- The following sections describe the steps to set up a fixed port for WMI. These steps are applicable for Windows Vista and above.

#### SET UP A FIXED PORT FOR WMI THROUGH COMMAND LINE

- At the command prompt, type `winmgmt -standalonehost`
- Stop the WMI service by typing the command `net stop "Windows Management Instrumentation"`
- Restart the WMI service again in a new service host by typing `net start "Windows Management Instrumentation"`
- Establish a new port number for the WMI service by typing `netsh firewall add portopening TCP 24158 WMIFixedPort`

#### SET UP A FIXED PORT FOR WMI THROUGH CONTROL PANEL

- On the taskbar, click **Start** and then click **Control Panel**.
- Click **Windows Firewall**.
- Click **Allow a program or feature through Windows Firewall**.
- Click **Change setting** button.
- In the **Allowed programs and features** list, select **Windows Management Instrumentation (WMI)**.

If you chose not to open port 22, 445, 135, 139 and WMI port on your network, you can setup and use a remote cache that is located in the same network in which the client computer resides. Port 8400 must be opened temporarily in order to allow the client computer to communicate with the CommServe and download Calypso firewall configuration.

---

## USER PERMISSIONS

- For the CommServe and Client computers, specific permissions must be granted to the user group(s) whose user members will be administering this feature. For more information, see Capabilities and Permitted Actions.

For the CommCell, if Authentication for Agent Installs is enabled, users must belong to a user group with Installation capabilities for the CommCell. The users can also belong to a user group with Administrative Management capabilities for the CommCell or an existing client computer. However, it is not recommended to add non-administrators to this user group.

- For install software on clients running Unix operating systems, the client computer must have SSH (secure shell) enabled, and the `PermitRootLogins` must be set to yes in the `sshd_config` file.

---

## GENERAL

- Verify that the computers in which you wish to install the software satisfies the minimum requirements specified in System Requirements.
- Install Software from the CommCell Console does not support downloading packages from HTTP Proxy.

## CONFIGURATION

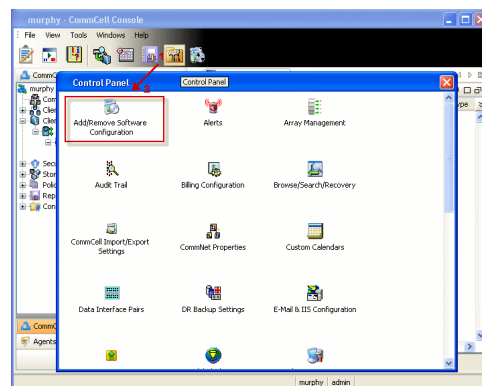
Install from CommCell Console is configured in the following sequences:

1. Configure the CommServe Cache Directory to copy or download the required software packages in the CommServe Cache directory. The directory is configured to serve as a holding area for software and update packages.
2. Configure Download Software to download the software packages to the CommServe Cache directory using an FTP source site.

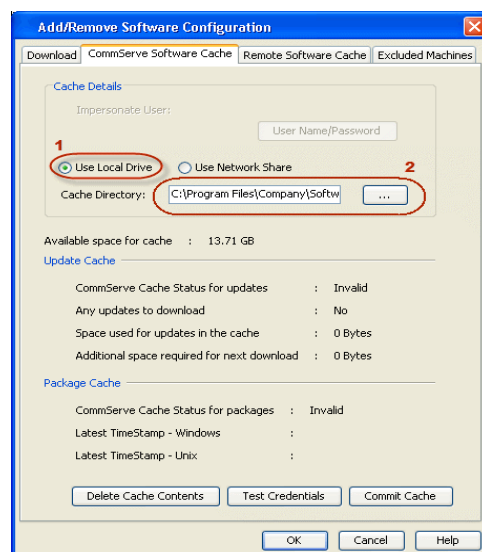
The following sections provide step-by-step instructions for configuring Install from CommCell Console.

### CONFIGURE THE COMMSERVE CACHE DIRECTORY

1. Verify that you have adequate space in the CommServe cache directory for the latest service pack.
2. From the CommCell Browser, click **Control Panel** and then click the **Add/Remove Software Configuration**.



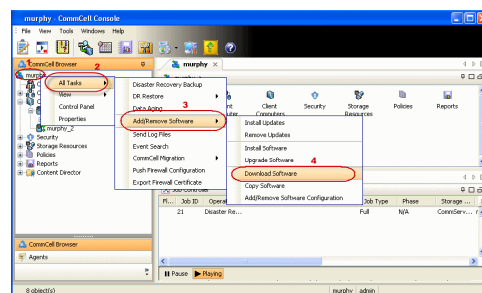
3. Select the **CommServe Software Cache** tab and select **Use Local Drive** to specify the local drive to use as a cache directory to store software packages in the **Cache Directory** field.



4. Click **OK**.

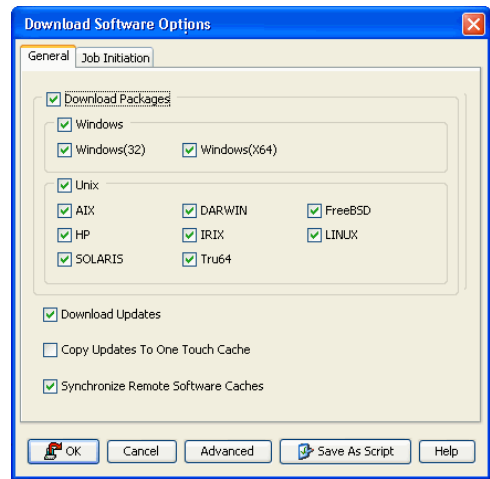
### CONFIGURE DOWNLOAD SOFTWARE

1. Verify that you have adequate space for the packages.
2. From the CommCell Browser, right-click on the CommServe computer node, and click **All Tasks -> Add/Remove Software -> Download Software**.

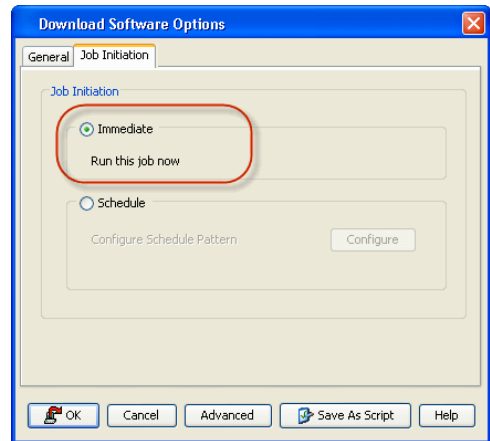


3.
  - From the **General** tab, select the **Download Packages** option which automatically selects both **Windows** and **Unix** options.

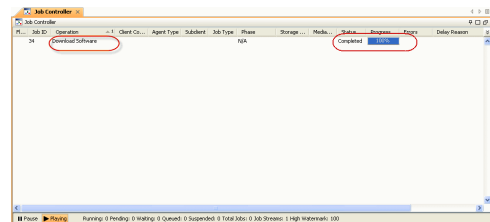
- Select **Windows** to download Windows packages for clients running Windows based operating systems.
- Select **Unix** to download Unix packages for clients running Unix based operating systems.



4.
  - Click **Job Initiation** tab.
  - Select **Immediate** to run the job now.
  - Click **OK**.



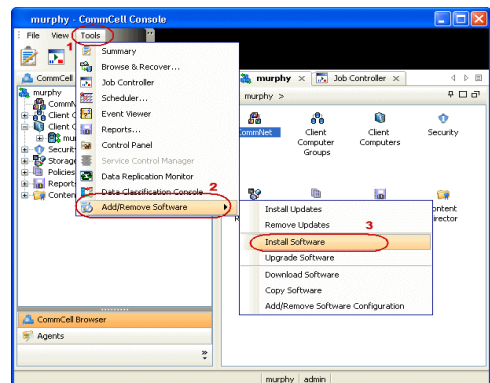
5. Once initiated, you can track the progress of the job from the **Job Controller** window.



## INSTALL SOFTWARE

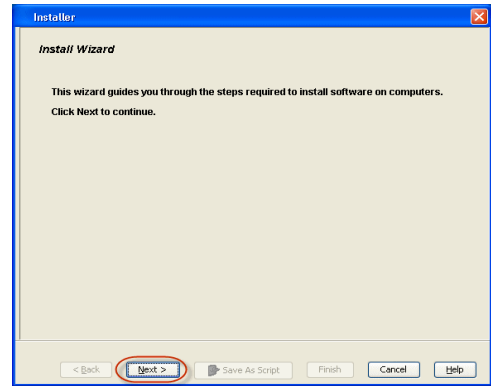
Use the following steps to install software on Windows Clients:

1. Verify that your client computer cache directories have adequate space for the software packages.
2. From the CommCell Browser, click **Tools**, point to **Add/Remove Software** and then click **Install Software**.

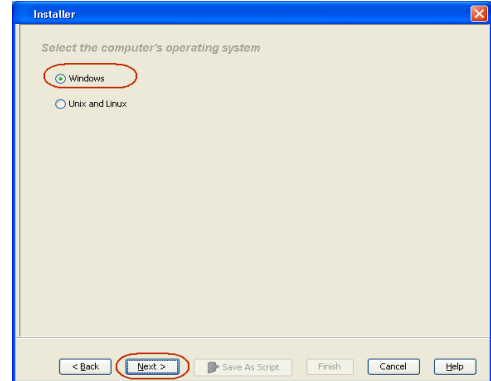


3. **Install Wizard Welcome** screen is launched. Click **Next**.

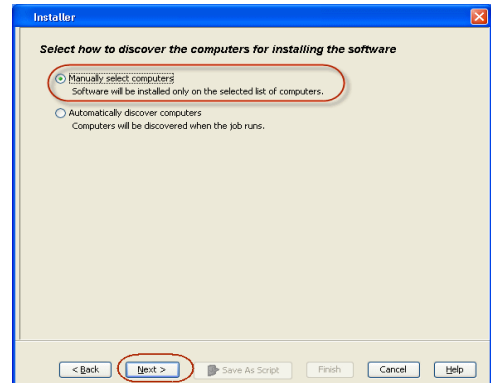
4. Select **Windows** and then click **Next**.



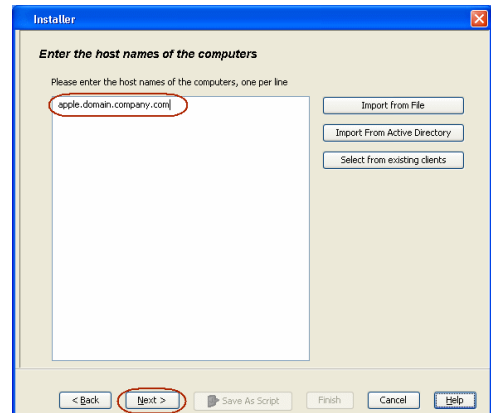
5. Select **Manually Select Computers** and then click **Next**.



6. Type the host names of the computers in the window pane manually to which you want to install the software. Computer names must be entered in the following format:  
 <computer.domain.company.com>  
 Click **Next**.



7. In the **Select Software Cache** dialog box, **Software Cache** field displays the default software cache directory in which the software packages are downloaded.  
 This Software Cache is the cache directory from which the software packages will be obtained for the client computers selected for install. If you wish to use the default, then do not select any options, and click **Next**.



8. In the **User Name** and **Password** box, specify the user account information and then click **Next**.

This user account must have administrative rights to the computer to which the software will be installed, and read-access to the computer from which the software will be retrieved.

Click **Next**.

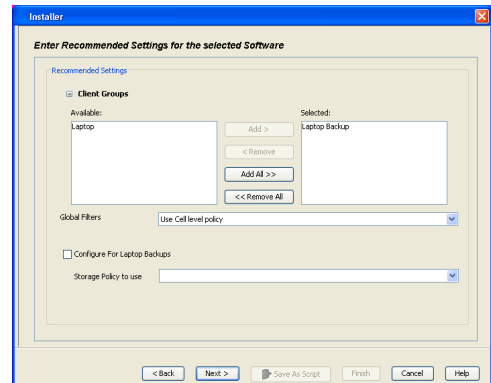
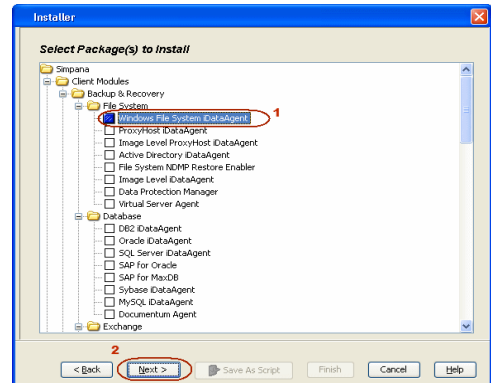
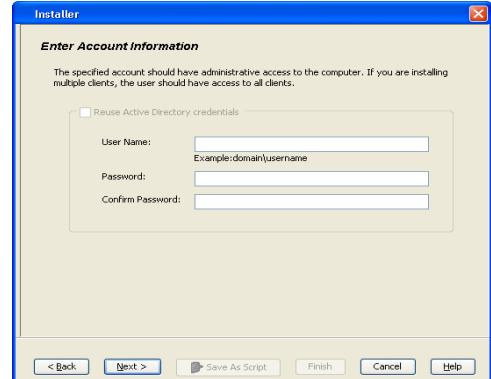
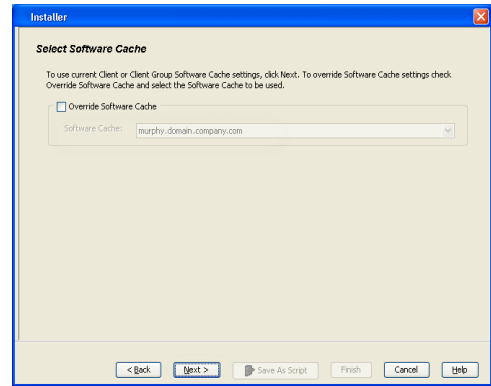
9. Select the software **Package(s)** to Install on the selected computers and then click **Next**.

- If the computer meets the requirements for the agent software, the agent software will be installed, if it does not meet the requirements, the software will not be installed on the computer, but skipped. For example, if you selected Exchange Database iDataAgent as a component for installation, this will only be installed on systems where the Exchange database is present.

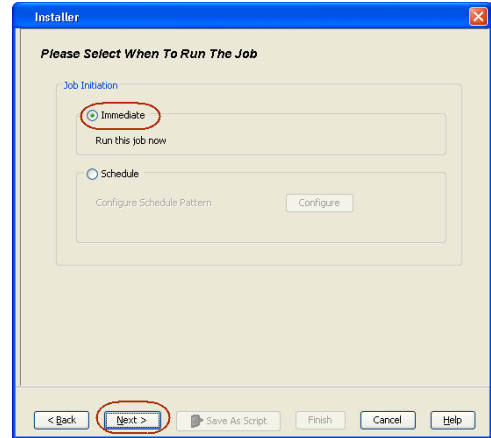
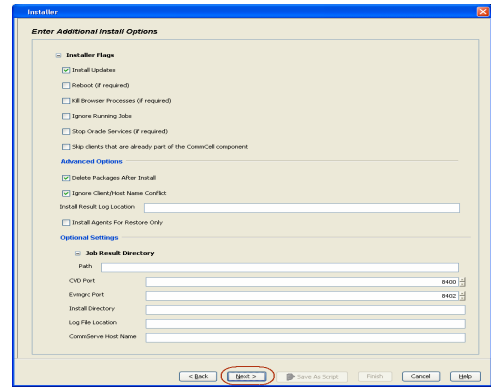
For an explanation of the options and their possible values, refer to each component's interactive installation procedure in Deployment.

10.
  - Select **Client Group** from **Available** and click **Add**.
  - Select **Configure For Laptop Backups** option to install **Backup Monitor** utility. This utility allows you to view the backup job summary of your client computer. See Monitor - Laptop User for more information.
  - Select Storage Policy from **Storage Policy to use** drop-down list.
  - Click **Next**.

11. Select and configure the **Additional Install Options** associated with the software packages that will be installed or leave the Additional Install Options at their default values and click **Next**.

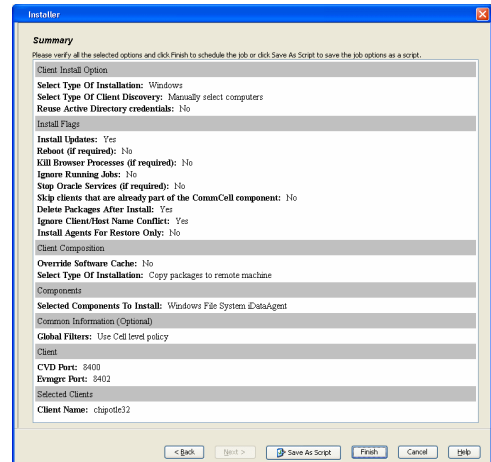


12. Select **Immediate** to run the job now and then click **OK**.



13. The summary of install operation will be displayed. Click **Finish**.

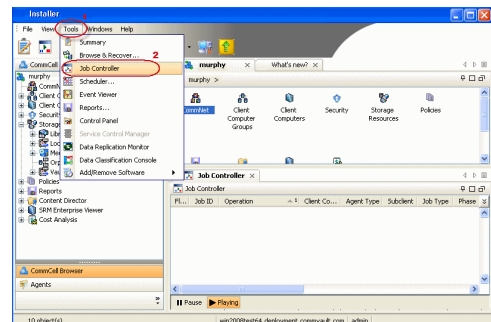
- Review the Post-Install Considerations specific to the components that were installed using this procedure.
- The software packages that are pushed to the selected client computer (s) to run the install operations are automatically deleted from the client computer(s) after the install operations have completed.



## VIEW JOB DETAILS

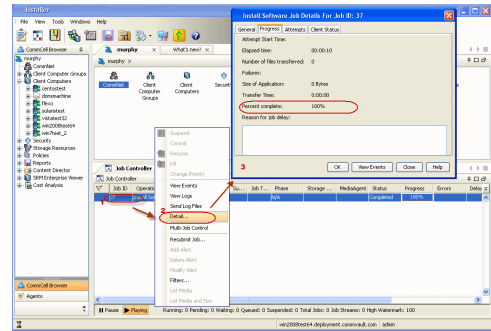
To view the job details:

1. From the **CommCell Console**, from the **Tools** menu select the **Job Controller** icon. The **Job Controller** window appears.





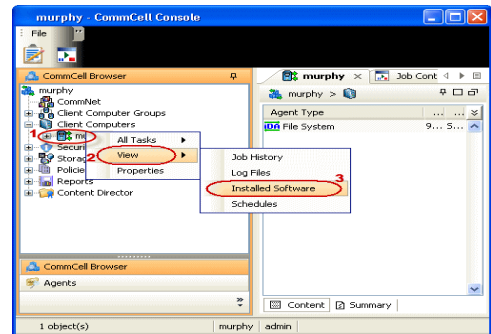
- Right-click the job and then click **Detail** from the shortcut menu. The details of the job you selected are displayed in the **Install Software Job Details For Job ID** dialog.



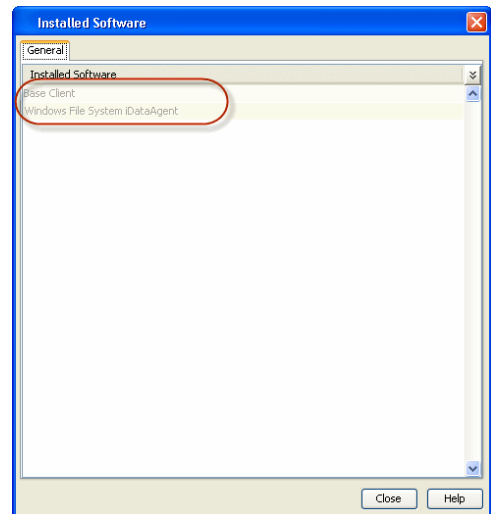
- Click **OK**.
  - If viewing the details of a job with a pending or failed status, the **Reason for Job Delay** field will contain an Error Code, which, if clicked, will launch the customer support website displaying troubleshooting article(s) related to the specific issue. Additionally, if cache corruption has been found, the field will also contain the information pertaining to the missing updates or service packs.
  - Multiple installation jobs (or uninstall jobs) can be scheduled to occur in parallel as long as the selected client computers are not scheduled for both jobs, i.e., the same client computer can not be selected for both scheduled jobs. The ability to schedule jobs in parallel can drastically reduce installation periods for your environment.

## VERIFY INSTALLATION ON CLIENTS

- From the CommCell Browser, right-click the icon of a client computer, and click **View --> Installed Software**.



- View the installed software packages from the **Installed Software** window. Click **OK**.



# Install the CommNet Browser - Windows

## TABLE OF CONTENTS

### Install Requirements

#### Before You Begin

#### Install Procedure

- Getting Started
- Cluster Selection
- Select Components for Installation
- Set Up the CommNet Interface Name
- Set Up the CommNet Browser for Web-Based Administration
- Verify Summary of Install Options
- Install Remaining Cluster Nodes
- Setup Complete

#### Post-Install Considerations

## INSTALL REQUIREMENTS

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

The CommNet Browser is the graphical user interface (GUI) that you use to control the operation of the CommNet Server. Setup allows you to install the CommNet Browser on any one or more of the following:

- CommNet Server
- Client computer
- Any other computer that can communicate with the CommNet Server via a TCP/IP network

By installing the CommNet Browser on another computer, you can remotely administer the CommNet Server.

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

Review the following Install Requirements before installing the software:

---

### GENERAL

- The CommNet Browser can only be installed after the CommNet Server has already been installed and is running.
- Close all applications and disable any programs that run automatically, including anti-virus, screen savers and operating system utilities.  
Some 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 has completed.
- 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 or upgrade the software. If you are not sure, contact your software provider.

---

### CLUSTER

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 client as local Administrator or as a member of the Administrators 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

---

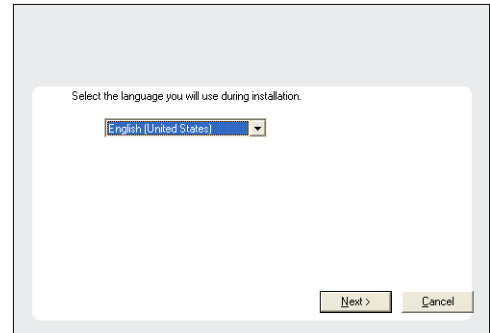
### GETTING STARTED

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**

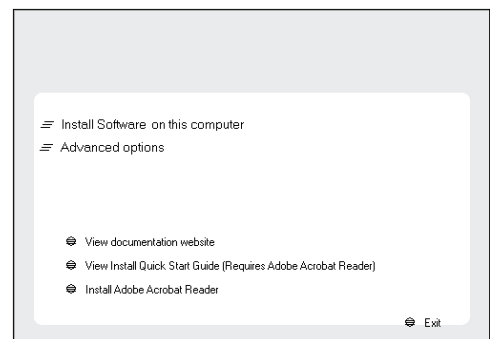
- If you are installing on Windows Server Core editions, mount to Software Installation Disc through command line, go to the **AMD64** folder and run **Setup.exe**.
2. Choose the language you want to use during installation. Click the down arrow and select the desired language from the drop-down list,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



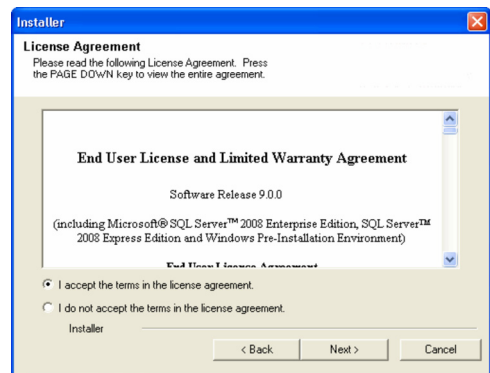
3. Select the option to install software on this computer.

**NOTES**

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



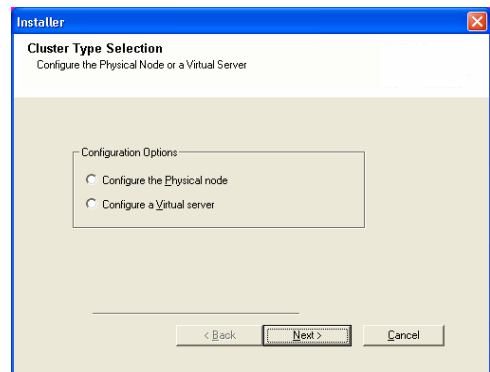
4. Read the license agreement, then select **I accept the terms in the license agreement**.  
Click **Next** to continue.



**CLUSTER SELECTION**

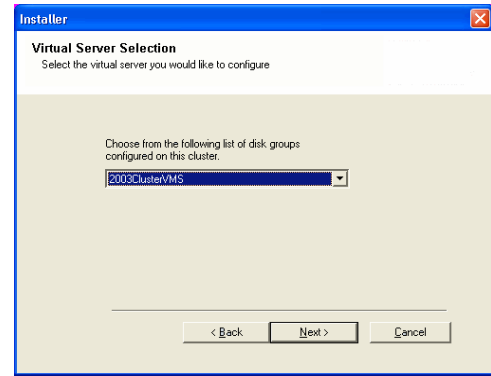
If you are installing in clustered environment, follow the steps below. For non-clustered environment, skip to Select Components for Installation.

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 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 CommNet Browser, from the `Common Technology Engine` folder expand the `CommCell Console` folder, and then select the following:

- CommNet Browser.

When you select this option, the Java Runtime Environment is automatically selected for install.

8. 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.

9. Select **Add programs to the Windows Firewall Exclusion List**, if you wish to add CommCell programs and services to the Windows Firewall Exclusion List.

### NOTES:

- If Windows Firewall is enabled on the computer, this option is selected by default and must be enabled to proceed with the installation.
- If Windows Firewall is disabled on the computer, you can select this option to add the programs and services to enabled CommCell operations across the firewall, if the firewall is enabled at a later time.

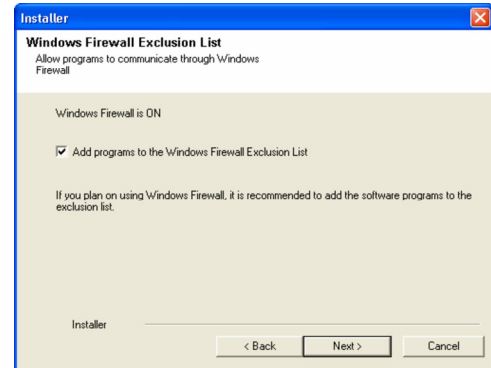
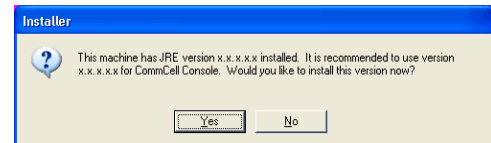
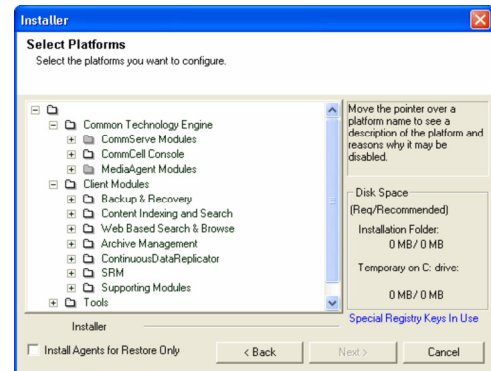
You can either select this option during install or add the programs and services after installation. For adding the programs and services after installation, see [Configure Windows Firewall to Allow CommCell Communication](#).

Click **Next** to continue.

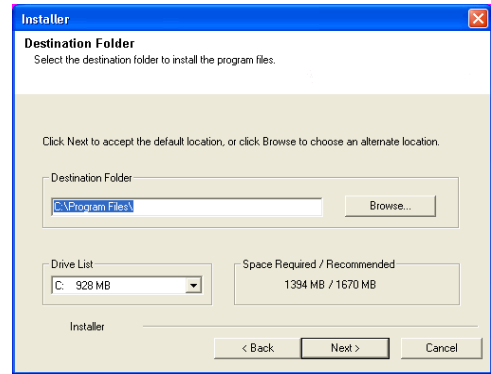
10. Specify the location where you want to install the software.

### 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.

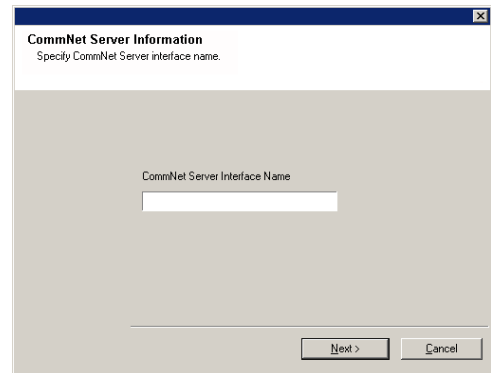


Click **Browse** to change directories.  
 Click **Next** to continue.



## SET UP THE COMMNET INTERFACE NAME

11. Specify the CommNet Server Interface Name.  
**CommNet Server Interface Name** - The TCP/IP network interface name of the CommNet Server computer.  
 Select or Enter the information and click **Next** to continue.



## SET UP THE COMMNET BROWSER FOR WEB-BASED ADMINISTRATION

12. If the Internet Information Server (IIS) is installed on this computer, the install program asks if you want to configure the software for web-based administration.  
 Click **Yes** to continue.

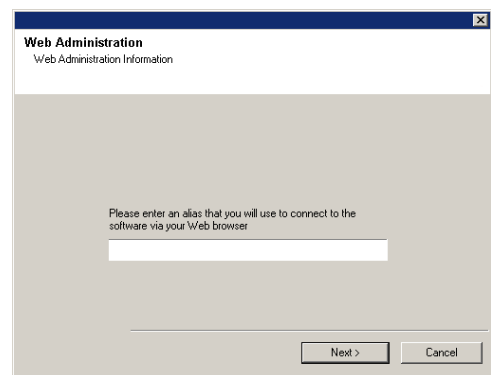
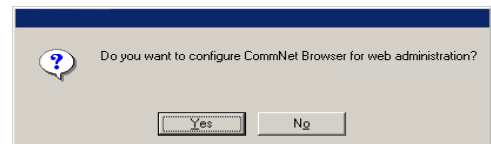
**NOTES**

- If IIS is not installed then you will not receive this prompt.
- The screen to the right may look different depending upon the software selected for install or upgrade.

13. When prompted for an alias, type the name (or use the default) of the Web alias that you want to use for accessing the CommNet Browser remotely.  
 Click **Next** to continue.

**NOTES**

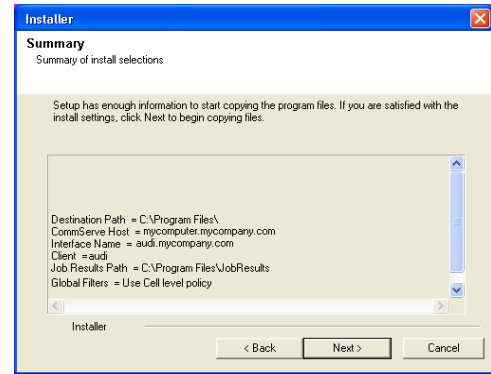
- If IIS is not installed then you will not receive this prompt.



## VERIFY SUMMARY OF INSTALL OPTIONS

14. 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.

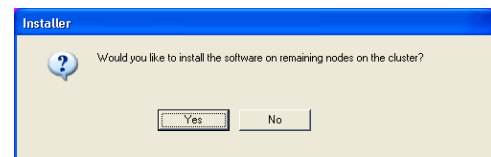
The install program now starts copying the software to the computer. This step may take several minutes to complete.



## 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.

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

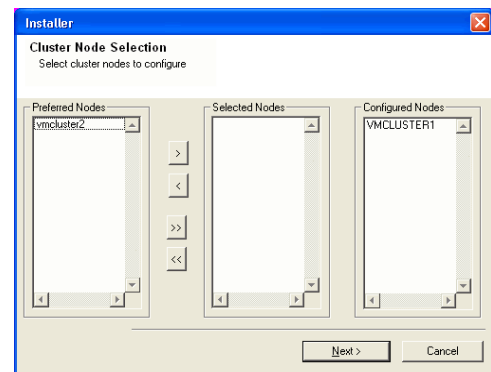


16. Select cluster nodes from the **Preferred Nodes** list and click the arrow button to move them to the **Selected Nodes** list.

### NOTES

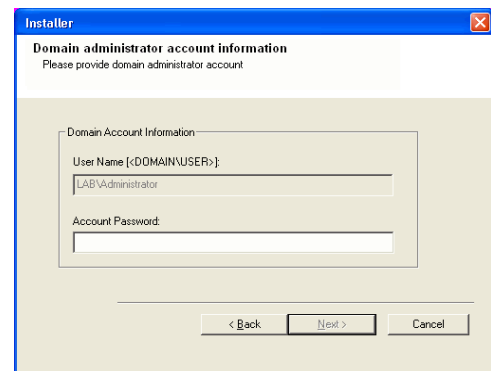
- The list of **Preferred Nodes** displays all the nodes found in the cluster; from this list you should only select cluster nodes configured to host this cluster group server.
- Do not select nodes that already have multiple instances installed. For more information, see Multi Instancing.

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



17. 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.



18. 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

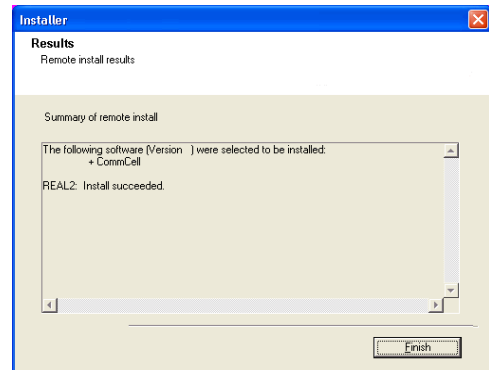
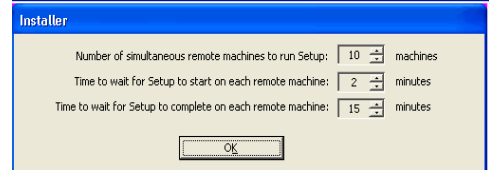
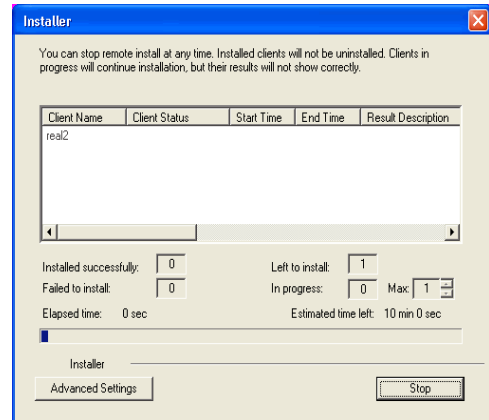
interrupted, you must perform a local install on that node. When you do, the install begins from where it left off, or from the beginning if necessary. For procedures, see [Manually Installing the Software on a Passive Node](#).

19. 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

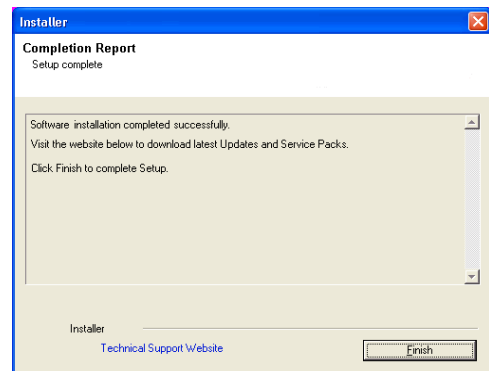
20. Setup displays the successfully installed components.

#### NOTES

- The **Setup Complete** message displayed on your screen will reflect the components you installed, and may look different from the example shown.
- If **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.



## POST-INSTALL CONSIDERATIONS

### GENERAL

- 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 CommNet Browser.

# Install the CommNet Browser - Macintosh

## TABLE OF CONTENTS

### Install Requirements

#### Before You Begin

#### Install Procedure

- Getting Started
- Select Components for Installation
- Base Software Installation

#### Post-Install Considerations

## INSTALL REQUIREMENTS

The following procedure describes the steps involved in installing the CommNet Browser software.

Review the following Install Requirements before installing the software:

---

### GENERAL

- Before installing CommNet Browser on the Macintosh/Linux platform, verify that the appropriate version of Java Runtime Environment (JRE) is installed. See System Requirements - CommNet Browser.
- Verify that the computer in which you wish to install the software satisfies the minimum requirements specified in System Requirements - CommNet Browser.
- Close all applications and disable any programs that run automatically, including anti-virus, screen savers and operating system utilities.  
Some 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 has completed.
- 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 or upgrade the software. If you are not sure, contact your software provider.

## BEFORE YOU BEGIN

- Log on to the client as root.

## INSTALL PROCEDURE

---

### GETTING STARTED

1. Place the software installation disc for the Unix platform into the disc drive.

You can also install the product using a disc drive mounted on another computer on the network.

- On Solaris, double-click the **cvpkgadd** program from the File Manager window.
- On other Unix platforms, open the Terminal window, navigate to the software installation disc and then enter **./cvpkgadd**.

2. The product banner and other information is displayed.

Press **Enter** to continue.

3. Read the license agreement. Type **y** and press **Enter** to continue.

4. Enter the number corresponding to the setup task you want to perform.

Please select a setup task you want to perform from the list below:

Advance options provide extra setup features such as creating custom package, recording/replaying user selections and installing External Data Connector software.

- 1) Install data protection agents on this computer
- 2) Advance options
- 3) Exit this menu

Your choice: [1]

#### NOTES

- For Install data protection agents on this computer option, follow the steps described in this procedure.
- Advance options provide additional setup features such as record and play setup, creating a custom package and External Data Connector Agent software.

To create a custom package and for record and play setup, follow the steps described in Custom Package - Unix.

To install the External Data Connector Agent, follow the steps described in External Data Connector - Unix.

5. If you have only one network interface, press **Enter** to accept the default network interface name and continue.

If you have multiple network interfaces, enter the number corresponding to the network interface that you wish to use as default, and then press **Enter** to continue.

Network interface with the following IPs have been found available on your system. One of these interfaces should be associated with the physical machine being installed. It will also be used by the CommServe to initiate connections to the physical machine. Note that you will be able to additionally customize Datapipe Interface Pairs



**NOTES**

- The interface name and IP addresses depend on the computer in which the software is installed and may be different from the example shown.

Verify the default network interface name.

Press **Enter** to accept the default network interface name and continue, or Type the default network interface name, and then press **Enter** to continue.

**NOTES**

- This prompt will be displayed only when you have multiple network interfaces for the computer.
6. Specify the client name for the computer.

Press **Enter** to accept the default name and continue, or Enter a new client name for the computer and then press **Enter** to continue.

used for the backup data traffic later in the Calypso Java GUI.

Please select the correct network interface below.  
1) client (201.42.33.598)  
2) hk97::489:9glg:hk8d:9490  
3) client.company.com (hr90:8842:2:78:013:8ghh:hg8k:9x54)

Interface number: [1]

Please verify the physical machine interface name below. Make it as complete (with fully qualified domain name) as possible:

Physical Machine Host Name: [angel.company.com]

Please specify the client name for this machine.

It does not have to be the network host name: you can enter any word here without spaces. The only requirement is that it must be unique on the CommServe.

Physical Machine Client name: [angel]

**SELECT COMPONENTS FOR INSTALLATION**

7. Enter the number corresponding to the **CVGxQGUI** module.

A confirmation screen will mark your choice with an "X". Type "d" for **Done**, and press **Enter** to continue.

**NOTES**

- To select multiple component, enter the number by adding a space.
- Your screen may look different from the example shown.
- Components that either have already been installed, or which cannot be installed, will not be shown.
- In addition, the list of modules that appear depends on the specific Unix File System in which the package is installed. (e.g., **CVGxWA** will appear only when the installation package is run on a Solaris computer.)

Install Calypso on physical machine client.company.com

Select the Calypso module that you would like to install

```
[ ] 1) Media Agent          [1301] [CVGxMA]
[ ] 2) FileSystem IDA      [1101] [CVGxIDA]
> ) >>>> NEXT PAGE >>>>>
```

[a=all n=none r=reverse q=quit d=done >=next <=previous ?=help]

Enter number(s)/one of "a,n,r,q,d,>,<,>?" here: 2

**BASE SOFTWARE INSTALLATION**

8. If you wish to install the agent software for restore only, enter **Yes** and press **Enter** to continue. See *Installing Restore Only Agents* for more information.

Otherwise, accept **no**, press **Enter** to continue.

9. Type the appropriate number to install the latest software scripts and press **Enter** to continue.

**NOTES**

- Select **Download from the software provider website** to download the latest software scripts from your software provider website.  
Make sure you have internet connectivity when you are using this option.
- Select **Use the one in the installation media**, to install the software scripts from the disc or share from which the installation is performed.
- Select **Use the copy I already have by entering its unix path**, to specify the path if you have the software script in an alternate location.

10. Enter **Yes** to download and install the latest service packs and post packs from the software provider.

**NOTES**

- Internet connectivity is required to download updates.
- This step is applicable for multi instancing.

Press **Enter** to continue.

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

**NOTES**

- The amount of free space required depends on the components selected for install, and may look different from the example shown.

Press **Enter** to accept the default path and continue, or

Do you want to use the agents for restore only without consuming licenses? [no]

Installation Scripts Pack provides extra functions and latest support and fix performed during setup time. Please specify how you want to get this pack.

If you choose to download it from the website now, please make sure you have internet connectivity at this time. This process may take some time depending on the internet connectivity.

```
1) Download from the software provider website.
2) Use the one in the installation media
3) Use the copy I already have by entering its unix path
Your choice: [1] 2
```

Keep Your Install Up to Date - Latest Service Pack

Latest Service Pack provides extra functions and latest support and fix for the packages you are going to install. You can download the latest service pack from software provider website.

If you decide to download it from the website now, please make sure you have internet connectivity at this time. This process may take some time depending on the internet connectivity.

Do you want to download the latest service pack now? [no]

Press <ENTER> to continue ...

Please specify where you want us to install Calypso binaries.

It must be a local directory and there should be at least 394MB of free space available. All files will be installed in a "calypso" subdirectory, so if you enter "/opt", the files will actually be placed into "/opt/calypso".

Installation Directory: [/opt]

Enter a path and then press **Enter** to continue.

Press **Enter** again to confirm the path.

12. The installation is now complete.

..

Calypso will be installed in /opt/calypso.  
Press ENTER to continue ...

Done.

Thank you for choosing Bull.

## POST-INSTALL CONSIDERATIONS

---

### GENERAL

Install post-release updates or Service Packs that may have been released after the release of the software. When you are installing a Service Pack, ensure that it is the same version as the one installed in the CommServe Server. Alternatively, you can enable Automatic Updates for quick and easy installation of updates in the CommCell component.

[Back to Top](#)

# CommNet User Administration and Security

Topics | How To | Tasks | Troubleshoot | Related Topics

Overview

Capabilities and Permitted Actions

User Tasks

User Group Tasks

Single Sign On

## OVERVIEW

Users have access to the resources and features of the CommCell based on the following:

- User accounts
- User Groups

## USER GROUPS

A user group is a logical entity through which capabilities are assigned. Users that are members of a user groups are entitled to the same rights as the user group. A user group can either administer the CommNet Server, (with the CommNet Server capability), or can administer a selected CommCell (with the CommCell Administration capability), or both.

The master user group is created automatically upon installation of the software. This group is automatically assigned to administer the CommNet Server and any CommCell that is part of the CommNet domain. Additional user groups can be created from the CommNet Browser.

## USERS

All users that perform software functions must have a user account and be assigned to one or more user group(s). Once a user is part of a user group, this user assumes all the rights of the member user group.

When a user opens a CommNet Browser, depending on the user group to which the user is attached, only those CommCells that can be controlled by the user will be displayed. If a user is part of a user group that does not have the capability to control specific Cells, that user will not see those Cells in the CommNet Browser.

A default user is automatically created when the software is installed. This user is by default assigned to the **master** user group.

If necessary, additional users can be created.

## NAME SERVERS

Name Servers comprises of external domains and external user groups to which CommNet 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.

## CAPABILITIES AND PERMITTED ACTIONS

The capabilities of each user group permit its member users to perform certain actions. For information on these permitted actions. The following table lists the actions that a user can perform based on the assigned capabilities of the member user group: (Note that a user group with the CommCell Administration capability can only perform actions on the associated CommCells.)

Capability	Permitted Action
CommNet Administration Only	License Administration Cell Registration / Cell Re-Registration Modify CommNet Server properties Create or modify a user Create/modify a user group with only CommNet Administration capability Create/modify/delete alerts Modify/delete schedules (a user that created a schedule can modify and/or delete it without the CommNet administration capability) Create/modify/delete cost categories and billable entities

	Configure/modify the SLA configuration Create/modify/delete cell-client groups Add/Modify/Delete Global Filters
CommCell Administration Only	Generate CommCell reports Generate client computer and storage resource information of a CommServe Create/modify/delete cell-client groups (a user can only modify/delete a cell-client group that they created) Create schedules Able to view: <ul style="list-style-type: none"> <li>• Client status</li> <li>• License summary</li> <li>• Drive status</li> <li>• Event Viewer</li> <li>• MediaAgent status</li> <li>• Library status</li> <li>• Job Controller</li> </ul>
CommNet Administration and CommCell Administration	All capabilities from CommNet Administration and CommCell Administration, and: Synchronize CommCells Modify CommCell registration Modify CommServe data collection policy CommCell authentication Modify CommCell configuration Create/modify a user and user group with the CommCell Administration capability only Create/modify/delete cell-client groups

## USER TASKS

For the Users node, the Users Status task from the **Users Tasks** section of the CommNet Browser can be used to view the various attributes of all the users within the CommNet domain.

For a particular user, the Summary task from the **User Tasks** section of the CommNet Browser can be used to view detailed information about that user.

Each window displays the local time of the CommNet Server.

## USER GROUP TASKS

For the User Groups node, the User Groups Status task from the **User Groups Tasks** section of the CommNet Browser can be used to look at various attributes of all the user groups within the CommNet domain.

For a particular user group, the Summary task from the **User Group Tasks** section of the CommNet Browser can be used to view all members and capabilities of a user group.

Each task window displays the local time of the CommNet Server.

## SINGLE SIGN ON

The Single Sign On feature enables users to login to the CommNet Server using their user-account credentials for the Active Directory service provider, inheriting capabilities on the CommNet Server based on their Active Directory group membership permission(s), 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 CommNet Server and select **Cancel** before the application initiates the login process. The username field is pre-populated if the user is connecting to the CommNet Server, and the Active Directory domain they are currently logged into has been configured on the CommNet Server. 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 CommNet Server automatically recognizes that the password information must be authenticated by the external domain server.

Single Sign On supports Active Directory configured with secure Lightweight Directory Access Protocol (LDAP), which provides additional network security. If Active Directory (the external domain) is configured with LDAP, you can configure the external domain controller from the Add/Edit New Domain Controller dialog box to use the secure 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. If this protocol is enabled from the CommNet Browser's Add/Edit New Domain Controller dialog box, but not

configured from the external domain; the feature is not enabled.

---

## CONFIGURATION

Before the Single Sign On feature can be used, users must provide the information required to communicate with the Active Directory service provider (such as domain name, hostname of directory server, directory service type, username and password) so that it will be maintained in the CommNet database for authentication purposes. To do this, you must Add a New Domain Controller, which registers the external domain with the CommNet Server. Once you enter this information, you or an administrator, must associate certain external domain user groups (domain name\user group) with a user group defined in the CommNet. This will provide the external domain users access to the CommNet entities. For more information, see Add a New External User Group.

Once configured, if necessary, users can temporarily disable the feature or change user credentials. For more information, see Disable Single Sign On from a Specific Browser.

There are no license requirements to utilize this feature.

[Back to Top](#)

# CommNet User Administration and Security - How To

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

---

## User Groups

[Create a User Group](#)

[Delete a User Group](#)

[Modify the Properties of a User Group](#)

[Change the Capabilities and Association of a User Group](#)

[Change the Members of a User Group](#)

## Users

[Create a User](#)

[Delete a User](#)

[Change the Password of a User](#)

[Change the User Group Association of a User](#)

[Modify the Properties of a User](#)

## Single Sign On

[Add a New Domain Controller](#)

[View/Edit Properties of an External Domain](#)

[Delete a Domain](#)

[Add New External User Group](#)

[Enable/Disable Single Sign On](#)

[Disable Single Sign On from a Specific Browser](#)

---

## CREATE A USER GROUP

*Required Capability:* See Capabilities and Permitted Actions

▶ To create a user group:

1. From the CommNet tree, expand **Security**, right-click the **User Groups** node, and click **New User Group**.
2. In the Enter General Information dialog box, enter the name of the user group and a description, then click **Next**.
3. In the Members dialog box, select the users that should be associated with this group, then click **Next**.
4. In the Set Capabilities dialog box, assign the capabilities to the user group.
5. Click **Finish**.

## DELETE A USER GROUP

*Required Capability:* See Capabilities and Permitted Actions

▶ To delete a user group:

1. From the CommNet tree, expand **Security**, then expand **User Groups**.
  2. Right-click the user group to be deleted, and choose **Remove User Group**.
  3. Click **Yes** to the confirmation message. The user group is now deleted.
- 

## MODIFY THE PROPERTIES OF A USER GROUP

*Required Capability:* See Capabilities and Permitted Actions

▶ To modify the properties of a user group:

1. From the CommNet tree, expand **Security**, then expand **User Groups**, and select the user group to be modified.
  2. On the general pane of the **User Group Summary** window, click **Modify**.
  3. In the User Group Properties dialog box, change the appropriate fields, as necessary.
  4. Click **OK**.
- 

## CHANGE THE CAPABILITIES AND ASSOCIATIONS OF A USER GROUP

*Required Capability:* See Capabilities and Permitted Actions

▶ To change the capabilities and associations of a user group:

1. From the CommNet tree, expand **Security** and **User Groups**, then select the appropriate user group.
  2. On the capabilities pane of the **User Group Summary** window, click **Modify**.
  3. From the User Group Capabilities dialog box, select either CommNet Administration or CommCell Administration.  
For CommCell Administration from the CommCells tab, select or de-select the CommCells, as necessary.
  4. Click **OK**.
- 

## CHANGE THE MEMBERS OF A USER GROUP

*Required Capability:* See Capabilities and Permitted Actions

▶ To change the members of a user group:

1. From the CommNet tree, expand **Security** and **User Groups**, then select the appropriate user group.
  2. On the members pane of the **User Group Summary** window, click **Modify**.
  3. In the User Group Members dialog box, select or deselect users to/from the user group, as necessary.
  4. Click **OK**.
- 

## CREATE A USER

*Required Capability:* See Capabilities and Permitted Actions

▶ To create a user:

1. From the CommNet tree, expand **Security**, right-click **Users**, and select **New User**.
  2. In the Enter General Information dialog box, enter the appropriate fields as necessary, then click **Next**.
  3. In the User Group Association dialog box, select the user group(s) that the user should belong to.
  4. Click **Finish**.
-

## DELETE A USER

*Required Capability:* See Capabilities and Permitted Actions

▶ To delete a user:

1. From the CommNet tree, expand **Security**, then expand **Users**.
2. Right-click the user to be deleted, then select **Remove User**.
3. Click **Yes** to the confirmation message. The user is now deleted.

If this user account was used to schedule a report or create an alert, upon deletion of the account, you will be prompted to transfer ownership of the report schedule or alert to another user.

---

## CHANGE THE PASSWORD OF A USER

*Required Capability:* See Capabilities and Permitted Actions

▶ To change the password of a user:

1. From the CommNet tree, expand **Security**, then expand **Users**.
  2. Right-click the appropriate user, then select **Change Password**.
  3. Enter the old password in the **Logged in User Password** field.
  4. Enter and confirm the new password in the **New Password for** and **Confirm New Password** fields.
  5. Click **OK**.
- 

## CHANGE THE USER GROUP ASSOCIATION OF A USER

*Required Capability:* See Capabilities and Permitted Actions

▶ To change the user group association of a user:

1. From the CommNet tree, expand **Security**, then expand **Users**, and select the appropriate user.
  2. On the user group association pane of the **User Summary** window, click **Modify**.
  3. From the User Group Association dialog box, add or remove user groups to/from this user, as necessary.
  4. Click **OK**.
- 

## MODIFY THE PROPERTIES OF A USER

*Required Capability:* See Capabilities and Permitted Actions

▶ To modify the properties of a user:

1. From the CommNet tree, expand **Security**, then expand **Users**, and select the user to be modified.
  2. On the General section of the **User Summary** window, click **Modify**.
  3. In the User Properties dialog box, change the appropriate fields, as necessary.
  4. Click **OK**.
- 

## ADD A NEW DOMAIN CONTROLLER

*Required Capability:* See Capabilities and Permitted Actions

▶ To add a new domain controller:

1. From the CommNet Browser, expand **Security**, and right-click on **Name Servers**. From the popup menu, select **New Domain**.
2. Enter the appropriate information in the Add New Domain Controller dialog box. You will need to enter the following information:
  - Domain Name
  - Directory Server Host Name

- o User Account: Click **Edit** to enter the user account information for the external domain.

Upon entering this information, you will need determine whether the domain controller should be enabled for the SSO feature (Single Sign On) and/or disabled for use.

3. Enable the secure Lightweight Directory Access Protocol (**LDAP**) Communication 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. If this protocol is enabled from this dialog box, but not configured from the external domain; the feature is not enabled.
  4. Click **OK**.
- 

## VIEW/EDIT SUMMARY OF AN EXTERNAL DOMAIN

*Required Capability:* See Capabilities and Permitted Actions

▶ To view the summary of an external domain:

1. From the CommNet Browser, expand **Security**, and right-click on **Name Servers**.
  2. Right click on the domain for which you wish to view the summary, and select **Summary** from the popup menu.
  3. Click **Modify** to launch the Edit Domain Controller dialog box where you can edit the properties of the external domain.
- 

## DELETE AN EXTERNAL DOMAIN

*Required Capability:* See Capabilities and Permitted Actions

▶ To view the properties of an external domain:

1. From the CommNet Browser, expand **Security**, and right-click on **Name Servers**.
  2. Right click on the domain for which you wish to view the properties, and select **Remove Name Server** 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 CommNet Browser, expand **Security**, then 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 CommNet User groups.
  4. Select the CommNet user groups to associate with the specified external user group.
  5. Click **OK**.
- 

## ENABLE/DISABLE SINGLE SIGN ON

*Required Capability:* See Capabilities and Permitted Actions

▶ To enable/disable Single Sign On:

1. From the CommNet Tree, 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.
- 

## DISABLE SINGLE SIGN ON FROM A SPECIFIC BROWSER

*Required Capability:* See Capabilities and Permitted Actions

▶ To disable Single Sign On from a specific browser:

1. Right-click on the application icon, and select **Properties**.
2. From the **Browser Properties** dialog box, select the **Shortcut** tab.



3. 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.

---

[Back to Top](#)

# Set Up IIS Server for Web Administration

Topics | How To | Troubleshoot | Related Topics

The CommNet Browser as a Remote Web-Based Application allows you to administer the system from a Java-enabled web browser. During the installation of the CommNet Server, you will be prompted to configure web administration if Internet Information Service (IIS) is installed and running on the computer.

If the CommNet Server computer does not have IIS installed and running, you can use another computer with IIS in your domain to set up web administration, allowing the CommNet Browser to be run remotely from a Java-enabled web browser. Once the setup is complete, you should be able to enter the IIS server name and alias (e.g., `http://server1/Monitor`) into a web browser to start the web-based CommNet Browser.

For example, you have a CommNet Server called **green**. Green does not have IIS installed, however, another computer in your network, **blue**, already has IIS installed and running. To configure the web-based CommNet Browser to run using **blue** as the IIS server, you create a virtual directory called **Monitor** on blue that points to **green\<Software Install Path>**. The web alias is the virtual directory name, **Monitor**. Once this is complete, you can start the web-based CommNet Browser by entering **http://blue/Monitor** into your web browser.

You can remotely administer a CommCell by opening the CommCell Console from the CommNet Browser.

Note that when the CommNet Browser is opened as a remote web-based application, the CommCell Console is also opened as a remote web-based application. If the CommNet Browser is opened as an application, the user is provided with the option to open the CommCell Console either as an application (if the CommCell Console is appropriately installed in the target CommCell) or as a remote web-based application.

## Set Up IIS Server for Web Administration - How To

Topics | How To | Troubleshoot | Related Topics

Configure an IIS server other than the CommNet Server for Web Administration

Change the URL for Launching the CommCell Console for Remote Administration

### CONFIGURE AN IIS SERVER OTHER THAN THE COMMNET SERVER FOR WEB ADMINISTRATION

*Required Capability:* See Capabilities and Permitted Actions

▶ To configure an IIS Server:

1. On the computer that has IIS installed and running, log on as an Administrator or member of the Administrators group.
2. Open the Windows Internet Information Service Manager.
3. Create a virtual directory. The virtual directory name will be the web alias.
4. Configure the virtual directory to point the installation folder on the CommNet Server. You can enter a UNC path to the CommNet Server or **Browse** to the location.



Once the setup is complete, you should be able to enter the IIS server name and alias (e.g., `http://server1/Monitor`) into a web browser to start the CommNet Browser as a remote web-based application.

### CHANGE THE URL FOR LAUNCHING THE COMMCELL CONSOLE FOR REMOTE ADMINISTRATION

*Required Capability:* See Capabilities and Permitted Actions

▶ To change the URL:

1. On the **Setup** menu, click **Cell Configuration**.
2. From the Cell Configuration (General) dialog box, type the new URL in the **URL** box.
3. Click **OK**. The new URL is saved.
  - You can edit the URL to use another IIS server which points to the CommServe computer. Once saved, the CommNet Browser will subsequently use the URL to launch the appropriate Console, when you choose the **Remote Administration** option from the appropriate Cell.
  - If the correct version of the CommCell Console is installed locally on the computer in which the CommNet Browser is launched, then the CommCell Console will be launched as an application instead of as a remote web-based application. This option is supported on Macintosh.



# 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
<b>AGENT - RELATED FEATURE LICENSES</b>		
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
<b>COMMSERVE - RELATED FEATURE LICENSES</b>		
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
<b>MEDIA MANAGEMENT - RELATED FEATURE LICENSES</b>		
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
<b>CONTENT INDEXING AND SEARCH - RELATED FEATURE LICENSES</b>		
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
<b>ACTIVE DIRECTORY</b>		
Active Directory	<i>iDataAgent</i> for Active Directory	1 license per installed instance of the component
Active Directory Offline Mining Enabler	Offline Mining Enabler for Active Directory	1 license per installed instance of the component
<b>AIX</b>		
IBM AIX File System	<i>iDataAgent</i> for IBM AIX File System	1 license per installed instance of the component
<b>COMMNET</b>		
CommNet Server	CommNet Server	1 license per CommNet Server
CommNet Agent	CommNet Agent	1 license per CommServe
CommNet Advanced Reporting	CommNet Advanced Reporting	1 CELL Level license on Associated CommServe
<b>CONTENT STORE</b>		
Content Store	Content Store	1 license per installed instance of the component
<b>CONTINUOUSDATAREPLICATOR</b>		
ContinuousDataReplicator	ContinuousDataReplicator	1 license per installed instance of the component
ContinuousDataReplicator for Windows	ContinuousDataReplicator for MS Windows	1 license per installed instance of the component
ContinuousDataReplicator for Unix	ContinuousDataReplicator for Unix	1 license per installed instance of the component
<b>DATA PROTECTION MANAGER</b>		
Data Protection Manager	Data Protection Manager	1 license per installed instance of the component
Data Protection Manager for Windows	<i>iDataAgent</i> for MS Data Protection Manager	1 license per installed instance of the component
<b>DATAARCHIVER</b>		
Exchange Compliance Archiver	Data Archiver Compliance for MS Exchange	1 license per installed instance of the component
File Archiver for Windows	Data Archiver for Files - MS Windows	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"> <li>• More than one instance for Celerra can be created by consuming one license.</li> <li>• More than one instance for Network Share/FPolicy can be created by consuming one license.</li> </ul>
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
<b>DB2</b>		
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.
<b>DOCUMENTUM</b>		
Documentum	Documentum	1 license per installed instance of the component
<b>EXCHANGE</b>		
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
<b>EXTERNAL DATA CONNECTOR</b>		
External Data Connector	External Data Connector	1 license per installed instance of the component
<b>FREEBSD</b>		
Free BSD File System	iDataAgent for FreeBSD	1 license per installed instance of the component
<b>HP-UX</b>		
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



<b>IMAGE</b>		
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
<b>INFORMIX</b>		
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
<b>IRIX</b>		
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
<b>LINUX</b>		
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
<b>LOTUS NOTES</b>		
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
<b>MEDIAAGENT</b>		
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
<b>MACINTOSH</b>		
Macintosh File System	iDataAgent for Apple Macintosh File System	1 license per installed instance of the component
<b>MYSQL</b>		
MySQL on Unix	MySQL	1 license per installed instance of the component
<b>NAS</b>		
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.
<b>NETWARE</b>		
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
<b>NOVELL GROUPWISE</b>		
Novell GroupWise	iDataAgent for Novell GroupWise Database	1 license per installed instance of the component
<b>OES FILE SYSTEM</b>		
OES File System	iDataAgent for OES File System	1 license per installed instance of the component
<b>ORACLE</b>		
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	
<b>OSSV PLUG-IN</b>		
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.
<b>POSTGRESQL</b>		
PostgreSQL on Unix	Postgress	1 license per installed instance of the component
<b>PROXYHOST</b>		

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
<b>QUICK RECOVERY AGENT</b>		
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.		
<b>RECOVERY DIRECTOR</b>		
Recovery Director	iDataAgent for Recovery Directory	1 license per installed instance of the component
<b>SAP</b>		
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
<b>SERVERLESS DATA MANAGER</b>		
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
<b>SHAREPOINT</b>		
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
<b>SNAPSHOT</b>		
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
<b>SNMP ENABLER</b>		
CommCell SNMP Enabler	CommCell SNMP Enabler	1 license per enabler
<b>SOLARIS</b>		
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
<b>SRM (STORAGE RESOURCE MANAGER)</b>		
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
<b>SYBASE</b>		
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
<b>SQL</b>		
Microsoft SQL Server	iDataAgent for Microsoft SQL Server	1 license per installed instance of the component
<b>TRU64</b>		
TRU64 File System	iDataAgent for TRU64 File System	1 license per installed instance of the component
<b>WINDOWS</b>		
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.		
<b>WORKSTATION BACKUP AGENT</b>		
Workstation Backup Agent on Windows	Workstation Backup	1 license per installed instance of the component
<b>VIRTUAL SERVER</b>		
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"> <li>Data protection operations and auxiliary copy operations to Centera libraries will stop running.</li> <li>New Centera libraries cannot be</li> </ul>	Before the application of a permanent license: <ul style="list-style-type: none"> <li>Check if the number of Centera licenses available in the permanent license</li> </ul>

		<p>configured.</p> <p>The following will continue to work:</p> <ul style="list-style-type: none"> <li>• Data recovery operations from Centera libraries and storage policy copies created on media from Centera libraries.</li> <li>• Data Aging of data from Centera libraries.</li> <li>• Deconfiguration of Centera libraries.</li> </ul>	<p>is less than the number of evaluation Centera licenses in use.</p> <ul style="list-style-type: none"> <li>• If so, the number of Centera libraries that make up the difference must be deconfigured first.</li> </ul>
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"> <li>• New VaultTracker Policies cannot be created.</li> <li>• VaultTracker policies cannot run.</li> <li>• VaultTracker Policies can be deleted.</li> <li>• VaultTracker policy schedules cannot be created.</li> <li>• Scheduled Data Protection or Auxiliary Copy jobs that already have the Vault Tracker option enabled will continue to run, but Export jobs will fail.</li> <li>• The VaultTracker node and all VaultTracker policies will continue to be displayed in the CommCell Console.</li> <li>• Existing Vault Tracker schedules can be deleted.</li> <li>• Reports will continue to function.</li> </ul>	<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"> <li>• Data protection operations and auxiliary copy operations to disk libraries will stop working.</li> <li>• New disk libraries cannot be configured.</li> </ul> <p>The following will continue to work:</p> <ul style="list-style-type: none"> <li>• Data recovery operations from disk libraries and storage policy copies created on media from disk libraries.</li> <li>• Data Aging of data from disk libraries.</li> <li>• Deconfiguration of disk libraries.</li> </ul>	<p>Before the application of a permanent license:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• If so, the number of disk libraries that make up the difference must be deconfigured first.</li> </ul>
Data Encryption	The Data Encryption is not available in the CommCell Console at the client and subclient levels.	<ul style="list-style-type: none"> <li>• The Data Encryption option from the properties of a client computer or a subclient is still available.</li> <li>• Data Protection operations of encrypted data will not run. These operations will resume functioning once the Data Encryption option is disabled.</li> <li>• Schedules of data protection operations of encrypted data cannot be saved or the jobs of the schedule cannot be run immediately.</li> <li>• Data recovery operations of encrypted data can be performed.</li> </ul>	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"> <li>• The Data Multiplexing option on a storage policy copy is still available.</li> <li>• 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.</li> </ul>	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"> <li>• An operation that uses more than one data path cannot run.</li> <li>• Data recovery operations will still be able to run.</li> </ul>	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"> <li>• Data protection operations and auxiliary copy operations to libraries with the single instancing option enabled will stop running.</li> <li>• Libraries cannot be configured with the</li> </ul>	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"> <li>• Data recovery operations from libraries with the single instancing option enabled.</li> <li>• Data Aging of data from libraries with the single instancing option enabled.</li> <li>• Deconfiguration of libraries with the single instancing option enabled.</li> </ul>	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"> <li>• Data protection operations and auxiliary copy operations will fail.</li> <li>• Discovering these media types in the library or upon the configuration of a library will not work.</li> </ul> <p>The following will continue to work:</p> <ul style="list-style-type: none"> <li>• Data recovery operations from WORM/DVD/UDO media and storage policy copies created on WORM/DVD/UDO media.</li> <li>• Data Aging of data from WORM/DVD/UDO media.</li> </ul>	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"> <li>• Items may be selected to be erased, but the list cannot be submitted from the Browse Options dialog box.</li> <li>• The Media password will be unavailable but can be reset.</li> <li>• Erase Data jobs cannot run.</li> </ul>	The media password can be set by a user.
Proxy Stub Subclient	<ul style="list-style-type: none"> <li>• The Proxy Stub Subclient cannot be enabled.</li> <li>• The authentication credentials to access the filer for proxy stub recall capabilities cannot be configured.</li> </ul>	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"> <li>• The Client Computer Groups that were already created will continue to exist and function.</li> <li>• Client Computer Groups can be removed, but new groups cannot be created.</li> <li>• A client cannot be added or removed from a client computer group.</li> </ul>	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"> <li>• If the CommCell Readiness Report is created, the report includes the message:  License to run this report does not exist or has expired.</li> <li>• A schedule for the CommCell Readiness Report cannot be added.</li> </ul>	N/A
Single Sign On (SSO)	<ul style="list-style-type: none"> <li>• Active Directory Service Provider credentials can be configured.</li> <li>• External user groups cannot be mapped to those created in the CommServe.</li> <li>• The CommServe cannot be accessed with the Active Directory credentials.</li> </ul>	<ul style="list-style-type: none"> <li>• Active Directory Service Provider credentials can be configured.</li> <li>• External user groups cannot be mapped to those created in the CommServe.</li> <li>• The CommServe cannot be accessed with the Active Directory credentials.</li> <li>• Search or Content Indexing operations can be run.</li> </ul>	N/A
SnapProtect Backup	<ul style="list-style-type: none"> <li>• The option to create a snapshot copy for a storage policy is not available.</li> <li>• The option to enable SnapProtect Backup for a client is not available.</li> </ul>	<p>SnapProtect Backup will fail.</p> <p>The following will continue to work:</p> <ul style="list-style-type: none"> <li>• Data recovery operations from existing snapshots.</li> </ul>	N/A
<b>ADVANCED FILE SYSTEM /DATAAGENT FEATURES</b>			
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
<b>ADVANCED COPY FEATURES</b>			
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.
<b>ADVANCED MEDIA MANAGEMENT FEATURES</b>			
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).
<b>CONTENT INDEXING AND SEARCH</b>			
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. • 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](#)

# Clustering

Topics | Windows Cluster | Unix Cluster | NetWare Cluster | Troubleshoot | Support

Overview

Terminology

Supported Cluster Configurations

Adding or Removing Cluster Nodes

Important Considerations

- Network TCP Ports
- Multi Instancing

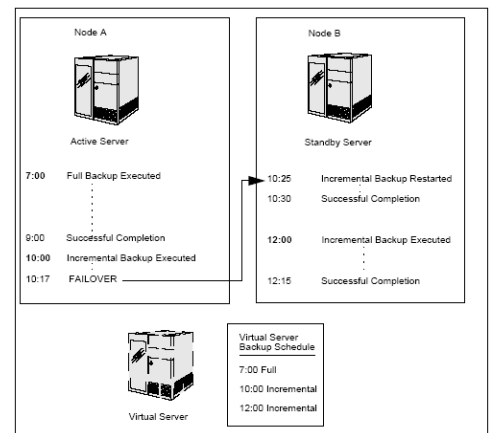
## OVERVIEW

A collection of multiple server computers into a single unified cluster provides an added measures of performance, reliability, and fault tolerance. The CommServe, MediaAgent, and supported Agents take advantage of the failover protection afforded in the clustering environment. If an active node fails, the software will still be able to function from the node that has not failed, and will continue to be able to perform data protection and recovery operations.

You can create schedules for data protection operation on cluster servers in the same way as you create data protection operation schedules for data on a physical node.

All schedules are saved on the CommServe. When a job is scheduled in a cluster server, the CommServe executes that job on the active server. If the active server fails while jobs are in progress, a failover will occur, and running jobs are temporarily placed in a pending state. Once the failover completes, the new active server will restart the jobs. In addition, remaining scheduled jobs are implemented on this new active node. This is shown in the illustration; the cluster server is associated with *Node A* and *Node B*. Since *Node A* is the active node (and therefore has access to the shared disk), scheduled jobs for the virtual server are executed on *Node A*. When *Node A* fails, after the failover, a new data protection operation is started on *Node B* which is now the active node. In addition, the remaining scheduled jobs are executed on *Node B*.

Regardless of the hosting node, the software can perform operations for a virtual server, including data protection and recovery operations, as long as the software has access to the network and to the virtual server's network name and Internet Protocol (IP) address.



## TERMINOLOGY

When referring to the physical servers that comprise a cluster group, individual computers are referred to as nodes. The physical server may be called one of the following depending upon the context in which it is being discussed: "physical computer," "physical node," "Client computer". Also, the "physical server" may be an "active node" or a "standby (passive) node" depending on its role within the cluster environment at a given point in time.

"Cluster Server" or "Virtual Node" refers to the hardware and software components (Cluster Resource Group) within the cluster that are managed by Cluster Service as a single, logical unit. The virtual server is actually not a physical computer but a logical construct within the system. However, like the physical servers, the virtual server has an Internet Protocol (IP) address and a network name. As such, the virtual server secures its own license on the CommServe, and it has its own registry information. This registry information is included on all physical nodes in the cluster. Once the proper installations are made to the physical nodes, the virtual server can be configured on each node to function within the clustering environment.

"Cluster Service" refers to the collection of components on each node that perform cluster-specific activity, managing the Cluster Resource Group.

The "Shared Disk" resource is connected to each physical computer. This disk resource is designed to include shared data for CommCell operations (e.g., data protection and recovery operations). Information that is relevant only to each physical server should be included only on the physical server's local disk and not on the shared disk.

## SUPPORTED CLUSTER CONFIGURATIONS

Both Active/Passive, and Active/Active cluster configurations are supported.

## ADDING OR REMOVING CLUSTER NODES

After a computer has been added to a cluster as a new node, and has been verified to be functional, you can install CommServe, MediaAgent or Agent software on it. MediaAgent or Agent software can also be installed as non-cluster-aware (a "physical" installation.) Normal installation procedures can be used for this.

Before removing a node from a cluster, the CommServe, MediaAgent or Agent software can be uninstalled and/or Deconfigured, if it is not running any jobs, and if it is not the current active node. The normal uninstall and deconfiguration procedures can be used for this. For more information and procedures, see Uninstalling Components.

---

## **IMPORTANT CONSIDERATIONS**

---

### **NETWORK TCP PORTS**

Every physical node in a cluster which is configured to host a given cluster server, must have the same TCP port numbers configured for that cluster server. For more information, see Network TCP Port Requirements - Clusters.

---

### **MULTI INSTANCING**

Multi Instancing is supported for clusters, with some restrictions. For more information, see Multi Instancing.

---

[Back to Top](#)

# CommNet Alerts and Monitoring

Topics | How To | Troubleshoot

---

Overview

SNMP Traps

Available Alerts and Entity Association

Alert Tasks

Important Considerations

---

## OVERVIEW

Alerts can inform you of conditions occurring within the CommNet domain 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. Alerts are sent to a pre-determined set of users, and/or escalated to a different set of users (in the case of a severe condition).

Alerts are based on conditions which have occurred within the entity associated with the alert. This entity can be a CommNet Server, CommCell, client, agent, MediaAgent, or library. These entities, by default, are monitored at 20-minute intervals. If they meet the defined alert conditions, the alert (if configured) will be generated at this time.

You will be notified of the alert condition:

- Once conditions within the entity have met pre-determined threshold criteria.
  - Either:
    - When the condition is detected or after the condition has persisted for a certain length of time. The alert update time frame can be selected from the Cell Data Collection Policy dialog box.
    - You can also be notified repeatedly, and also after the condition clears.
  - By any combination of the following pre-determined notification methods:
    - By E-mail
    - By pager
    - By SNMP traps if the SNMP Enabler is installed on the CommNet Server
    - From a Windows System Event Viewer on the CommNet Server
    - The execution of a command script
- 

## SNMP TRAPS

An SNMP Trap is used for alert notifications sent by the CommNet Server 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 the CommNet Server generates an alert. SNMP traps are sent in the Management Information Protocol (MIB) format.

A CommNet Server computer can send alerts via SNMP traps to multiple computers. These computers can receive these alerts even if they do not have the software installed. These alerts are sent only if the CommNet Server SNMP Enabler has been installed on the CommNet Server and alerts have been configured to be sent via SNMP traps.

In order for an alert to be sent as an SNMP trap:

- Ensure that SNMP services are started on the CommNet Server computer.
- Install the CommNet Server SNMP Enabler software on the CommNet Server computer. For information on how to install the SNMP Enabler software, see [Install the CommNet Server SNMP Enabler](#).
- Check that the computers that are to receive the SNMP Traps are set up with the appropriate trap receiver software.
- Ensure that the CommNet Server computer that sends the trap and the remote computer that receives the trap are accessible.
- You can add additional computers to receive SNMP Traps. For information on how to add additional computers to receive SNMP Traps, see [Install the CommNet Server SNMP Enabler](#).
- Configure alerts to be sent as SNMP Traps from the Notification Method(s) Selection tab of the **Alert Wizard** dialog box. For a list of the alerts that can be sent as SNMP traps, see [Available Alerts and Entity Association](#).

---

## SAMPLE SNMP TRAP MESSAGE

All SNMP traps are sent in the Management Information Base (MIB) format. When the CommNet Server SNMP Enabler is installed, the MIB file is automatically installed on the CommNet Server computer and is located at `\<Software Installation Directory>\Mib\Simpana.mib`.

**EXAMPLE****Part 1:**

Agent Address: 172.19.61.216

OID Prefix: 1.3.6.1.4.1.14604.2.2

Time Stamp: 26126615

Generic: 6

Specific: 5013

**Part 2:**

OID: 1.3.6.1.4.1.14604.2.2.4.1.0

**SNMP TRAP COMPONENTS****PART 1**

The following table describes Part 1 of the example of the SNMP trap message:

Field	MIB Definition
Agent Address 172.19.61.216	Address of the computer generating the trap
OID Prefix: <u>1.3.6.1.4.1.14604.2.2</u>	The first part of the OID Prefix 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 OID Prefix, <u>2.2</u> , indicates products and the software, respectively.
Time Stamp: 26126615	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: 5013	The specific trap type. Each alert type will be sent using a unique identification number. The alert type (e.g., CommCells Unreachable, CommNet Database Disk Allocation, etc.) can be identified in the content of the trap message.

**PART 2**

The example that follows describes the `OID` field as identified as Part 2 of the SNMP trap message:

1.3.6.1.4.1.14604.2.2.4.1.0

The third to last number, number 4, represents the software product.

The second to last number of the OID identifies the object type. The following table lists the object types and their corresponding MIB definitions:

Object Type	MIB Definition
1	Display name
2	Date and time of the alert detection
3	Creator of the alert
4	Alert type
5	Alert status
6	Alert actual threshold

**LIST OF TRAP MESSAGES**

The following table provides a list of Trap Messages generated by the SNMP Enabler.

Alert Number	OID	Notes (Feature generating the Alert)
5001	.1.3.6.1.4.1.14604.2.2.4.0.5001	Drives Offline
5002	.1.3.6.1.4.1.14604.2.2.4.0.5002	Libraries Offline
5003	.1.3.6.1.4.1.14604.2.2.4.0.5003	MediaAgents Offline
5004	.1.3.6.1.4.1.14604.2.2.4.0.5004	Job Failures over time
5005	.1.3.6.1.4.1.14604.2.2.4.0.5005	Clients not protected over time
5006	.1.3.6.1.4.1.14604.2.2.4.0.5006	Subclients not protected over time
5008	.1.3.6.1.4.1.14604.2.2.4.0.5008	CommNet database space check
5009	.1.3.6.1.4.1.14604.2.2.4.0.5009	CommCells Unreachable
5010	.1.3.6.1.4.1.14604.2.2.4.0.5010	Consecutive Job Failures



5011	.1.3.6.1.4.1.14604.2.2.4.0.5011	Cells Not Synchronized
5012	.1.3.6.1.4.1.14604.2.2.4.0.5012	CommNet database backup check

## AVAILABLE ALERTS AND ENTITY ASSOCIATION

The following table includes the available alerts, their associated entities and criteria description. The alerts available are grouped into three categories:

- Administrative
- Job Management
- Media Management

### ADMINISTRATIVE

Alert Type	Entity	Criteria	Description
<b>CommCells Unreachable</b>	CommNet Server, CommCell	Criteria can only be percentage or value based.	Value of $n$ can be a whole number or a percentage.
		Detect when $n$ or more CommCells are unreachable.	The CommNet Server software detects that the specified number or percentage of selected CommCells are not reachable.
<b>CommNet Database Disk Allocation</b>	CommNet Server	Criteria can only be value based.	Value of $n$ can only be a whole number.
		Detect when $n$ MB of disk is used by the CommNet database.	The CommNet Server software detects that the specified amount of disk space is being used by the CommNet database.
<b>CommNet Database Backup Failure</b>	CommNet Server	Criteria can only be value based.	Value of $n$ can only be a whole number.
		Detect when $n$ days since last successful CommNet database backup.	The CommNet Server software detects that the specified number of days have passed since the last successful CommNet database backup.
<b>Cell Synchronization Failure Over Time</b>	CommNet Server, CommCell	Criteria can only be value based. Detect when $n$ or more cells have synchronization failure during the last $n$ days.	Value of $n$ can only be a whole number. The CommNet Server software detects that the specified number of cells has had a synchronization failure during the last specified number of days.

### JOB MANAGEMENT

Alert Type	Entity	Criteria	Description
<b>Clients Not Protected Over Time</b>	CommNet Server, CommCell, Client	Criteria can be percentage or value based.	Value of $n$ can be a whole number or a percentage.
		Detect when $n$ or more clients have not been protected during the last $n$ days.	The CommNet Server software detects that the specified number of clients' data has not been backed up during the last specified number of days.
		Include Entities Without Schedules	Include those entities that have no scheduled jobs.
<b>Consecutive Job Failures</b>	<b>Client Based Entity:</b> CommNet Server, CommCell, Client <b>Storage Policy Based Entity:</b> CommNet Server, CommCell, Storage Policies	Criteria can only be value based.	Value of $n$ can only be a whole number.
		Detect when $n$ or more jobs have failed consecutively during the last $n$ days.	The CommNet Server software detects that the specified number of jobs have failed consecutively during the last specified number of days.
<b>Job Failures Over Time</b>	CommNet Server, CommCell, Client, Cell-Client Group	Criteria can be percentage or value based.	Value of $n$ can be a whole number or a percentage.
		Detect when $n$ or more jobs have failed during the last $n$ hours.	The CommNet Server software detects that the number of specified jobs have failed during the last specified number of hours.
<b>Subclients Not Protected Over Time</b>	CommNet Server, CommCell, Client, Cell-Client Group	Criteria can be percentage or value based.	Value of $n$ can be a whole number or a percentage.
		Detect when $n$ or more subclients have not been protected during the last $n$ days.	The CommNet Server software detects that the specified number of subclients' data has not been backed up during the last specified number of days.
		Include Entities Without Schedules	Include those entities that have no scheduled jobs.
		Exclude Command Line Subclients	Exclude those subclients created via command line.

### MEDIA MANAGEMENT

Alert Type	Entity	Criteria	Description
<b>Drives Offline*</b>	CommNet Server, CommCell, Library	Criteria can be percentage or value based.	Value of $n$ can be a whole number or a percentage.
		Detect when $n$ or more drives are offline.	The CommNet Server software detects that the specified number of drives are offline.
<b>Libraries Offline</b>	CommNet Server, CommCell, Library	Criteria can be percentage or value based.	Value of $n$ can be a whole number or a percentage.
		Detect when $n$ or more libraries are offline.	The CommNet Server software detects that the specified number of libraries are offline.
<b>MediaAgents Offline</b>	CommNet Server, CommCell, MediaAgent	Criteria can be percentage or value based.	Value of $n$ can be a whole number or a percentage.
		Detect when $n$ or more MediaAgents are offline.	The CommNet Server software detects that the specified number of MediaAgents are offline.

\*The Drives Offline alert only supports the physical drive level.

---

## ALERT TASKS

For the Alerts node, tasks are available from the **All Alerts Tasks** or **My Alerts Tasks** section of the CommNet Browser. These tasks allow you to display information regarding important aspects of the alerts that are configured within the CommNet domain.

The following is a list of alert tasks:

- All Alerts
  - My Alerts
- 

## IMPORTANT CONSIDERATIONS

The user account used to access the CommNet Browser when you created the alert is the owner of the alert. Only the owner, or a user who is associated with all of the objects associated with the alert, can modify it. Therefore, if the user account is deleted, ownership of the alert should be transferred to another user to enable it to be modified, if necessary. You can transfer ownership of an alert upon deletion of the owner's user account. For more information, see [Delete a User](#).

---

[Back to Top](#)

# CommNet Alerts and Monitoring - How To

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

---

[Configure an Alert](#)

[Remove an Alert](#)

[Modify an Alert](#)

[Define the Mail Server](#)

[Define the Sender's Address](#)

[Define the Port for the SMTP Server](#)

---

## CONFIGURE AN ALERT

*Required Capability:* See [Capabilities and Permitted Actions](#)

▶ To configure an alert:

1. Define a Mail Server, Sender's Address, and SMTP Port in the **Configuration** tab of the CommNet Properties dialog box.
2. From the CommNet tree, right-click the **Alerts** node, click either **All Alerts** or **My Alerts**, and then click **Add** from the All Alerts or My Alerts window.
3. In the General Information dialog box:
  - Enter the display name of the alert
  - Select the alert category and type.
  - Click **Next**.
4. In the Entities Selection dialog box, select the entities that will be associated with this alert. Click **Next**.
5. In the Threshold and Notification Criteria Selection dialog box, select the following options:
  - If the regular or escalated alert should be generated after a selected percentage or value has exceeded within the entity.
  - If the regular or escalated alert should be sent to the recipients immediately or after the condition persists for a certain length of time, if the alert should be repeated, and if the alert should be sent after the condition has cleared.
  - Click **Next**.
6. In the Notification Method(s) Selection dialog box, use the **E-mail**, **Pager**, **SNMP**, **Event Viewer**, and/or **Run Command** tabs to select the type of notification method. Click **Next**.
7. In the User(s) and User Group(s) Selection dialog box, select the users and/or user groups who will receive the alert. Click **Next**.
8. The Summary screen lists the options you selected to configure the alert.
9. Click **Finish**.

- If the Mail Server, Sender's address, and SMTP port are not configured properly, alerts will not be sent to the e-mail and pager recipients.
  - An alert can be configured to send e-mail notifications to external domain users.
- 

## REMOVE AN ALERT

*Required Capability:* See Capabilities and Permitted Actions

▶ To remove an alert:

1. From the CommNet tree, right-click the **Alerts** node, click either **All Alerts** or **My Alerts**, select an alert from the All Alerts or My Alerts window, then click **Remove**.
  2. Click **Yes** from the confirmation window.
- 

## MODIFY AN ALERT

*Required Capability:* See Capabilities and Permitted Actions

▶ To modify an alert:

1. From the CommNet tree, right-click the **Alerts** node, click either **All Alerts** or **My Alerts**, select an alert from the All Alerts or My Alerts window, then click **Modify**.
  2. Follow the steps from the **Modify Alert Wizard**.
  3. Click **Finish** from the **Summary** window.
- 

## DEFINE THE MAIL SERVER

*Required Capability:* See Capabilities and Permitted Actions

▶ To define the Mail Server that is used to send alerts and scheduled tasks:

1. From the CommNet tree, right-click the CommNet Server node, and then click **Properties**.
2. From the CommNet Properties dialog box, enter the new mail server in the **Mail Server** box.
3. Click **OK**.

If the Mail Server is not configured properly, alerts and scheduled tasks will not be sent to their intended recipients. If these are not sent properly, this information will be collected in the CommNet Server database and will not be sent until the Mail Server is configured properly. After this information has been accumulated for 24 hours, the CommNet Server will start pruning this information.

---

## DEFINE THE SENDER'S ADDRESS

*Required Capability:* See Capabilities and Permitted Actions

▶ To define the Sender's Address of all mail messages sent from the CommNet Server:

1. From the CommNet tree, right-click the CommNet Server node, and then click **Properties**.
2. From the CommNet Properties dialog box, enter the new sender's address in the **Sender's Address** box.
3. Click **OK**.

If the Sender's Address is not configured properly, alerts and scheduled tasks will not be sent to their intended recipients. If these are not sent properly, this information will be collected in the CommNet Server database and will not be sent until the Sender's Address is configured properly. After this information has been accumulated for 24 hours, the CommNet Server will start pruning this information.

---

## DEFINE THE PORT FOR THE SMTP SERVER

*Required Capability:* See Capabilities and Permitted Actions

▶ To define the port at which the alert subsystem connects to the SMTP server:

1. From the CommNet tree, right-click the CommNet Server node, and then click **Properties**.

2. From the CommNet Properties dialog box, select an SMTP port from the **SMTP Port** box.
3. Click **OK**.

If the SMTP Port is not configured properly, alerts and scheduled tasks will not be sent to their intended recipients. If these are not sent properly, this information will be collected in the CommNet Server database and will not be sent until the SMTP Port is configured properly. After this information has been accumulated for 24 hours, the CommNet Server will start pruning this information.

---

[Back to Top](#)

# CommNet Cost Analysis

[CommNet](#) | [CommCell](#) | [How To](#) | [Example](#) | [Troubleshoot](#) | [Related Topics](#)

---

Overview

Cost Categories

- Primary Storage Resource
- Secondary Storage Resource

Billable Entities

Billing Reports

Billing Configuration Tasks

Important Considerations

---

## OVERVIEW

The software provides a flexible costing model to calculate the cost of both the primary and secondary storage based on the types of storage media used. In addition the storage costs can be distributed to billable entities, such as departments within a company. The costing model can be defined centrally and is automatically distributed to all CommCells within the CommNet domain. The costing model consists of defining the cost categories and billable entities. These are explained in the following sections.

---

## COST CATEGORIES

The estimated per megabyte cost to store and protect data on a type of storage entity can be defined in a cost category. Cost categories can be associated with the following storage entities:

---

### PRIMARY STORAGE RESOURCE

Cost categories defined for primary storage can be associated with actual primary storage resources in the CommCell Console for SRM entities, once a CommCell is registered with the CommNet Server. Primary storage resources include:

- Disks
- Unix logical volumes
- NAS volumes
- SharePoint databases
- NetWare pools

---

### SECONDARY STORAGE RESOURCE

Data protection operations that create protected copies of primary storage data are managed from the CommCell Console. Cost categories can be assigned to these storage resources in the CommNet Server and then can be viewed from a CommCell Console, once that CommCell is registered with the CommNet Server. Secondary storage resources include:

- Tape, optical, and disk media
- Quick Recovery scratch volume pools

Note that if you do not have an elaborate model for defining cost categories and billable entities in your organization, you can also generate the Billing Charge Back Report using a fixed costing. See **Fixed Costing** section in Billing Charge Back Report for more information.

---

## BILLABLE ENTITIES

A billable entity can be associated with the following objects, wherever applicable:

- Clients
- Agents
- Databases
- Backup Sets

- Instances
  - Subclients (for SRM Agents, only subclients can be associated with Billable Entities)
- 

## BILLING REPORTS

After defining the Cost Categories and Billable Entities, you must associate the appropriate primary and secondary storage entities in the CommCells. You must also Synchronize Cells before generating the reports. See Cost Analysis - Example for more information.

The following reports can be generated:

- The Billing Charge Back Report provides you with the costs of your primary and secondary storage, from fixed based costing methods or category costing methods, for a particular client computer or for all objects that are included in a billing entity.
  - The Billing Association Report provides you with the information of the association of your cost categories and billable entities of the CommNet domain.
  - The Billing Detail Report provides, for a particular cell or client, a detailed view of the charges. Can be derived by clicking on the Number of Data Protection operations, total price, Data size, or the Price for data protection or price for storage.
- 

## BILLING CONFIGURATION TASKS

For the Billing Configuration node, tasks are available from the **Cost Categories Tasks** and **Billable Entities Tasks** section of the CommNet Browser. These tasks allow you to view information regarding important aspects of the cost categories and billing entities that are configured within the CommNet domain.

The following is a list of Billing Configuration tasks:

Cost Categories

Billable Entities

---

## IMPORTANT CONSIDERATIONS

When the following configurations are modified, the changes are immediately pushed to the active CommCell(s); cell synchronization is not required to propagate this information to the cells.

- Global Filters
- Billable Entities
- Cost Categories
- Data Collection Policy
- Comments (Note that Comments made using the CommCell Console are pushed to the CommNet Server only during cell synchronization. For more information, see Comments.)

This information will be pushed accordingly when services (CommNet Server or Bull Calypso Server Event Manager) are restarted as well.

---

[Back to Top](#)

# CommNet Cost Analysis - How To

[CommNet](#) | [CommCell](#) | [How To](#) | [Example](#) | [Troubleshoot](#) | [Related Topics](#)

---

[Add a Cost Category](#)

[Modify a Cost Category](#)

[Remove a Cost Category](#)

[Add a Billable Entity](#)

[Modify a Billable Entity](#)

[Remove a Billable Entity](#)

[Assign a Billable Entity to a CommCell Object](#)

[Set up the Unit Price For Secondary/Primary Storage](#)

---

## ADD A COST CATEGORY

*Required Capability:* See Capabilities and Permitted Actions

▶ To add a cost category:

1. From the CommNet tree, from the **Billing Configuration ->Cost Categories** node, click **Add** from the **Cost Categories** window.
  2. From the Cost Category dialog box:
    - type a name of the cost category
    - select cost per MB for this category
    - type a description
    - select the media that will be assigned with this cost category.
  3. Click **OK**.
    - You can create a cost category without the association of any drives.
    - If you select, for example, a drive type of SDLT to be assigned to this cost category, all of the CommCells that are registered with the CommNet Server will automatically assign this cost category to each drive pool containing SDLT drives.
    - You cannot associate a disk library, QR Scratch Volume, or a primary storage entity to a cost category from the CommNet Server. This must be done manually from the appropriate Console (explicit association).
- 

## MODIFY A COST CATEGORY

*Required Capability:* See Capabilities and Permitted Actions

▶ To modify a cost category:

1. From the CommNet tree, right-click the **Billing Configuration** node, click **Cost Categories**, and then select a cost category and click **Modify** from the **Cost Categories** window.
  2. From the Cost Category dialog box, modify the options, as necessary.
  3. Click **OK**.
- 

## REMOVE A COST CATEGORY

*Required Capability:* See Capabilities and Permitted Actions

▶ To remove a cost category:

From the CommNet tree, right-click the **Billing Configuration** node, click **Cost Categories**, and from the **Cost Categories** window, select the cost category and click **Remove**.

Once a cost category is deleted, information from operations that were performed using this cost category will still be used in billing and costing calculations.

---

## ADD A BILLABLE ENTITY

*Required Capability:* See Capabilities and Permitted Actions

▶ To add a billable entity:

1. From the CommNet tree, from the **Billing Configuration -> Billable Entities** node, click **Add** from the **Billable Entities** window.
  2. From the Billable Entity dialog box, enter the:
    - name of the billable entity
    - a description
    - any relevant contact information.
  3. Click **OK**.
- 

## MODIFY A BILLABLE ENTITY

*Required Capability:* See Capabilities and Permitted Actions

▶ To modify a billable entity:

1. From the CommNet tree, right-click the **Billing Configuration** node, click **Billable Entities**, select a billable entity and click **Modify** from the **Billable Entities** window.
  2. From the Billable Entity dialog box, modify the options, as necessary.
  3. Click **OK**.
- 

## REMOVE A BILLABLE ENTITY

*Required Capability:* See Capabilities and Permitted Actions

▶ To remove a billable entity:

From the CommNet tree, right-click the **Billing Configuration** node, click **Billable Entities**, and from the **Billable Entities** window select the billable entity and click **Remove**.

---

## ASSIGN BILLABLE ENTITY TO A COMMCELL OBJECT

Billable Entity can be assigned to CommCell objects only when the CommCell is registered with the CommNet Server.

*Required Capability:* See Capabilities and Permitted Actions

▶ To assign billable entity to a CommCell object:

1. Select **Control Panel** from the **CommCell Console** and click Billing Configuration.
  2. Select a CommCell object, then select a billing department (as defined in the CommNet Browser) and click **Apply**.
  3. Click **OK**.
- 

## SET UP THE UNIT PRICE FOR SECONDARY/PRIMARY STORAGE

*Required Capability:* See Capabilities and Permitted Actions

▶ To set up the unit price for the secondary storage/primary storage Fixed Costing option in the Billing Charge Back Report:

1. On the **Setup** menu, click **Cell Configuration**.
  2. From the Cell Configuration (General) dialog box, type the price in the **Price per Data Protection** and **Price per MB of Data** boxes.
  3. Click **OK**.
- 

[Back to Top](#)



# Dashboard

Topics | How To

---

## Overview

- Last 7 Days Job Success
  - Last 7 Days DP Coverage
  - Last 7 Days Data Growth - Combined
- 

## OVERVIEW

The Dashboard displays a pictorial view of a CommNet entity's, the CommNet domain's or a CommCell's, last seven days. It contains the details of successful jobs, data protection coverage and data growth for the CommNet entity specified by the user. This is extremely useful for those needing to quickly obtain the status of their CommNet domain environment and for troubleshooting. The dashboard can display up to six (6) reports at one time. By default, it displays the following reports:

---

### LAST 7 DAYS JOB SUCCESS

This bar graph depicts the data protection job success rate for the last seven days, according to the CommCell Browser's local time. It displays the total number of data protection jobs executed during this time, as well as those that have completed, were killed and failed. If viewing the last seven days of a CommCell rather than the entire CommNet domain, you can click on the graph to see a detailed report of the data protection jobs within this time period.

---

### LAST 7 DAYS DP COVERAGE

This bar graph depicts the data protection coverage per subclient for the last seven days, according to the CommCell Browser's local time. It displays the total number of subclients with data protection coverage as well as those with no activity, or with coverage that failed or was killed. If viewing the last seven days of a CommCell rather than the entire CommNet domain, you can click on the graph to see a detailed report of the data protection jobs per subclient within this time period.

---

### LAST 7 DAYS DATA GROWTH - COMBINED

This bar graph depicts the data growth for both incremental and full data protection jobs for the last seven days, according to the CommCell Browser's local time. It displays the total growth for both incremental and full data protection jobs per day in GB. If viewing the last seven days of a CommCell rather than the entire CommNet domain, you can click on the graph to see a detailed report of the data growth within this time period.

Other reports available for display in the Dashboard are:

- Last 7 Days Data Growth - Incremental
- Last 7 Days Data Growth - Full
- Last 7 Days DP Activity - Data Size
- Last 7 Days DP Activity - Job Detail

To customize the Dashboard view, refer to [Customize the CommNet Dashboard](#).

---

## Dashboard - How To

Topics | How To

---

### CUSTOMIZE THE COMMNET DASHBOARD

*Required Capability:* See [Capabilities and Permitted Actions](#)

▶ To customize the CommNet Dashboard:

1. From the **Settings** menu, click **Browser Options**. The Browser Options dialog box is displayed.
2. Select the **Customize Dashboard** tab.
3. Arrange the available reports to display in the dashboard by dragging each report into the appropriate space or right-click on a report space to **Add** and/or

**Change** a report from the popup menu. Available reports include:

- Last 7 Days Data Growth - Combined
- Last 7 Days Data Growth - Incremental
- Last 7 Days Data Growth - Full
- Last 7 Days DP Activity - Data Size
- Last 7 Days DP Activity - Job Detail
- Last 7 Days DP Coverage
- Last 7 Days Job Success

4. Right-click on a space to remove a report from the dashboard.
  5. If desired, select options to include chart options or a chart table.
  6. Click **OK**.
-

# CommNet Scheduling

Topics | How To | Tasks | Troubleshoot

---

## OVERVIEW

Scheduling ensures that you can run tasks such as reports and summaries on a consistent basis. You can use the scheduling feature to send this critical organizational information to multiple users at multiple times and intervals, in the format that works best for you.

CommNet Scheduling also allows you to:

- Save the scheduled task to a specified folder and be sent as an e-mail to users and user groups.
- Run a particular schedule immediately.
- View the history of schedules with the status of each attempt performed along with the corresponding failure reason, if needed.
- View the schedules that were created by you, along with the number of schedules that you will receive.
- Determine if a schedule is enabled or disabled.
- Disable the scheduler activity for a particular schedule or the entire scheduler.
- Filter schedules on a particular report type or summary window.
- Generate files in either PDF or TSV (Tab Separated Values) format.

In order for scheduled tasks to run, you must have the following minimum requirements:

- A CommNet Browser installed on a CommNet Server
- A valid e-mail server and a senders e-mail address for the CommNet Server
- The correct user Capabilities and Permitted Actions.
- A Windows Scheduled Task Service that is up and running. Note the following:
  - All CommNet scheduled tasks are displayed in the **Windows Scheduled Tasks** dialog box.
  - All tasks in the Windows Scheduled Task window are the same as the CommNet scheduled tasks in the CommNet Browser. An update runs when the Windows Scheduled Tasks service is started, and once every hour after that.
  - All CommNet scheduled tasks are deleted from the Windows Scheduled Tasks service if the CommNet Server software is uninstalled.
  - Do not modify a scheduled task from the Windows Task Scheduler.

If a scheduled task is modified from the Windows Task Scheduler, the software will not get updated with the new start time. The scheduled task will start at the time specified in the Windows Task Scheduler and will be ignored at the time it is scheduled to start in the CommNet Browser. It is recommended all scheduled tasks be modified from CommNet Browser.

---

## CommNet Scheduling - How To

Topics | How To | Tasks | Troubleshoot

---

Create a Schedule

Remove a Schedule

Modify a Schedule

Enable or Disable All Scheduled Tasks


Run a Scheduled Task On Demand

---

## CREATE A SCHEDULE

*Required Capability:* See Capabilities and Permitted Actions

▶ To create a schedule:

1. From the CommNet tree, click the appropriate CommNet Summary, CommCell Summary, Client Summary, or report, and then click **Schedule** or the  icon.
2. In the Task dialog box:
  - Type the name of the schedule and enter a description.

- Enable or disable the schedule.
  - Review the task summary information. If the task is a report schedule and it needs to be modified, click **Modify Task**, and then modify the options, as necessary.
  - Click **Next**.
3. In the Schedule Pattern dialog box:
    - Select the time zone, interval, and start date and start time of the schedule.
    - Determine if the schedule should be repeated and at which interval(s).
    - Click **Next**.
  4. In the Output dialog box:
    - Select the file format.
    - Determine if the task is to be saved to a file.
    - Determine if the task should be sent as an email attachment to a user or user group. If the task is to be sent as an email attachment, make sure that a valid Mail Server, Sender's Address, and SMTP port number is specified on the CommNet Properties dialog box.
  5. Click **Finish**. The schedule is now created.
    - A disabled schedule will not run at the scheduled time and will only run when the schedule is enabled again.
    - Once a schedule is created, it is also displayed in the **Windows Scheduled Tasks** dialog box.
    - If you are creating a report schedule, make sure that the CommNet Browser is installed on the same computer as the CommNet Server.
    - A scheduled report can be configured to be sent to external domain users.
- 

## REMOVE A SCHEDULE

*Required Capability:* See Capabilities and Permitted Actions

▶ To remove a schedule:

1. From the CommNet tree, right-click the **Schedules** node, click either **All Schedules** or **My Schedules**, select a schedule from the All Schedules or My Schedules window, and then click **Remove**.
  2. Click **Yes** from the confirmation window. The schedule is now removed.
- 

## MODIFY A SCHEDULE

*Required Capability:* See Capabilities and Permitted Actions

▶ To modify a schedule:

1. From the CommNet tree, right-click the **Schedules** node, click either **All Schedules** or **My Schedules**, select a schedule from the All Schedules or My Schedules window, and then click **Modify**.
  2. Follow the prompts from the **Modify Schedule Wizard**.
  3. Click **Finish**. The schedule is now modified.
- 

## ENABLE OR DISABLE ALL SCHEDULED TASKS

*Required Capability:* See Capabilities and Permitted Actions

▶ To enable or disable all schedule tasks:

From the CommNet tree, right-click the **Schedules** node, click **All Schedules**, and from the All Schedules window select the **Scheduler Activity Enabled** or the **Scheduler Activity Disabled** field. All scheduled tasks within the CommNet domain are now enabled or disabled.

If the **Scheduler Activity** is disabled, scheduled tasks can still be run immediately.

---

## RUN A SCHEDULED TASK ON DEMAND

*Required Capability:* See Capabilities and Permitted Actions

▶ To run a schedule tasks immediately:

From the CommNet tree, right-click the **Schedules** node, click either **All Schedules** or **My Schedules**, select a schedule from the All Schedules or My Schedules window, and then click **Run Now**. The scheduled task is run.

A scheduled task can be run immediately even if the **Scheduler Activity** has been disabled.

---

[Back to Top](#)

# CommNet Reports

[Topics](#) | [Troubleshoot](#) | [How Do I](#) | [Related Topics](#)

---

Overview

Report Features

- Uninstalled and Deleted Objects
- Considerations

Report Tasks

Available Reports

- Billing Reports
- Data Protection Reports
- Data Recovery Reports
- Media Management Reports
- Primary Storage Reports
- Other Reports

Filters

- Time Range Selection Filter - Weekends
- Client Status Selection Filter
- Exclude Command Line Subclients

Data Availability Timelines

License Requirement

---

## OVERVIEW

Reports allow you to view and analyze data related to various aspects of different entities like CommCells, Clients, MediaAgents and libraries in the CommNet domain.

Information is presented in a logically grouped, tabular format, with the ability to also plot the information as a bar chart or pie chart wherever possible. On all reports and summaries, and in addition to selected pie or bar charts, the exact chart details display in a data table.

When you select a given report, various filters will be available to select the entities and options to be included when the report is generated. If a report will contain tables, you can pre-select which columns will be displayed, as well as their order.

Once you generate a report, information is displayed in the bottom pane of the same report window, and wherever possible you are provided with a list of chart options to create different types of charts from the data displayed in the report.

There is a range of functionality available in the CommNet Browser related to Reports; see CommNet Browser.

---

## REPORT FEATURES

When viewing a report in the CommNet Browser, you can:

- Generate for multiple CommCells; however, information for each CommCell is presented in its own section for easy readability.
- CommNet reports are automatically generated for Data Growth, Data Protection Job Success, SLA and Media Prediction, which provide a concise view of the relevant data for all the selected CommCells.
- Print, Save as a PDF or an MHTML (.mht) file, or Export in Microsoft Excel format by clicking the appropriate icon at the top of the report window.
- To print the details of all CommCells, open the details for view in the CommNet Browser. Alternatively, to selectively print the details for a few of the CommCells, make sure to open only the CommCells that are required for printing.
- Schedule a report or summary by clicking the Schedule icon at the top of the report window.
- Copy any chart in BMP format to the clipboard by right-clicking the chart and selecting **Copy Chart**. This allows you to easily copy a chart into other applications. Note that the Copy Charts function is not compatible with Microsoft WordPad.
- Re-generate with different filtering by expanding the top pane of the report window and selecting the new filtering options (this can be done with a **Data Protection Detail Report** also); the current report will be replaced by the newly generated one, unless you click the push-pin icon at the top of the window.

- For most charts and tables, click any item to see either a **Data Protection Detail Report** with a listing of individual data protection operations, or an additional chart showing a further break-down of that day's data protection operations by application. In the **Data Protection Detail Report**, you can double-click any entry to access the Job Detail screen, which provides more space for Failure Reason, Attempt and Copy information to be displayed.
- Rearrange tabular columns by clicking and dragging the column titles to the left or right.
- For some tables, re-sort the information by clicking a column title.
- Change the columns displayed by right-clicking any row and selecting/clearing any column names from the pop-up View menu. (Column names that appear dimmed will always be displayed, as they are defaults.)
- For most charts, place the cursor over an item to display a tool-tip window with a summary of additional information available for that item.
- For some reports, cells containing data that is not compatible with the Agent will be shaded.
- In reports where column section is allowed, there are minimum default columns that will display regardless of selection.
- The following Microsoft Windows File Systems: Windows XP, Windows Server 2008 and Windows Vista, are grouped together and displayed as **Win FS** in all Reports and Summaries. Note that this does not apply to Operating System fields where the specific operating system will be displayed.
- The Data Protection Detail Report provides an error code for jobs that have not completed successfully. For more information, see Obtaining Information about Job Errors.
- Launch detail reports for specific information pertaining the selected entity in the report. Clicking on a non-zero value in the report will initiate the associated detail report. Refer to the following table:

Name of Detail Report	Report(s) from which the Detail Report can be launched
Data Protection Detail Report	All Data Protection Reports
Load Detail Report	CommCell Load Report, Load Report
Data Protection Subclient Detail Report	Data Protection Coverage Report, Dashboard Report
Data Recovery Detail Report	Data Recovery Activity Report, Data Recovery Job Success Report
Data Recovery Recall Detail Report	Data Recovery Recall Report
CommCell Growth Drive Detail Report	CommCell Growth Report
CommCell Growth Library Detail Report	CommCell Growth Report

- When specifying a time range during your selection of filter options for reports and summaries, you can easily and quickly adjust the calendar by months or years from the enhanced calendar options, which makes it easy to select the time range required for your report. Use the inner arrow selection button ( > ) to move the calendar in monthly increments, and the outer arrow selection button ( >> ) to move the calendar in yearly increments.
- Data displayed in tables can be sorted, filtered, exported, resized and/or hidden. These features are accessible by right-clicking on the table-header, and selecting the corresponding option from the popup menu. Refer to the following:

Option	Description
Auto Resize Column	Select this option to resize the selected column to its original size
Auto Resize All Columns	Select this option to resize all the columns in the table to their original size
Show All Hidden Columns	Select this to display the hidden columns.
Export Table	Select this option to export the data currently displayed in the table to a Microsoft Excel spreadsheet.
Filter	Select this option to display data containing a specific value. You will be prompted to enter the value.

- Data Type Size can now be displayed in terms of Application or Media Sizes in the following reports and summaries:
  - CommNet Data Protection Activity Overview
  - Data Protection Job Activity Report
  - Data Protection Data Growth Report
  - CommCell Summary
  - Cell-Client Group Summary

Application size indicates the amount of data protected during backup operations where Media Size is the amount of data written to the media; this includes backup, encrypted, compressed, and deduplicated data if applicable. Reporting in each method can be extremely useful for quickly determining amounts of backup data and media usage within your CommCell.

## UNINSTALLED AND DELETED OBJECTS

Each report and summary has been designed to either reflect uninstalled and deleted objects or not, based on the way the report is designed to be used. For instance, the backed up data for a deleted subclient is retained, and thus it is reflected in the Data Protection Coverage Report. Refer to the following table to determine how each Report will treat deleted objects:

<b>NOTE:</b> Yes = it is included in charts and/or totals and/or details report	Deleted Subclient	Deleted BackupSet	Uninstalled iDataAgent	Deleted iDataAgent	Uninstalled Client with Uninstalled <b>not</b> deleted iDataAgent	Uninstalled Client <b>with</b> deleted iDataAgent	Deleted Client
<b>Reports</b>							
Data Protection Coverage	<b>Yes</b>	No	<b>Yes</b>	No	<b>Yes</b>	No	No
Data Protection Summary	<b>Yes</b>	No	<b>Yes</b>	No	<b>Yes</b>	No	No

Data Protection Activity	<b>Yes</b>	Yes	<b>Yes</b>	No	<b>Yes</b>	No	No
Job Success	<b>Yes</b>	Yes	<b>Yes</b>	Yes	<b>Yes</b>	Yes	Yes
Data Growth	<b>Yes</b>	Yes	<b>Yes</b>	Yes	<b>Yes</b>	Yes	No
Window Utilization	<b>Yes</b>	Yes	<b>Yes</b>	Yes	<b>Yes</b>	Yes	Yes
SLA	Yes	No	Yes	No	Yes	No	No
Client SLA	Yes	No	Yes	No	Yes	No	No
Data Recovery Activity	--	Yes	Yes	Yes	Yes	Yes	Yes
Data Recovery Job Success	--	Yes	Yes	Yes	Yes	Yes	Yes
Data Recovery Recall	No	No	No	No	No	No	No
Update Status Report	No	No	No	No	No	No	No
<b>Summaries</b>							
CommCell	<b>Yes</b>	Yes	<b>Yes</b>	No	<b>Yes</b>	No	No
Client	No	No	No	No	--	--	--
Client Data Growth	<b>Yes</b>	Yes	<b>Yes</b>	--	--	--	--
Subclient Data Growth	<b>Yes</b>	--	<b>Yes</b>	--	--	--	--

## CONSIDERATIONS

- When you generate a report, several dates are shown in the report window:
  - Generated at** - The local time on your machine where you generated the report.
  - Reported as of** - All data protection reports are based on the latest information obtained from the CommCells at the interval specified in the Cell Data Collection Policy dialog box, which means it is not "real time" data; this date shows when the last update occurred. If it is necessary to update the information from a CommCell immediately, see Synchronize Cells for more information. This is the local time of the CommCell.
  - Time Range** - The reporting period that you chose in the **Time Range Selection** filter. If you are generating reports for multiple CommCells across different time zones, bear in mind that this time is based on the CommCell's local time. If the time range filters include the **Include current period** option, then the results reported will include the most current data, e.g., if the you configured a report with a time range of the last 7 days with the **Include current period** option selected, the results would include data from the current day as well, even though the 24 hour cycle has not completed. If the option was not selected, the results would have excluded the current day.
- Most reports have a 31 day window of reporting. You can choose any calendar period, 31 days at a time, for which you still have data on the CommNet Server. Data protection history is available for whatever retention period you have set in the CommNet Properties dialog box. (The **Data Growth Report** has limits of 31 days, or 24 weeks, or 6 months; however, the same principles apply.)
- Some **Data Protection Detail Reports** have an **Is Pruned** column; this indicates if the protected data is still being stored, or if it has been pruned by the MediaAgent.
- A SQL Agent which is installed in a CommCell, but which has no subclient content configured yet, may not appear in Reports or Summaries. Once an instance has been configured as subclient content for the Agent, all Reports and Summaries will reflect the presence of the Agent in the CommCell.
- Data related to Workstation Backup and ContinuousDataReplicator agents are displayed in the following reports and/or summaries:
  - Data Protection Summary
  - Client Summary
  - Data Replication Monitor
- The user account used to access the CommNet Browser when you schedule a report is the owner of the report. Only the owner can modify the report schedule. Therefore, if the user account is deleted, ownership of the report schedule should be transferred to another user to enable it to be modified, if necessary. You can transfer ownership of a report schedule upon deletion of the owner's user account. For more information, see Delete a User.

## REPORT TASKS

For the Reports node, the Reports task is available from the **Report Tasks** section of the CommNet Browser. This task allows you to select a Billing, Data Protection, Data Recovery, Media Management, Primary Storage, or License Report.

## AVAILABLE REPORTS

There are several tasks you should accomplish before generating reports, which are summarized in Getting Started. To learn more about each available report, click the links provided in the table below.

The table below displays reports that are available in CommNet Browser when CommNet Advanced Reporting license is enabled or disabled.

COMMNET ADVANCED REPORTING LICENSE ENABLED	COMMNET ADVANCED REPORTING LICENSE DISABLED
<b>Billing Reports</b>	None



<ul style="list-style-type: none"> <li>• Billing Association Report - shows the association of billable entities and cost categories to CommCell storage entities and objects. Also shows the storage entities and objects that do not have any billing entity or cost category association.</li> <li>• Billing Charge Back Report - generates a list of computed charges for primary and secondary storage based on defined cost categories. Has the capability to calculate these charges automatically from a fixed costing method. Can also charge based on a billing entity or a client computer.</li> <li>• Billing Detail Report - displays, for a particular cell or client, an exhaustive view of the charges. This report can be derived by clicking on the number of data protection operations, total price, data size, or the price for data protection or price for storage.</li> </ul>	
<p><b>Data Protection Reports</b></p>	
<ul style="list-style-type: none"> <li>• Data Protection Coverage Report - displays whether or not a subclient has consistent data protection coverage. The data contained within the <b>Subclient Status</b> table can be displayed in image or text format; viewing this table in text format is useful when colors cannot be identified, e.g., viewing a black and white printout of the report.</li> <li>• Data Protection Client Summary Report - a summary of the data protection operations each day</li> <li>• Data Protection Activity Report - shows data protection jobs that were completed, and/or failed or killed, for all subclients</li> <li>• Data Protection Job Success Report - shows a trend of how jobs are completing over a range of days</li> <li>• Data Protection Admin Job History Report - shows the administration jobs that were completed, and/or failed or killed, for selected clients, client computer groups, and/or CommCells.</li> <li>• Data Protection Data Growth Report - shows the trend of data growth within a CommCell</li> <li>• Data Protection Window Utilization Report - shows a summary of data protection operations relative to the data protection window</li> <li>• Data Protection SLA Report - provides averages and performance ratings to quickly determine if your CommCells, clients, applications, and subclients have adequate data protection coverage</li> <li>• Data Protection Consecutive Job Failure Report - shows the consistency of backups over a range of time</li> <li>• Data Protection Detail Report - provides a list of individual data protection operations (e.g., start times, duration, interruptions, multiple attempts, and reasons for failures). This is not a primary report. Rather, it is derived from the Data Protection Data Growth, Window Utilization, Activity, Coverage, and Job Success Reports. The maximum number of jobs that are displayed per CommCell or Cell-Client Group in this report can be configured from the CommNet Properties dialog box.</li> </ul>	<ul style="list-style-type: none"> <li>• Data Protection Client Summary Report - a summary of the data protection operations each day</li> </ul>
<p><b>Data Recovery Reports</b></p>	
<ul style="list-style-type: none"> <li>• Data Recovery Activity Report - shows data recovery jobs that were completed, and/or failed or killed, for all subclients</li> <li>• Data Recovery Job Success Report - shows a trend of how jobs are completing over a range of days</li> <li>• Data Recovery Recall Report - shows the number of recall jobs that have completed, failed, or have been killed for the Migration Archiving #DataAgents in a CommCell.</li> </ul>	<p>None</p>
<p><b>Media Management Reports</b></p>	
<ul style="list-style-type: none"> <li>• Media Management MediaAgent Report - provides information about each MediaAgent in a CommCell</li> <li>• Media Management Drive Report - provides information about each drive in a CommCell</li> <li>• Media Management Media Information Report - provides information on the status of media in the CommCell.</li> <li>• Media Management Library Report - provides information about each library in a CommCell</li> <li>• Media Management Performance Report - provides performance related information on the libraries and drives in the CommCells</li> <li>• Media Management Capacity Planning Report - predicts the amount of media that will be required in the CommCells</li> <li>• Media Management Cleaning Media Report - provides information about the average usage of cleaning media libraries as well as the cleaning media detail per library.</li> <li>• Media Management VaultTracker Report - provides information on VaultTracker actions occurring in the CommCell.</li> <li>• Media Management Tape Slot and Utilization Report - provides information on the utilization of media within the CommCell.</li> </ul>	<ul style="list-style-type: none"> <li>• Media Management MediaAgent Report - provides information about each MediaAgent in a CommCell</li> <li>• Media Management Drive Report - provides information about each drive in a CommCell</li> <li>• Media Management Library Report - provides information about each library in a CommCell</li> </ul>
<p><b>Primary Storage Reports</b></p>	
<ul style="list-style-type: none"> <li>• SRM Job Activity Report - shows SRM jobs the were completed, and/or failed or killed, for all selected CommCells and/or Cell-Client groups.</li> <li>• SRM Job Success Report - shows a trend of how SRM jobs are completing over a range of days.</li> </ul>	<p>None</p>

<ul style="list-style-type: none"> <li>Primary Storage Data Growth Report - provides information about the data size of the primary storage in CommCells. Also provides the ability to generate predictive trending for better capacity planning.</li> </ul>	
<b>Other Reports</b>	
<ul style="list-style-type: none"> <li>CommCell Growth Report - provides a summary of the weekly, monthly and/or yearly growth patterns of all the CommCells' data protection jobs, iDataAgents, subclients, libraries and drives.</li> <li>Dashboard Report - provides a pictorial view of a CommNet entity's last seven days. By default, four reports are displayed in the Dashboard, but users can select up to six reports to be displayed in the Dashboard. Dashboard Report can be customized via the <b>Browser Options</b> dialog box.</li> <li>License Summary Report - provides a summary of licenses for selected CommCell(s).</li> <li>Load Report - provides CommCell job activity details as well as peak load status.</li> <li>Update Status Report - provides the overall update status of the clients in the CommCells.</li> </ul>	<ul style="list-style-type: none"> <li>License Summary Report - provides a summary of licenses for selected CommCell(s).</li> </ul>

## FILTERS

Filtering allows you to minimize the amount of extraneous data in your reports, so you can concentrate on only that data which is essential to managing your CommCells. Each report has multiple filters available for such things as Time Range, CommCell, Client, Price, Association, Configuration, Entity Selections, and others, appropriate to each report.

### TIME RANGE SELECTION FILTER - WEEKENDS

Some reports have a **Time Range Selection** filter with an **Override CommCell Weekend Configuration** option. This allows you to generate reports that treat weekend days as you specify, regardless of how each particular CommCell Data Protection Window is configured. Using this option will ensure that the report you generate is consistent across all selected CommCells, but will not affect the settings in the Cell Configuration (Data Protection Window), only the report you generate in this instance.

### CLIENT STATUS SELECTION FILTER

In the Data Protection Summary Report, the **Client Status Selection** filters allow you to include the following for each selected CommCell in this report:

- All clients
- Only clients that have not had data protection coverage in a specified number of days; additionally, this filter can exclude those clients with no schedules, such as unutilized default subclients.
- Only clients that do not have schedules set up, such as unutilized default subclients.

If you select the option **Clients with no data protection in last <x> days**, you will find that all clients with an unused default subclient are included in the report, even if they have other subclients that have regularly scheduled data protection. To exclude them, so you can see a report of only those clients whose scheduled data protection has not completed successfully, select the **Exclude those without schedules** option. Note that this option will exclude all clients that have no schedule, not just the ones with unused subclients. Thus it might be useful to generate a separate report using only the **Clients with no schedules** option, and ascertain if that status is appropriate for each.

The Data Protection SLA Report and the Client SLA Summary similarly have an **Exclude Subclients without schedules** option. Select this filtering option so you can see a report of only those clients whose scheduled data protection has not completed successfully. Importantly, selecting this option will raise the calculated SLA for the CommCell, Client, and Application, since it will no longer include these subclients.

### EXCLUDE COMMAND LINE SUBCLIENTS

The following reports contain the **Exclude Command Line Subclients** option, which allows you to exclude those subclients, created using the command line interface, in report calculations.

- CommCell Growth Report
- Data Protection Coverage Report
- Data Protection Summary Report
- Data Protection SLA Report

## DATA AVAILABILITY TIMELINES

When a CommCell is registered with a CommNet Server, the job history in the CommCells and the data growth information are collected. The following table describes when and/or how far back this information is available in the various reports and summaries, depending on the CommServe software version.

Report/Summary/Task	CommServe 7.0.0	CommServe 8.0.0	CommServe 9.0.0
Data Protection	Supported	Supported	Supported

<ul style="list-style-type: none"> <li>• Coverage Report <ul style="list-style-type: none"> <li>○ Subclient Detail Report</li> </ul> </li> <li>• Activity Report</li> <li>• Job Success Report</li> <li>• Data Growth Report</li> <li>• Window Utilization Report</li> <li>• SLA Report</li> <li>• Consecutive Job Failure Report</li> </ul> <p>CommCell Summary</p> <p>Secondary Storage Client Data Growth (Client node tasks)</p> <p>Subclient Data Growth (Client node tasks)</p>			
Billing Charge Back Report (Secondary Storage)	Supported	Supported	Supported
Billing Charge Back Report (Primary Storage)	Supported	Supported	Supported
Billing Detail Report	Supported	Supported	Supported
Billing Association Report	Supported	Supported	Supported
Data Protection Summary Report (Client Summary)	Supported	Supported	Supported
Data Protection Admin Job History Report	Supported	Supported	Supported
Data Recovery Activity Report	Supported	Supported	Supported
Data Recovery Job Success Report	Supported	Supported	Supported
Data Recovery Recall Report	N/A	Supported	Supported
Media Management <ul style="list-style-type: none"> <li>• MediaAgent Report</li> <li>• Drive Report</li> <li>• Library Report</li> </ul> <p>Library Summary</p> <p>MediaAgent Summary</p>	Supported	Supported	Supported
Media Management Performance Report	Supported	Supported	Supported
Media Management Capacity Planning Report	Supported	Supported	Supported
Media Management Cleaning Media Report	N/A	Supported	Supported
Primary Storage Data Growth Report	Supported	Supported	Supported
Primary Storage Client Data Growth (Client node task)			
License Summary Report	Supported	Supported	Supported
CommCell Growth Report	Not available.	Supported	Supported
CommNet Data Protection Activity Summary	Supported	Supported	Supported
CommNet Primary Storage Summary	Supported	Supported	Supported
Cell-Client Groups	Supported	Supported	Supported
Dashboard Report	Supported	Supported	Supported
Load Report	Supported	Supported	Supported
Jobs and Resources View	Supported	Supported	Supported
Update Status Report	N/A	Supported	Supported

## LICENSE REQUIREMENT

This component requires a Product License to be available in the CommNet 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](#)

# CommNet Summaries

Topics | Troubleshoot

Overview

Summary Features

- Considerations

Available Summaries

Data Availability Timelines

## OVERVIEW

Summary pages provide a concise view of the current state of the physical entities within the CommNet Browser. Information is presented in a logically grouped, tabular format, as well as a bar chart or pie chart wherever appropriate. For a listing, and links to more specific information about each Summary, see Available Summaries.

Information that will facilitate troubleshooting is available as well, such as:

- Clients that are not reachable from a Cell
- Data growth
- CommCell related:
  - MediaAgents, libraries, and drives that are not operational. Clicking problem areas underlined in red, such as a MediaAgent that is not operational, displays more detailed information about the problem.
  - Data protection activity that failed, was killed, or was incomplete. Clicking a failed or killed data protection job in Job activity charts, displays a Data Protection Detail Report.
  - Media that was consumed, or how much a MediaAgent was utilized.
  - Comparison information between full data protection operations with non-full data protection operations that were performed.

## SUMMARY FEATURES

There is a range of functionality available in the CommNet Browser related to Summaries; see CommNet Browser. The following functionality is also available:

- Print, Save as a PDF file, or Export in Microsoft Excel format by clicking the appropriate icon at the top of the summary window.
- Schedule a summary by clicking the Schedule icon at the top of the summary window. Note that initially, summaries are generated automatically.
- Copy any chart in BMP format to the clipboard by right-clicking the chart and selecting **Copy Chart**. This allows you to easily copy a chart into other applications. Note that charts cannot be copied into Microsoft WordPad.
- For most charts and tables, click any item to see either a **Data Protection Detail Report** with a listing of individual data protection operations, or an additional chart showing a further break-down of that day's data protection operations by application. In the **Data Protection Detail Report**, you can double-click any entry to access the **Job Detail** screen, which provides more space for Failure Reason, Attempt and Copy information to be displayed.
- Rearrange tabular columns by clicking and dragging the column titles to the left or right.
- For some tables, re-sort the information by clicking a column title.
- Change the columns displayed by right-clicking any row and selecting/clearing any column names from the pop-up View menu. (Column names that are dimmed will always be displayed, because they are defaults.)
- For most charts, place the cursor over an item to display a tool-tip window with a summary of additional information available for that item.
- The following Microsoft Windows File Systems: Windows XP, Windows Server 2008 and Windows Vista, are grouped together and displayed as **Win FS** in all Reports and Summaries. Note that this does not apply to Operating System fields where the specific operating system will be displayed.
- When specifying a time range during your selection of filter options for reports and summaries, you can easily and quickly adjust the calendar by months or years from the enhanced calendar options, which makes it easy to select the time range required for your report. Use the inner arrow selection button ( > ) to move the calendar in monthly increments, and the outer arrow selection button ( >> ) to move the calendar in yearly increments.
- Data displayed in tables can be sorted, filtered, exported, resized and/or hidden. These features are accessible by right-clicking on the table-header, and selecting the corresponding option from the popup menu. Refer to the following:

Option	Description
Auto Resize Column	Select this option to resize the selected column to its original size
Auto Resize All Columns	Select this option to resize all the columns in the table to their original size
Show All Hidden Columns	Select this to display the hidden columns.

Export Table	Select this option to export the data currently displayed in the table to a Microsoft Excel spreadsheet.
Filter	Select this option to display data containing a specific value. You will be prompted to enter the value.

## CONSIDERATIONS

- A SQL Agent which is installed in a CommCell, but which has no subclient content configured yet, may not appear in Reports or Summaries. Once an instance has been configured as subclient content for the Agent, all Reports and Summaries will reflect the presence of the Agent in the CommCell.
- Data related to Workstation Backup and ContinuousDataReplicator agents are displayed in the following reports and/or summaries:
  - Data Protection Summary
  - Client Summary
  - Data Replication Monitor

## AVAILABLE SUMMARIES

There are several tasks you should accomplish before generating summaries, which are summarized in Getting Started. To learn more about each available summary, click the links provided:

- CommNet Summary
- CommNet Data Protection Activity Summary
- CommNet Primary Storage Summary
- User Summary
- User Group Summary
- CommCell Summary
- Library Summary for Tape/Optical/Stand-alone libraries
- Library Summary for Magnetic libraries
- MediaAgent Summary
- Cell-Client Group Summary
- Client Summary
- Secondary Storage Client Data Growth
- Secondary Storage Client Data Growth (Subclient)
- Client SLA
- Primary Storage Client Data Growth

## DATA AVAILABILITY TIMELINES

When a CommCell is registered with a CommNet Server, the job history in the CommCells and the data growth information are collected. The following table describes when and/or how far back this information is available in the various reports and summaries, depending on the CommServe software version.

Report/Summary/Task	CommServe 7.0.0	CommServe 8.0.0	CommServe 9.0.0
Data Protection	Supported	Supported	Supported
<ul style="list-style-type: none"> <li>• Coverage Report <ul style="list-style-type: none"> <li>○ Subclient Detail Report</li> </ul> </li> <li>• Activity Report</li> <li>• Job Success Report</li> <li>• Data Growth Report</li> <li>• Window Utilization Report</li> <li>• SLA Report</li> <li>• Consecutive Job Failure Report</li> </ul>			
CommCell Summary			
Secondary Storage Client Data Growth (Client node tasks)			
Subclient Data Growth (Client node tasks)			
Billing Charge Back Report (Secondary Storage)	Supported	Supported	Supported
Billing Charge Back Report (Primary Storage)	Supported	Supported	Supported
Billing Detail Report	Supported	Supported	Supported
Billing Association Report	Supported	Supported	Supported
Data Protection Summary Report (Client Summary)	Supported	Supported	Supported
Data Protection Admin Job History Report	Supported	Supported	Supported

Data Recovery Activity Report	Supported	Supported	Supported
Data Recovery Job Success Report	Supported	Supported	Supported
Data Recovery Recall Report	N/A	Supported	Supported
Media Management <ul style="list-style-type: none"> <li>• MediaAgent Report</li> <li>• Drive Report</li> <li>• Library Report</li> </ul> Library Summary MediaAgent Summary	Supported	Supported	Supported
Media Management Performance Report	Supported	Supported	Supported
Media Management Capacity Planning Report	Supported	Supported	Supported
Media Management Cleaning Media Report	N/A	Supported	Supported
Primary Storage Data Growth Report	Supported	Supported	Supported
Primary Storage Client Data Growth (Client node task)			
License Summary Report	Supported	Supported	Supported
CommCell Growth Report	Not available.	Supported	Supported
CommNet Data Protection Activity Summary	Supported	Supported	Supported
CommNet Primary Storage Summary	Supported	Supported	Supported
Cell-Client Groups	Supported	Supported	Supported
Dashboard Report	Supported	Supported	Supported
Load Report	Supported	Supported	Supported
Jobs and Resources View	Supported	Supported	Supported
Update Status Report	N/A	Supported	Supported

[Back to Top](#)

# CommCells

Topics | How To | Tasks | Troubleshoot | Related Topics

---

Overview

Register and Synchronize a CommCell

- CommNet Client Connectivity

Register and Synchronize a CommCell with Two CommNet Servers

- What Happens When the Roles of the Primary CommNet Server and Secondary CommNet Server are Reversed

CommCell Jobs and Resources

- Jobs View
  - Resources View
- 

## OVERVIEW

The software provides an efficient way of managing multiple CommCells, by reporting all the vital information in a concise manner, highlighting only the problem areas instead of reporting all the details which could easily overwhelm an administrator.

---

## REGISTER AND SYNCHRONIZE A COMMCELL

In order to monitor the CommCells in your CommNet domain, you must register the CommCell with your CommNet Server. See, Register a CommCell.

Once registered, each CommCell node displays the following:

- A list of Clients available in the CommCell, with each Client node providing the specific information about the client.
- A list of Storage Resources available in the CommCell, which includes the MediaAgents and Libraries. Each MediaAgent and Library nodes provide specific information about the MediaAgent or Library.

CommCell Summary displays the date and time at which the data was obtained from the CommCell in the title of the summary page. If you wish to obtain a more up-to-date information on the CommCell, you can synchronize the CommCell as described in Synchronize Cells.

The following information is synchronized from the selected CommCells:

- Configuration information which includes the following:
  - Client information
  - MediaAgent information
  - Library information
  - Job history
  - Media Management history
  - Resource view update information
  - Load Report information (data necessary to generate report)
  - Time zone information
- Information associated with the CommCell jobs
- Events associated with the CommCell jobs

The following information is synchronized from selected the SRM components in a CommCell:

- Information from the SRM Agents including the following:
  - space utilization and volume information for file systems and NAS shares
  - space utilization and content for file system subclients
  - space utilization for databases, instances, stores and storage groups
  - Billable Entity and Cost Category assignments for primary storage

When the following configurations are modified, the changes are immediately pushed to the active CommCell(s); cell synchronization is not required to propagate this information to the cells.

- Global Filters
- Billable Entities

- Cost Categories
- Data Collection Policy
- Comments (Note that Comments made using the CommCell Console are pushed to the CommNet Server only during cell synchronization. For more information, see Comments.)

This information will be pushed accordingly when services (CommNet Server or Bull Calypso Server Event Manager) are restarted as well.

## 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.

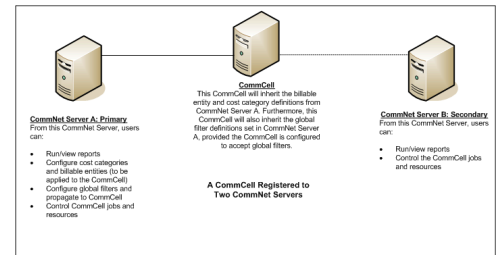
## REGISTER AND SYNCHRONIZE A COMMCELL WITH TWO COMMNET SERVERS

Your CommNet environment may require an alternate department (or even a third-party entity) to monitor a CommCell's data in your CommNet domain for the purpose of data and cost analysis. To satisfy this requirement, the CommCell can be registered with two CommNet Servers, which enables an alternate site to monitor the CommCell. During the CommCell registration process, the first server registered is designated as the primary server, where the other will be designated as the secondary server. The functional difference between the two CommNet servers are that only the primary server can push policies like global filters, billable entities and cost categories to the CommCell. Both CommNet Servers can collect data, monitor, control jobs and resources, and generate reports. The capabilities of the primary and secondary CommNet servers are outlined in the following table.

Primary CommNet Server	Secondary CommNet Server
Run and view reports.	Run and view reports.
Control Jobs: Suspend, Resume, Kill.	Control Jobs: Suspend, Resume, Kill.
Control Resources (libraries, drives/mountpaths, MediaAgents): Enable, Disable, or Reset.	Control Resources (libraries, drives/mountpaths, MediaAgents): Enable, Disable, or Reset.
Configure global filters and propagate downward to CommCell.	
Define billable entities and propagate downward to CommCell.	
Define cost categories and propagate downward to CommCell.	

Remember, the secondary CommNet server should be designated as the server for the alternate site due to its inability to distribute its global filter, billing and costing definitions to the CommCell. With this, a CommCell registered to two CommNet servers might resemble the diagram displayed to the right.

The capability differences between the primary and secondary CommNet servers warrant caution when registering a CommCell to two servers. If you register a CommCell to multiple servers, and inadvertently designate the primary server to a site designated to only monitor the data (perhaps even a third-party), they will now have the ability to define cost categories and billing entities, thereby jeopardizing the security and integrity of your data/environment. Furthermore, the CommNet server that is inadvertently designated as the secondary server, may appear to be failing b/c of the inability to execute cost analysis tasks. For verification, you can identify whether a CommNet Server is the primary or secondary server from the CommCell Summary. The General section of the summary will indicate whether or not the CommNet Server is the primary or secondary server for the CommCell.



## WHAT HAPPENS WHEN THE ROLES OF THE PRIMARY COMMNET SERVER AND SECONDARY COMMNET SERVER ARE REVERSED

It may be necessary to re-designate the roles of the primary and secondary servers perhaps due to a failover situation. To re-designate the servers, you must access the CommCell's Control Panel. From there, the CommNet Properties dialog will enable you to identify the CommNet Servers to which the CommCell is registered, as well as which server is designated as the CommCell's Primary CommNet Server; and if necessary, enable you to re-designate the Secondary CommNet Server as the Primary Server, and vice versa. If you reverse the roles, be sure to note the following considerations:

- When a CommCell is registered to two CommNet Servers, it will inherit the billable entity and cost category definitions configured in the Primary CommNet Server. Therefore, in an environment where a CommCell is registered two CommNet Servers and the roles of the CommNet Servers are reversed, the CommCell will inherit the billable entity and cost category definitions of the new primary server.
- CommCell jobs that have completed retain their cost category definitions, whereas currently running CommCell jobs inherit the cost category definitions from the server that is designated the primary server at the time the job completes its data writing phase. These costs will be included in the Billing Charge Back Report, which can be run from both the Primary and Secondary CommNet Servers.
- When a CommCell is registered to two CommNet Servers, it will inherit the global filter definitions configured in the Primary CommNet Server provided that the CommCell is configured to accept the CommNet Server's global filter definitions (see Global Filters). Therefore, in an environment where a CommCell is



registered two CommNet Servers and the roles of the CommNet Servers are reversed, the CommCell will inherit the global filter definitions of the new primary server and delete the filter definitions from the previous primary server.

For step-by-step instructions, see:

- Register a Cell
- Remove a Registered Cell
- Synchronize Cells

To register a CommCell with two CommNet Servers, all components must have the latest software version installed.

---

## COMMCELL JOBS AND RESOURCES

Jobs and Resources is a CommCell task in the CommNet Browser. When selected, users can select to view the CommCell's status information in a Jobs View and Resources View. See Run CommCell Tasks.

---

### JOBS VIEW

The Job View contains the all the jobs associated with the selected CommCell. This view is automatically refreshed every 30 seconds per CommCell. Users can view the status of the jobs and control them via this view, which is especially useful if the Jobs View indicates that there is a problem with a resource hindering a successful completion.

From this view, users can right click on a job and perform the following actions:

- Suspend
- Resume
- Kill

For more information, see Control Jobs from the CommCell Jobs View.

---

### RESOURCES VIEW

The Resources view contains the events that have occurred on a given mountpath, library, drive or MediaAgent. This view is automatically refreshed every 30 seconds per CommCell as well. Users can control the mountpath and resources via this view. It can be used to quickly identify whether any libraries and/or MediaAgents are offline, or if there are any other problems with any of the resources. Additionally, from this view, users can click on a Library, Drive, MediaAgent, or Media to launch another window displaying the resource's specific details. This is especially useful if the Jobs and Resources view indicates that there is a problem with a resource.

From this view, users can right-click on a Library, Drive/Mountpath, or MediaAgent to perform the following actions:

- Library: **Enable**, **Disable**, or **Reset** the library
- Drive: **Enable**, **Disable**, **Reset**, or **Unmount** the drive
- Mountpath: **Enable** or **Disable** the mountpath
- MediaAgent: **Enable** or **Disable** the MediaAgent.

Users can also filter the Resources View to only display details related to specific libraries or MediaAgents.

For more information, see Manage Resources from the CommCell Resources View.

---

## CommCells - How To

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

---

Synchronize Cells

Register a Cell

Register a Cell When the CommNet Server is not Reachable

- Stop All Other Tasks if Current Task Fails
- Register From the Command Line

Remove a Registered Cell

Modify the Display Name of a Cell  
Modify the CommServe Host Name  
Modify the Description or Contact Information of a Cell  
Change the Network Connection Type  
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  
Set up the Frequency for Checking Network Connectivity between CommNet Server and CommCells  
Configure Data Collection Policy  
Change the CommCell Authentication Password  
Run CommCell Tasks  
Control Jobs from the CommCell Jobs View  
Manage Resources from the CommCell Resources View

---

## SYNCHRONIZE CELLS

*Required Capability:* See Capabilities and Permitted Actions

▶ To synchronize the Cells:

1. On the **Setup** menu, click **Cell Synchronization**.
2. From the drop down tree of the Cell Synchronization dialog box, select the CommCells that you wish to synchronize.  
Click **OK**. This will start the synchronization process.

▶ To synchronize one CommCell:

1. Right-click on a CommCell in the CommNet Tree.
  2. Select **Synchronize** from the popup menu. This will start the synchronization process.
- 

## REGISTER A CELL

*Required Capability:* See Capabilities and Permitted Actions

▶ Use this procedure to register a cell using the CommNet Console:

1. On the **Setup** menu, click **Cell Registration**.
2. From the Cell Registration dialog box, click **Add CommCell** (or **Modify** if reregistering the Cell).
3. From the Register CommCell dialog box, specify the registration information.

If reregistering the Cell, click the **Register CommCell Again - CommCell Administrator** check box and specify the user account name and password. Click **OK**. The re-registered Cell is displayed in the Cell Registration dialog box.

4. Select the following options to collect the specific data thereby enabling you to run the corresponding reports. Note that this is only applicable when registering a CommCell.
  - **Collect Primary Storage Data:** Select this option to collect SRM data from the CommCell, enabling you to run the Primary Storage Data Growth Report against this CommCell. Select this option only if an SRM Server has been installed on the CommCell.
  - **Collect Media and VaultTracker Data:** Select this option to collect media and VaultTracker data from the CommCell, enabling you to run the Media Management Media Information and VaultTracker Actions reports against this CommCell.
5. Click **OK**.

The newly registered Cell is displayed in the Cell Registration dialog box. You can now see information associated with the Cell in the CommNet Browser.

- When you register a CommCell, a CommCell license is used.
  - Make sure that services are running on the appropriate cell before registering that cell with the CommNet Server.
  - CommNet Server can function with several CommCell versions. For more information, see the Compatibility Matrix.
-

## REGISTER A CELL WHEN THE COMMNET SERVER IS NOT REACHABLE

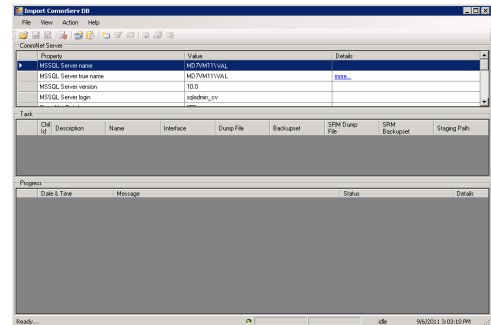
Use the following steps to register your cell and generate reports, if the CommNet Server is not reachable and you are not able to register your cell using the CommNet Console.

The following steps allows you to import multiple CommServe databases to the CommNet Server. SRM databases, if available in the CommServe, can also be imported to the CommNet Server.

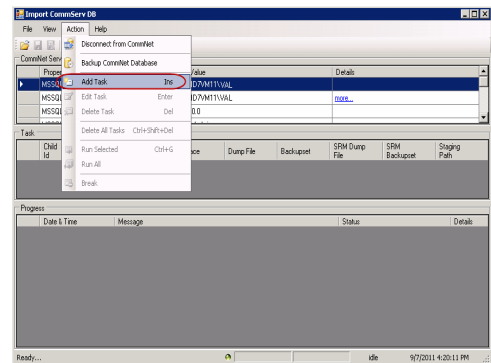
1. Use the following steps to download the tool:
  1. Click the **Download Now** button located on the right to download the **ImportCommServDBGui**.
  2. Select **<install directory>\Base** folder in the CommNet server as the location to save the .zip file.
  3. Navigate to the location of the .zip file and unzip the file.



2. Double-click **ImportCommServDBGui**.  
The **Import CommServe DB Tool** is displayed.



3. From the **Actions** menu click **Add Task**.  
The **Task** dialog box appears.



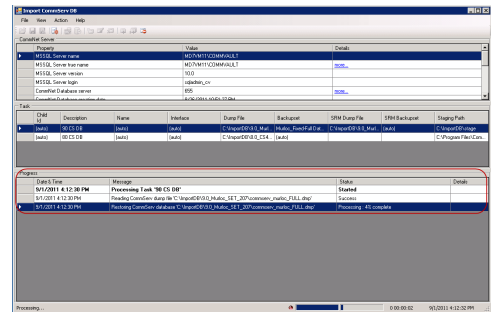
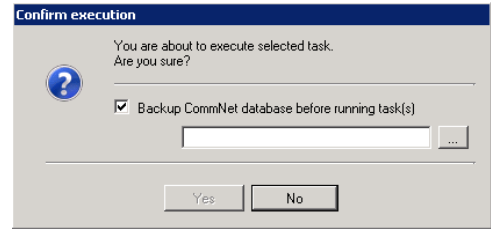
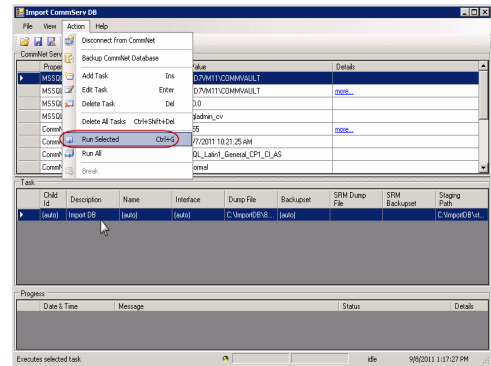
4.
  - In the **Description** field, type a description of the Import Task.  
The CommCell Properties are selected automatically, however you may change them if needed.
  - To edit any of the options under **CommCell Properties**, clear the check box, and then type the child ID, display name, or interface name in the box.
  - To browse to the CommServe Database Dump file, next to **CommServe Database Dump**, click the ellipsis button [...].

You can also browse SRM Server Database dump file along with the CommServe Database dump using this dialog box.

- Click **OK**.
5.
    - Select and highlight the added task and click **Actions** from top menu.
    - Click **Run Selected**.

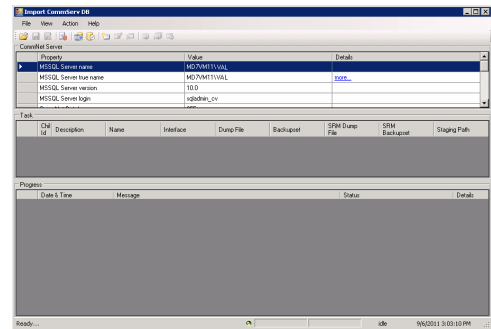
- Enter a path to backup CommNet database in Confirm Execution dialog box and click **Yes**.  
Alternatively, you may clear the **Backup CommNet database before running task** (s) and click **Yes** to not backup the CommNet database.

- You can view the progress of the import job in the Progress area.

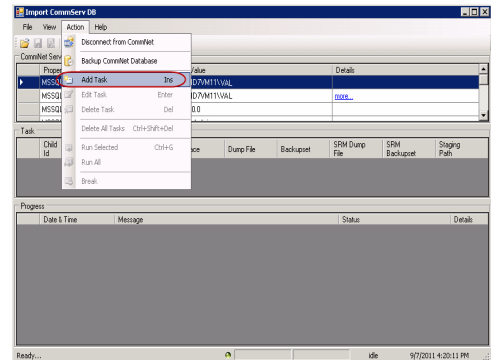


### STOP ALL OTHER TASKS IF CURRENT TASK FAILS

- Navigate to the <install directory>\Base folder in the CommNet computer.
  - Double-click **ImportCommServDBGui**.  
The **Import CommServe DB Tool** is displayed.



- From the **Actions** menu click **Add Task**.

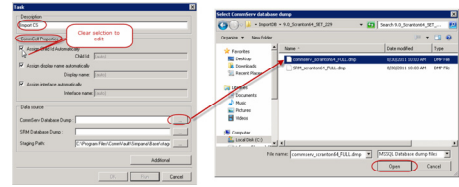


- Use the **Description** field to enter a description about the Import Task.

The CommCell Properties get selected automatically, however you may change them if needed.

- Click ... to browse to the CommServe Database Dump file.

You can also browse SRM Server Database Dump file along with the CommServe Database dump using this dialog box.



- From the **Actions** menu click **Add Task**.

- Add another CommServe Database Dump file and/or SRM Server Database Dump file.

- Click **Additional** to open the Custom options dialog box.

- Select **Cancel Import process for the rest of tasks** to stop all other tasks if current task fails.

By default this option is cleared in order to resume other tasks if current task fails.

- Additionally you may perform the following:

Select ... to browse and change to a new Schema script location.

Verify and edit the **Collection** parameters specified if needed.

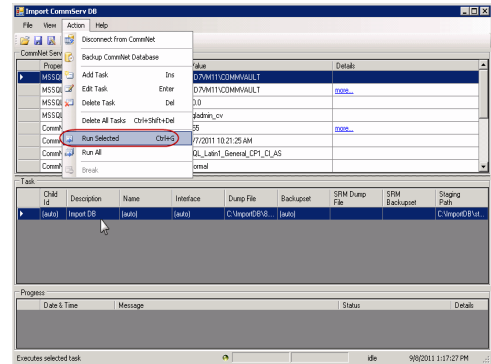
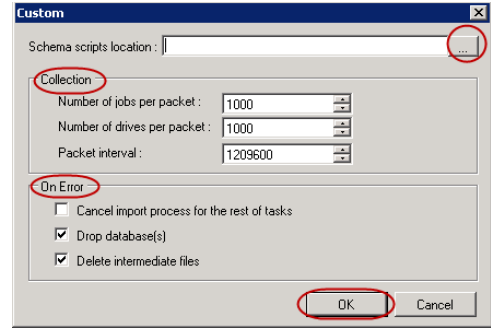
Clear **Drop database(s)** to retain database at the staging path after the task completes successfully.

Clear **Delete Intermediate** to retain intermediate files after the task completes successfully.

- Click **OK**.

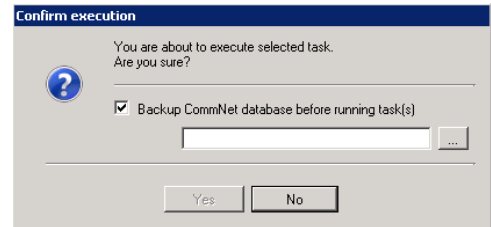
Click **OK**.

- Select and highlight the added task and click **Actions** from top menu.
  - Click **Run All Selected**.

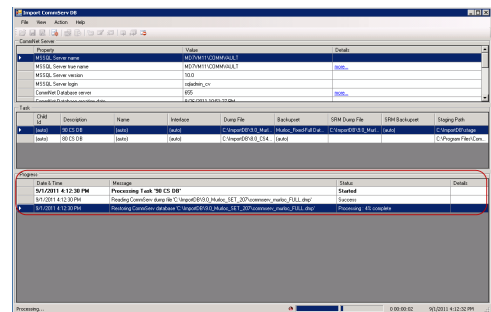


- Enter a path to backup CommNet database in Confirm Execution dialog box and click **Yes**.

Alternatively, you may clear the **Backup CommNet database before running task(s)** and click **Yes** to not backup the CommNet database.



- You can view the progress of the import job in the Progress area.



## REGISTER FROM THE COMMAND LINE

- From the command prompt, navigate to **<software\_install\_folder>\base** folder.
- Run the following command:

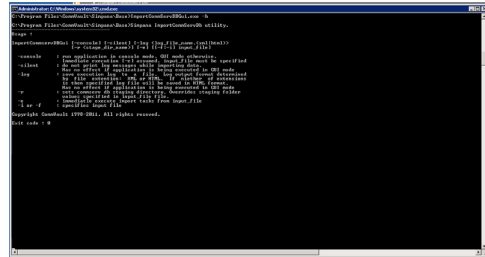
**ImportCommServDBGui** [-console] [-silent] [-log<log\_file\_name.<xml:html>> [-r<stage\_dir\_name>] [-e] [[-f:-i] input\_file]

For Example:

**ImportCommServDBGui -console -silent -log log\_file.htm -r C:/Program Files/Bull Calypso/Calypso/Base/stage -e input\_file.txt**

where

- console** Runs the application in console mode.
- silent** Does not allow printing of log messages while importing data.
- log** Saves execution log to a file. Log output format is determined by file extension that is either XML or HTML.
- r** Sets CommServe database staging directory. Overrides staging folder values specified in input file file.
- e** Immediately executes import tasks from input file.
- i or -f** Specifies input file.



## REMOVE A REGISTERED CELL

*Required Capability:* See Capabilities and Permitted Actions

▶ To remove a registered Cell:

1. On the **Setup** menu, click **Cell Registration**.
2. From the Cell Registration dialog box, select a CommCell, and then click **Remove**.
3. Click **OK** in the **Warning** prompt.
4. In the **Enter Confirm** dialog box, type Confirm and then click **OK**. The Cell is removed in the Cell Registration dialog box.
  - A CommCell license gets released when you remove a registered CommCell from the CommNet domain.
  - Make sure services are running on the appropriate Cell before removing that registered Cell.
  - After removing the registered Cell, you should remove the Cell-Client Groups that are only associated with the removed Cell. For more information, see Remove Cell-Client Group.
  - Users can unregister a CommCell from the CommNet Server using the CommServe software. For more information, see *Books Online* documentation for the CommServe.

## MODIFY THE DISPLAY NAME OF A CELL

*Required Capability:* See Capabilities and Permitted Actions

▶ To modify the display name of a Cell:

1. On the **Setup** menu, click **Cell Registration**.
2. From the Cell Registration dialog box, highlight the Cell for which you wish to modify the display name from the **Cell(s)** list, and then click **Modify**.
3. From the Modify CommCell dialog box, type the new name in the **Display Name** box.
4. Click **OK**.
5. Click **OK** in the **Registration Changed** prompt. The new name for the Cell is displayed in the Cell Registration dialog box.

The CommNet Browser uses the Display Name to display the Cell in the CommNet tree. Hence you can modify the display name to include relevant information that will help you to easily identify the Cell. For example, include the physical location of the Cell in the display name.

## MODIFY THE COMMSERVE HOST NAME

If the name of the CommServe computer changed, then you must change the host name in the CommServe computer and in the CommNet Browser.

### PREREQUISITE

Update the name of the CommServe computer in the CommCell Console. For instructions, see Change the Name of the CommServe Computer.

### UPDATE THE COMMCELL REGISTRATION

1. On the **Setup** menu, click **Cell Registration**.  
The Cell Registration dialog box appears.
2. In the **Cells** list, click the Cell where you want to modify the display name, and then click **Modify**.

The Modify CommCell dialog box appears.

3. In the the **Display Name** box, type the new name.
4. In the **CommCell Interface Name** box, type the full interface name.

For example: **cell.company.com**

5. Click **OK**.

A message appears that says that the registration changed.

6. Click **OK**.

The new name for the Cell is displayed in the Cell Registration dialog box.

## MODIFY THE DESCRIPTION OR CONTACT INFORMATION OF A CELL

*Required Capability:* See Capabilities and Permitted Actions

▶ To modify the description or contact information of a Cell:

1. On the **Setup** menu, click **Cell Registration**.
2. From the Cell Registration dialog box, highlight the Cell for which you wish to modify the description and/or contact information from the **Cell(s)** list, and then click **Modify**.
3. From the Modify CommCell dialog box:
  - Type the description in the **Description** box.
  - Type the contact information in the **Contact Information** box.
4. Click **OK**.
5. Click **OK** in the **Registration Changed** prompt.

You can record relevant reference information about the Cell in the description and contact information boxes. For example: you can record the contact information, such as the contact person, telephone numbers, email addresses, etc.

## CHANGE THE NETWORK CONNECTION TYPE

*Required Capability:* See Capabilities and Permitted Actions

▶ To change the network connection type:

1. On the **Setup** menu, click **Cell Registration**.
2. From the Cell Registration dialog box, highlight the Cell for which you wish to modify the network connection type from the **Cell(s)** list, and then click **Modify**.
3. From the Modify CommCell dialog box, choose the appropriate connection type from the **Connection Type** list.
4. Click **OK**.
5. Click **OK** in the **Registration Changed** prompt. The system saves the network connection type.
  - The connection type can be changed when the Cell is not accessible due to a low bandwidth in the connection.
  - Select LAN when you have a faster and reliable connection or WAN for slower and less reliable connections.
  - Keep in mind that by default the retry attempts for communication failures on WAN are more. The retry attempts for communication failures can be established in CommNet Properties dialog box.

## 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.
  - o 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.
  - o 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:
  - o Type the new name in the **Display Name** box.
  - o Choose the appropriate interface name from the **CommNet Interface Name** list.
  - o 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.

---

## SET UP FREQUENCY FOR CHECKING NETWORK CONNECTIVITY BETWEEN COMMNET SERVER AND COMMCELLS

*Required Capability:* See Capabilities and Permitted Actions

▶ To set up the frequency for checking the network connectivity between the CommNet Server and CommCells:

1. On the **Setup** menu, click **Cell Configuration**.
2. From the Cell Configuration (General) dialog box, type the frequency in the **Heartbeat Interval** box.
3. Click **OK**.

The idle time for the users logged in is calculated by the CommNet Server whenever the server checks the network connectivity to the CommCell.

---

## CONFIGURE DATA COLLECTION POLICY FOR OBTAINING CONFIGURATION INFORMATION

*Required Capability:* See Capabilities and Permitted Actions

▶ To configure Data Collection Policy for obtaining Configuration information:

1. On the **Setup** menu, click **Cell Data Collection Policy**.
2. From the Cell Data Collection Policy dialog box, click the arrow to set the time and the time frame (hours or minutes) in the **Configuration** boxes.
3. Click **OK** to save changes.

The updates are provided by the individual Cells and hence the update time is based on the CommCell time.



## CHANGE THE COMMCELL AUTHENTICATION PASSWORD

*Required Capability:* See Capabilities and Permitted Actions

▶ To change the CommCell authentication password:

1. On the **Setup** menu, click **CommCell Authentication**.
2. From the CommCell Authentication dialog box, click **Change Authentication**.
3. Type the new password in the **New Password** box.
4. Retype the password in the **Confirm Password** box
5. Click **OK**.

The authentication password is used as an internal security measure for CommNet-related communications. All computers within the CommNet domain will have a default password that is created when the software is installed on the computer. You can periodically change this password, to enhance security.

---

## RUN COMMCELL TASKS

*Required Capability:* See Capabilities and Permitted Actions

▶ To run CommCell Tasks:

1. From the CommNet Browser:
    - To run a task for all the CommCells, select the CommCells' parent node
    - To run a task for a specific CommCell, expand the CommCells' node, and select (highlight) a CommCell.
  2. From the CommCell(s) Tasks window, select a task. The corresponding view will display in the right-hand side windowpane.
- 

## CONTROL JOBS FROM THE COMMCELL JOBS VIEW

*Required Capability:* See Capabilities and Permitted Actions

▶ To control jobs from the CommCell Jobs View:

1. From the CommNet Browser, expand the CommCells' parent node.
  2. Select (highlight) a CommCell.
  3. From the CommCell Tasks window, select Jobs and Resources. The corresponding view will display in the right-hand side windowpane.
  4. From the right-hand side windowpane, select the **Jobs View** option. The CommCell's Job View will display in the right-hand side windowpane.
  5. Right-click any job and select **Tasks** or **View** from the popup menu:
    - Select **Tasks** to launch a popup menu allowing you to **Resume**, **Suspend**, or **Kill** the selected job. Select your option and confirm.
    - Select **View** to launch a popup menu listing those fields to add or delete from the Jobs View table display. Those items with a checkmark appearing before the field are active and currently displayed in the Job View. Click on a field to add it or remove it.
- 

## MANAGE RESOURCES FROM THE COMMCELL RESOURCES VIEW



*Required Capability:* See Capabilities and Permitted Actions

▶ To manage resources from the CommCell Resources View:

1. From the CommNet Browser, expand the CommCells' parent node.
2. Select (highlight) a CommCell.
3. From the CommCell Tasks window, select Jobs and Resources. The Resources View will display in the right-hand side windowpane.
4. From the right-hand side windowpane, select the appropriate option to display the information in tree or table format. The corresponding view will display in the right-hand side windowpane.
5. Right-click any field item and select **View** to launch a popup menu listing those fields to add or delete from the Resources View display. Those items with a checkmark appearing before the field are active and currently displayed in the Resources View. Click on a field to add it or remove it.
6. Click on a Library, Drive, Media and/or MediaAgent to launch a detail report regarding the selected entity. To close or minimize the detail report and return

to the Resources view, use the window controls.

7. Right click on a Library, Drive, or MediaAgent and select **Tasks** to launch a popup menu to manage the CommCell's resources. Options available are as follows:
  - o Library: **Enable**, **Disable**, or **Reset** the library
  - o Drive: **Enable**, **Disable**, **Reset**, or **Unmount** the drive
  - o Mountpath: **Enable** or **Disable** the mountpath
  - o MediaAgent: **Enable** or **Disable** the MediaAgent.
8. Click the icon next to the Resource View format options, Table View and Tree View, to initiate the Filter Dialog. Use this dialog box to select the specific libraries or MediaAgents to be included in the Resources View.

To use this filter, the CommNet Browser must be in a paused state, which stops updates to the current window; to do this, click on the **Pause**  button in the CommNet Browser tool bar. When finished with this filter, click on the **Play**  button to resume updates to the current window.

---

[Back to Top](#)

# CommNet Storage Resources

Topics | How To | Tasks

---

The Storage Resources node provides vital information about the MediaAgent and libraries in the CommCell. From this node you can quickly determine the MediaAgents, libraries or drives that are not operational in the CommCell.

Both the MediaAgent and Library summaries display the date and time at which the most recent information was obtained from the CommCell about MediaAgent, in the title of the summary page. If you wish to obtain more up-to-date information, you can synchronize the CommCell associated with the MediaAgent, as described in Synchronize Cells.

---


## CommNet Storage Resources - How To

Topics | How To | Tasks



---

### MANAGE RESOURCES FROM THE COMMCELL RESOURCES VIEW

*Required Capability:* See Capabilities and Permitted Actions

 To manage resources from the CommCell Resources View:

1. From the CommNet Browser, expand the CommCells' parent node.
2. Select (highlight) a CommCell.
3. From the CommCell Tasks window, select Jobs and Resources. The Resources View will display in the right-hand side windowpane.
4. From the right-hand side windowpane, select the appropriate option to display the information in tree or table format. The corresponding view will display in the right-hand side windowpane.
5. Right-click any field item and select **View** to launch a popup menu listing those fields to add or delete from the Resources View display. Those items with a checkmark appearing before the field are active and currently displayed in the Resources View. Click on a field to add it or remove it.
6. Click on a Library, Drive, Media and/or MediaAgent to launch a detail report regarding the selected entity. To close or minimize the detail report and return to the Resources view, use the window controls.
7. Right click on a Library, Drive, or MediaAgent and select **Tasks** to launch a popup menu to manage the CommCell's resources. Options available are as follows:
  - o Library: **Enable**, **Disable**, or **Reset** the library
  - o Drive: **Enable**, **Disable**, **Reset**, or **Unmount** the drive
  - o Mountpath: **Enable** or **Disable** the mountpath
  - o MediaAgent: **Enable** or **Disable** the MediaAgent.
8. Click the icon next to the Resource View format options, Table View and Tree View, to initiate the Filter Dialog. Use this dialog box to select the specific libraries or MediaAgents to be included in the Resources View.

To use this filter, the CommNet Browser must be in a paused state, which stops updates to the current window; to do this, click on the **Pause**  button in the CommNet Browser tool bar. When finished with this filter, click on the **Play**  button to resume updates to the current window.

---

# Libraries

[Topics](#) | [Tasks](#) | [Troubleshoot](#)

---

The library nodes in a CommCell provides vital information about the libraries in the CommCell. All the libraries that are not operational are highlighted in the CommNet tree.

The CommNet tree displays a node for each configured library in the CommCell, even when it is shared between multiple MediaAgents.

Library summaries display the date and time at which the most recent information was obtained from the CommCell about the library, in the title of the summary page.

If you wish to obtain more up-to-date information of the Client, you can synchronize the CommCell associated with the client, as described in [Synchronize Cells](#).

---

# MediaAgents

Topics | Tasks

---

The MediaAgent nodes in a CommCell provides vital information about all the MediaAgents in the CommCell. All the MediaAgents that are not operational are highlighted in the CommNet tree.

The CommNet tree displays a node for each MediaAgent in the CommCell. The Library Status and Drive Status display the status information associated with the physical entities that are controlled by the MediaAgent. For shared libraries the following information is displayed:

- For a library shared between multiple MediaAgents in a SAN DDS environment, the library and drive status information is displayed in all these MediaAgents.
- For a direct-attached shared library, the library information is displayed by the MediaAgent controlling the media changer. All the other MediaAgents, which share the drives in the library, display the drive information associated with the specific MediaAgent.

MediaAgent Summary displays the date and time at which the most recent information was obtained from the CommCell about the MediaAgent, in the title of the summary page.

---

# Cell-Client Groups

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

---

Cell-Client Groups, not to be confused with Client Computer Groups\*, is a CommNet feature that allows users to create a logical group of clients comprising of any of the CommCells within the CommNet domain. Users can select specific applications for the group as well. This feature can be used to quickly and easily analyze specific applications or application types throughout the entire CommNet domain.

\*Client Computer Groups are created in and inherited from the CommCell Console for the CommCell to which the clients belong and cannot be modified in the CommNet browser.

---

# Cell-Client Groups - How To

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

---

[Add/Modify a Cell-Client Group](#)

[Remove a Cell-Client Group](#)

---

## ADD/MODIFY A CELL-CLIENT GROUP

*Required Capability:* See Capabilities and Permitted Actions

▶ To add a cell-client group:

1. From the CommNet tree, right-click the **Cell-Client Group** node, and select **New Cell-Client Group** from the popup menu.
  2. From the New Cell-Client Group dialog box, enter the:
    - General Information
      - Cell-Client Group Name
      - Description
      - Time-Zone
  3. Click **Finish**.
- 

## REMOVE CELL-CLIENT GROUP

*Required Capability:* See Capabilities and Permitted Actions

▶ To remove a cell-client group:

1. From the CommNet tree, right-click the **Cell-Client Group** you wish to delete, and select **Remove Cell-Client Group** from the popup menu. You will be prompted with a warning message asking if you wish to continue with the deletion of the cell-client group.
  2. Click **OK** to delete the group. The Cell-Client Group is now removed.
- 

[Back to Top](#)

# CommNet Views

Topics | How To

## TABLE OF CONTENTS

### Overview

#### Views

CNEAppTypeView  
 CNEBKpJobsView  
 CNEChargeBackView  
 CNEClientInfoView  
 CNEJobsSummaryView  
 CNESCSchedPolicyAssoc  
 CNESubClientContentView  
 CNESubClientInfoView  
 CNESummaryView  
 CNETimeZoneDates

## OVERVIEW

The views in CommNet provide a way to query information on the CommCell components directly from the SQL database. These views are provided in addition to the CommNet Browser Report Selection feature.

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.

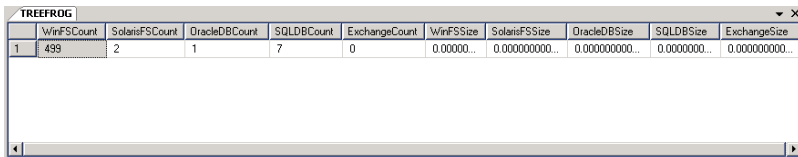
## VIEWS

The following view options are available in the CommNet.

### CNEAPPTYPEVIEW

The CNEAppTypeView provides an overview for the Agent Count and the amount of data backed up with each Agent for last 3 months.

The following image displays a sample CNEAppTypeView view:



WinFSCount	SolarisFSCount	OracleDBCCount	SQLDBCCount	ExchangeCount	WinFSSize	SolarisFSSize	OracleDBSize	SQLDBSize	ExchangeSize
1	499	2	1	7	0	0.00000...	0.0000000000...	0.0000000000...	0.0000000000...

COLUMN	DESCRIPTION
WinFSCount	Total number of windows File System Agents installed.
SolarisFSCount	Total number of Solaris File System Agents installed.
OracleDBCCount	Total number of Oracle Database Agents installed.
SQLDBCCount	Total number of SQL Database Agents installed.
ExchangeCount	Total number of Exchange Agents installed.
WinFSSize	Total amount of Windows File System data backed up in last 3 months.
Solaris FSSize	Total amount of Solaris File System data backed up in last 3 months.
OracleDBSize	Total amount of Oracle Database data backed up in last 3 months.
SQLDBSize	Total amount of SQL Database data backed up in last 3 months.
ExchangeSize	Total amount of Exchange data backed up in last 3 months.

### CNEBKPJOBVIEW

The CNEBKpJobsView provides detailed information on each job.

The following image displays a sample CNEBKpJobsView view:

ChildID	CommCellName	Pruned	TimeStart	TimeEnd	UnCompBytes	Client...	ClientName	AppType...	AppType	Inst...	
1	1004019	md7zhw	1	2009-11-20 02:05:30.000	2009-11-21 07:42:42.000	0	2	md7zhw	33	Win FS	1
2	1004019	md7zhw	1	2009-11-21 02:07:57.000	2009-11-21 07:42:43.000	0	2	md7zhw	33	Win FS	1
3	1004019	md7zhw	1	2009-11-29 02:05:15.000	2009-11-29 02:05:15.000	0	2	md7zhw	33	Win FS	1
4	1004019	md7zhw	1	2009-12-14 02:04:53.000	2009-12-14 14:48:45.000	0	2	md7zhw	33	Win FS	1
5	1004019	md7zhw	1	2009-12-17 02:04:25.000	2009-12-17 02:04:25.000	0	2	md7zhw	33	Win FS	1
6	1004019	md7zhw	1	2009-12-18 02:05:19.000	2009-12-18 02:05:19.000	0	2	md7zhw	33	Win FS	1
7	1004019	md7zhw	0	2010-01-09 02:03:10.000	2010-01-13 10:51:15.000	102364852318	2	md7zhw	33	Win FS	1

COLUMN	DESCRIPTION
CommCellName	CommCell name.
Pruned	Yes or No.
TimeStart	Start Time of backup job.
TimeEnd	End Time of backup job.
UnCompBytes	Application Size.
ClientID	Client computer.
ClientName	The client computer name.
AppTypeID	The unique ID of the Application.
AppType	Application name.
InstanceID	The unique ID of the Instance.
InstanceName	The Instance name.
BKSetID	The unique ID of backupset.
BKSetName	Backupset name.
SubClientID	The unique ID of Subclient.
SubClientName	Subclient name.
BKLevel	Full, Increment ,Diff, etc.
StatusID	Completed, Failed, Killed.
StatusName	Completed, Failed, Killed.
OpTypeID	Backup, Restore, Recover, Auxiliary copy, etc.
OpTypeName	Backup, Restore, Recover, Auxiliary copy, etc.
CommCellID	The unique ID of the CommCell.
JobID	The unique Job ID of the backup job.
WriteTime	The amount of time to write data on media.
NumOFObjects	The number of backup job objects.
Data_SPID	Data Storage Policy.
Data_SPNAME	Data Storage Policy name.
LOG_SPID	Log Storage Policy.
LOG_SPNAME	Log Storage Policy name.
DIFF_SPID	Differential Storage Policy.
DIFF_SPName	Differential Storage Policy name.
ScanFileFailures	The number of files failed to scan.
ScanFolderFailures	The number of folders failed to scan.
BackupFileFailures	The number of files failed to backup.
BackupFolderFailures	The number of folders failed to backup.

### CNECHARGEBACKVIEW

The CNEChargeBackView provides detailed information on each job for costing purposes.

The following image displays a sample CNEChargeBackView view:

CommCellName	Pruned	TimeStart	TimeEnd	UnCompBytes	ClientID	ClientName	AppTypeID
NA - admpu007m	0	2009-10-24 05:20:47.000	2009-10-24 07:06:21.000	29092405439	5	admpu012m	43
NA - admpu007m	0	2009-10-24 05:20:47.000	2009-10-24 07:06:21.000	2165723	5	admpu012m	43
NA - admpu007m	0	2009-12-12 01:26:45.000	2009-12-12 03:46:35.000	2165723	5	admpu012m	43
NA - admpu007m	0	2010-02-06 04:05:06.000	2010-02-06 04:21:05.000	2165723	5	admpu012m	43
NA - admpu007m	1	2010-02-05 21:08:48.000	2010-02-05 23:55:51.000	2165499	6	admpu009m	43
NA - admpu007m	1	2010-02-06 04:04:56.000	2010-02-06 04:38:31.000	100314965758	6	admpu009m	43

COLUMN	DESCRIPTION
CommCellName	CommCell name.
Pruned	Yes or No.
TimeStart	The time started for backup job.
TimeEnd	The time end for backup job.
UnComBytes	Backup Size.
ClientID	Client computer.
ClientName	The client computer name.
AppTypeID	The unique ID for Application.
AppType	Application name.
InstanceID	Instance.
InstanceName	The Instance name.
BKSetID	Backup set.
BKSetName	The backupset name..
SubClientID	The Subclient.
SubClientName	The Subclient name.



StatusID	Completed, Failed, Killed.
StatusName	Completed, Failed, Killed.
CommCellID	The unique ID for CommCell.
JobID	The unique Job ID of the backup job.
AuxCopyJobID	The Auxiliary copy job ID.
AttemptNumber	The job attempt number.
PhaseName	The job phase.
SPID	Storage Policy.
SPNAME	Storage Policy name.
SPCopyID	Storage Policy copy.
SPCopyName	Storage Policy copy name.
UnitCost	Unit Cost Per MB.

## CNECLIENTINFOVIEW

The CNEClientInfoView provides detailed information on client information.

The following image displays a sample CNEClientInfoView view:

1	CommCellNumber	CommCellName	ClientID	ClientName	InterfaceName	OSName	Version	DeC
1	1004019	md7zhtw	2	md7zhtw	md7zhtw	Windows Server (R) 2008 Enterprise	9.0.0	0
2	1004019	md7zhtw	14	techshare	techshare	Windows Server 2003 x64	9.0.0	0
3	1004019	md7zhtw	16	SQL1	SQL1	Windows Server 2003	9.0.0	0
4	1004019	md7zhtw	17	SQL2	SQL2	Windows Server 2003	9.0.0	0
5	1004019	md7zhtw	21	celebrity	celebrity	Windows Server 2003	9.0.0	0
6	1004019	md7zhtw	22	kystal-web	kystal-web	Windows Server 2003	9.0.0	0
7	1004019	md7zhtw	56	harold1	harold1	Windows 2000	9.0.0	0

COLUMN	DESCRIPTION
CommCellName	CommCell name.
CommCellNumber	CommCell number
ClientID	Client computer.
ClientName	The client computer name.
Interfacename	Interface name.
OSName	The client operating system name.
Version	The version number.
DeConfigured	Weather the client is de-configured or not.
TotalbkJobs	Number of total jobs.
PrunedJobs	Number of pruned jobs.

## CNEJOBSSUMMARYVIEW

The CNEJobsSummaryView provides an overview for data protection and data recovery jobs.

The following image displays a sample CNEJobsSummaryView view:

1	CommCellNumber	CommCellName	ClientID	ClientName	InterfaceName	OSName	Version	DeC
1	1004019	md7zhtw	2	md7zhtw	md7zhtw	Windows Server (R) 2008 Enterprise	9.0.0	0
2	1004019	md7zhtw	14	techshare	techshare	Windows Server 2003 x64	9.0.0	0
3	1004019	md7zhtw	16	SQL1	SQL1	Windows Server 2003	9.0.0	0
4	1004019	md7zhtw	17	SQL2	SQL2	Windows Server 2003	9.0.0	0
5	1004019	md7zhtw	21	celebrity	celebrity	Windows Server 2003	9.0.0	0
6	1004019	md7zhtw	22	kystal-web	kystal-web	Windows Server 2003	9.0.0	0
7	1004019	md7zhtw	56	harold1	harold1	Windows 2000	9.0.0	0

COLUMN	DESCRIPTION
DPJobCount	Number of Data Protection Jobs.
DPScsessHobCount	Number of Completed Data Protection Jobs.
DPFailedorKilledJobCount	Number of Failed or Killed Data Protection Jobs.
DPPrimaryDataSize	Total Data on the primary copy.
DRJobCount	Number of Data Recovery Jobs.
DRSuccessJobCount	Number of Completed Data Protection Jobs.
DRFailedorKilledJobCount	Number of Failed or Killed Data Protection Jobs.

## CNESCSCHEDPOLICYASSOC

The CNESCSChedPolicyAssoc view provides detailed information on Schedule Policies the Subclient is associated with.

The following image displays a sample CNESCSChedPolicyAssoc view:

ChildID	CommCellName	ClientID	ClientName	AppTypeID	AppTypeName	InstanceID	InstanceName	BackupSetID	BackupsetName
1	1004019	md7zhtw	2	md7zhtw	33	Win FS	1	3	defaultBackupSet
2	1004019	md7zhtw	2	md7zhtw	33	Win FS	1	1978	SIL0_BackupSet_SP_B_Primary
3	1004019	md7zhtw	2	md7zhtw	33	Win FS	1	1978	SIL0_BackupSet_SP_B_Primary
4	1004019	md7zhtw	2	md7zhtw	33	Win FS	1	1979	SIL0_BackupSet_SP_C_Primary
5	1004019	md7zhtw	2	md7zhtw	33	Win FS	1	1979	SIL0_BackupSet_SP_C_Primary
6	1004019	md7zhtw	2	md7zhtw	33	Win FS	1	1980	SIL0_BackupSet_SP_D_Primary
7	1004019	md7zhtw	2	md7zhtw	33	Win FS	1	1980	SIL0_BackupSet_SP_D_Primary

COLUMN	DESCRIPTION
ChildID	The unique ID for CommCell.
CommCellName	CommCell name.
ClientID	Client computer.
ClientName	The client computer name.
AppTypeID	The unique ID for Application.
AppType	Application name.
InstanceID	Instance.
InstanceName	The Instance name.
BKSetID	Backupset.
BKSetName	The backupset name.
SubClientID	The Subclient.
SubClientName	The Subclient name.
SchedPolicyID	The Schedule Policy ID.
SchedPolicyName	The Schedule Policy name.
BackupType	Full, Increment, Diff, etc.
BackupTypeStr	Full, Increment, Diff, etc.
AssocLevel	Client Level, Agent Level, etc.
AssocLevelStr	Full, Increment, Diff, etc.
SchedulePattern	One Time, Daily, Weekly, Monthly or Yearly.
TimeZone	Schedule TimeZone.

### CNESUBCLIENTCONTENTVIEW

The CNESubClientContentView provides an information on data path entries to the contents of a subclient.

The following image displays a sample CNESubClientContentView view:

ChildID	SubClientID	Content	
1	1004019	2	C:\Test1
2	1004019	2407	\
3	1004019	2408	\
4	1004019	1346	\
5	1004019	1569	\
6	1004019	1570	X:\Depts
7	1004019	1590	X:\Depts\CISER

COLUMN	DESCRIPTION
ChildID	The unique ID for CommCell.
SubClientID	The unique ID of Subclient.
Content	Data path entry to the contents of a subclient.

### CNESUBCLIENTINFOVIEW

The CNESubClientInfoView provides detailed information on subclient information.

The following image displays a sample CNESubClientInfoView view:

ChildID	ChildName	ClientID	ClientName	AppTypeID	AppTypeName	InstanceID	InstanceName	BackupSetID	BackupSetName	SubClientID
1	1004019	md7zhtw	39	bigblack-box	11	Windows 2000 File System	1	82	defaultBackupSet	121
2	1004019	md7zhtw	39	bigblack-box	11	Windows 2000 File System	1	82	defaultBackupSet	123
3	1004019	md7zhtw	26	picruiser	11	Windows 2000 File System	1	53	defaultBackupSet	60
4	1004019	md7zhtw	26	picruiser	11	Windows 2000 File System	1	53	defaultBackupSet	82
5	1004019	md7zhtw	49	delorean	11	Windows 2000 File System	1	102	defaultBackupSet	151
6	1004019	md7zhtw	49	delorean	11	Windows 2000 File System	1	102	defaultBackupSet	153
7	1004019	md7zhtw	56	harold1	11	Windows 2000 File System	1	116	defaultBackupSet	172

COLUMN	DESCRIPTION
ChildID	The unique ID for CommCell.
ChildName	The unique name for CommCell.
ClientID	Client computer.
ClientName	The client computer name.
AppTypeID	The unique ID for Application.
AppTypeName	Application name.
InstanceID	The unique ID of the Instance.
InstanceName	The Instance name.
BackupSetID	The unique ID of backupset.

BackupSetName	Backupset name.
SubClientID	The unique ID of Subclient.
SubClientName	Subclient name.
Created	Subclient created.
Modified	Modified data protection activity.
NextFullBackup	Time of the next Full Backup
NextIncrBackup	Time of the next Increment Backup
NextDiffBackup	Time of the next Differential Backup
SPName	Storage Policy name.
Scheduled	Provides subclient data protection schedules.
Deleted	Provides subclient data protection deleted time.
Encryption	Provides data encryption for a selected content.
DataProtActivity	Data Protection Activity of a Subclient.

## CNESUMMARYVIEW

The CNESummaryView provides an overview of the entities (Client, iDataAgent and Libraries) count present.

The following image displays a sample CNESummaryView view:

NumCommCells	NumClients	NumAgents	NumSubClients	NumMediaAgents	NumLibraries	NumDrives	NumLicenses
1	614	628	814	28	12	39	139

COLUMN	DESCRIPTION
NumCommCells	Total number of CommCells registered
NumClients	Total number of Clients
NumAgents	Total number of Agents
NumSubClients	Total number of SubClients
NumMediaAgents	Total number of MediaAgents
NumLibraries	Total number of Libraries
NumDrives	Total number of Drives
NumLicenses	Total number of Licenses

## CNETIMEZONEDATES

The CNETimeZoneDates view provides information on time zones. This is populated when the service starts for +10 and -10 years in the CommNet Database.

The following image displays a sample CNETimeZoneDates view:

ChildID	CommCellName	Year	TimeZoneName	TimeZoneStdName	DSTFlag	Bias	STDBias	STDDate	DSTBias	DSTDate	
1	1004019	md7zhtw	2000	(GMT+08:00) Taipei	Taipei Standard Time	0	28800	0	1970-01-01 00:00:00.0000	0	1970-01-
2	1004019	md7zhtw	2001	(GMT+08:00) Taipei	Taipei Standard Time	0	28800	0	1970-01-01 00:00:00.0000	0	1970-01-
3	1004019	md7zhtw	2002	(GMT+08:00) Taipei	Taipei Standard Time	0	28800	0	1970-01-01 00:00:00.0000	0	1970-01-
4	1004019	md7zhtw	2003	(GMT+08:00) Taipei	Taipei Standard Time	0	28800	0	1970-01-01 00:00:00.0000	0	1970-01-
5	1004019	md7zhtw	2004	(GMT+08:00) Taipei	Taipei Standard Time	0	28800	0	1970-01-01 00:00:00.0000	0	1970-01-
6	1004019	md7zhtw	2005	(GMT+08:00) Taipei	Taipei Standard Time	0	28800	0	1970-01-01 00:00:00.0000	0	1970-01-
7	1004019	md7zhtw	2006	(GMT+08:00) Taipei	Taipei Standard Time	0	28800	0	1970-01-01 00:00:00.0000	0	1970-01-

COLUMN	DESCRIPTION
ChildID	The unique ID for CommCell.
CommCellName	CommCell name.
Year	Year.
TimeZoneName	TimeZone name.
TimeZoneStdName	TimeZone standard name.
DSTFlag	Day Light Saving Flag is set or not.
Bias	Difference with GMT ( For Eastern Time Zone (GMT-05).
STDBias	Standard Bias.
STDDate	Standard date.
DSTBias	Day Light Saving Bias is set or not.
DSTDate	Day Light Saving Date is set or not.

Back to Top

# CommNet Views - How To

- Topics
- How To

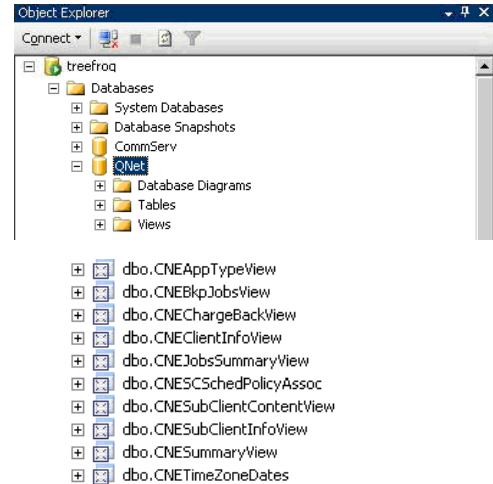
## ACCESS COMMNET VIEWS

This section describes the steps involved in accessing the CommNet Views using **SQL Server Management Studio**.

▶ To access the CommNet 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.



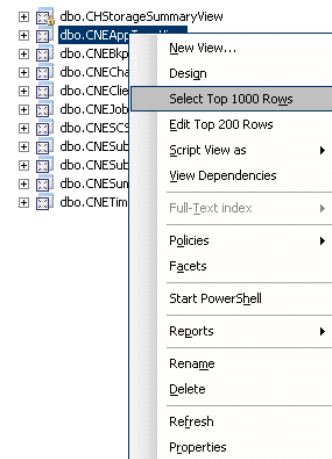
2. By expanding the tree in the left pane, go to the following location: <CommServe computer name\database\_instance\_name> | **Databases | QNet | Views**.

The available CommNet Views are listed in the right pane.

**NOTES**

- For a cluster, instead of the database instance, there will be a default or Named instance.

3. To open a view, right-click the view and then select **Select Top 1000 Rows**.



**DISCLAIMER**

Products in Germany are not distributed using the "QNet" brand.

In Deutschland werden keine Produkte der Marke "QNet" mehr vertrieben.

# CommNet Clients

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

---

[Overview](#)

[Client Tasks](#)

---

## OVERVIEW

The Client nodes in a CommCell provides vital information about the client which helps you to analyze the various aspects of the client's primary storage and secondary storage data growth.

In the client summary page, for primary storage, the date and time at which the most recent information was obtained from the SRM Server about the client is displayed in the **Primary Storage** section of the Client Summary. For secondary storage, the date and time at which the most recent information was obtained from the CommCell about the client, is displayed in the **Secondary Storage** section of the Client Summary. If you wish to obtain a more up-to-date information of the Client, you can synchronize the Cell associated with the client, as described in Synchronize Cells.

If the client is part of a CommCell, and is uninstalled (but not hard deleted), the client will be displayed as dimmed in the CommNet Browser.

---

## CLIENT TASKS

Information regarding important aspects of a client can be obtained using the tasks available from the **Client Tasks** section of the CommNet Browser.

If this client is part of a CommCell only, the following tasks are available:

- Secondary Storage Client Data Growth
- Secondary Storage Subclient Data Growth
- SLA
- Client Summary

If this client is part of a CommCell that has SRM Server, the following tasks are available:

- Primary Storage Client Data Growth
- Secondary Storage Client Data Growth
- Secondary Storage Subclient Data Growth
- SLA
- Client Summary

At the CommCell node, you can view the various attributes of all the clients with a CommCell from the Client Status task from the **CommCell Tasks** section of the CommNet Browser.

---

[Back to Top](#)

# Client Computer Groups

[Topics](#) | [Tasks](#) | [Related Topics](#)

---

Client Computer Groups are created in and inherited from the CommCell Console for the CommCell to which the clients belong and cannot be modified in the CommNet browser. A client computer group is a logical grouping of client computers that serves as a single CommCell entity in which selected options can apply to all member clients. Hence, the need to configure options for individual clients is eliminated once those clients are members of the group. Client Computer Groups cannot be modified in the CommNet Browser.

---

# CommNet Data Collection

Topics | How To

---

Overview

Cell Synchronization

---

## OVERVIEW

The CommNet Server monitors the CommCells that are registered in the CommNet Server. Data Collection can be done in two different ways:

**Automatically** - The software enables automatic data collection from Cells with a standard value. The default values can be changed to suit your requirements. As soon as the CommCell is registered, the system automatically downloads the data from the registered CommCell into the CommNet Server.

**Scheduling a Data Collection Policy** - Data Collection Policy allows specifying how often the system must automatically collect data from each CommCell at specified intervals. The system automatically synchronizes the data between the CommNet Server and the registered cells every 4 hours. The CommNet Server gathers vital information from the CommCell based on the frequency established in the Data Collection Policy.

You may perform the following tasks:

- Disable Data Collection, see Enable or Disable Data Collection for step-by-step instructions.
  - Manually Synchronize Cells, see Synchronize Cells for step-by-step instructions.
  - Configure Data Collection Policy, see Configure the Data Collection Policy for step-by step instructions.
- 

## CELL SYNCHRONIZATION

On a selected CommCell, the following information gets synchronized:

- Configuration information including:
    - Client information
    - MediaAgent information
    - Library information
    - Job history
    - Media Management history
    - Resource view update information
    - Load Report information (data necessary to generate report)
  - Information associated with the CommCell jobs
  - Events associated with the CommCell jobs
- 

# CommNet Data Collection - How To

Topics | How To

---

Enable or Disable Data Collection

Configure the Data Collection Policy

---

## ENABLE OR DISABLE DATA COLLECTION

*Required Capability:* See Capabilities and Permitted Actions

▶ To enable or disable data collection:

1. On the **Setup** menu, click **Cell Data Collection Policy**.
2. From the Cell Data Collection Policy dialog box, either select or clear **Data Collection Enabled**.
3. Click **OK** to save changes.

If the data collection for Cells fails, the data collection will be retried for 30 minute intervals.

## CONFIGURE THE DATA COLLECTION POLICY

*Required Capability:* See Capabilities and Permitted Actions

▶ To configure Data Collection Policy to obtain Configuration information:

1. On the **Setup** menu, click **Cell Data Collection Policy**.
2. From the Cell Data Collection Policy dialog box, click the arrow to set the time and the time frame (hours or minutes) in the **Configuration/Alerts Update/Job Controller Update/Event Viewer Update/Data Replication Monitor Update/Vault Tracker** boxes.
3. Click **OK** to save changes.
  - The updates are provided by the individual Cells and hence the update time is based on the CommCell time.
  - For CommCell Alerts update, if the Data Collection Policy is changed for multiple CommCells, the minimum time frame that was selected for these CommCells will be used for the alert detection. For example, if a time frame of 20 minutes is selected for CommCell A, and a time frame of 30 minutes is selected for CommCell B, then the time frame of 20 minutes will be used to detect alerts for both CommCells.

---

[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.

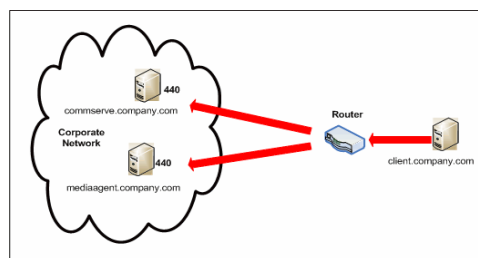
## OPERATING USING DIRECT CONNECTIONS

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.



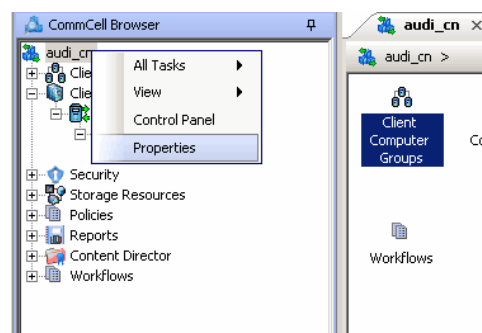
Review the following considerations before you begin.

- 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.

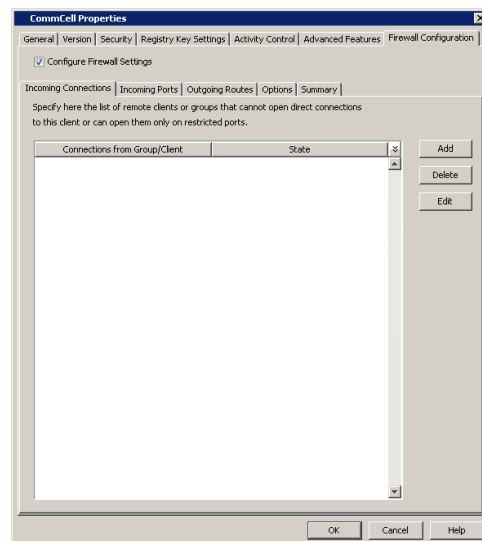
### SETUP CONNECTION TO THE COMMSERVE

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.

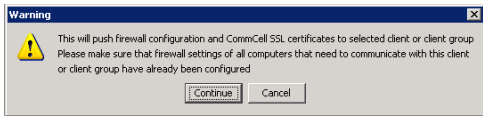
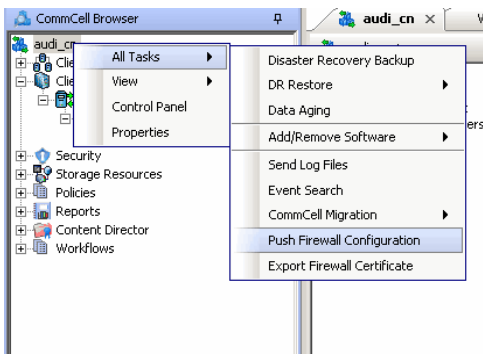
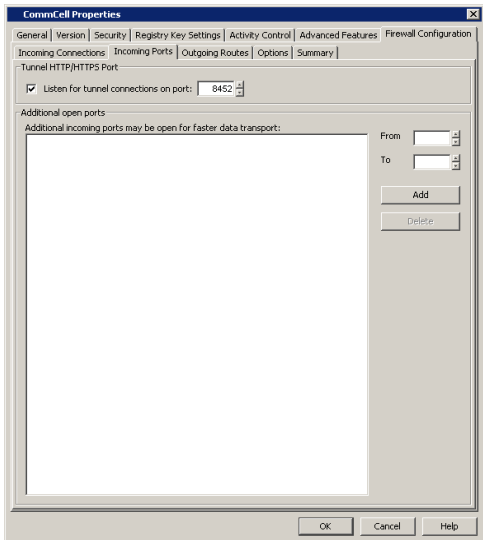
1. From the CommCell Console, right-click the CommServe computer and click **Properties**.



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**.



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**

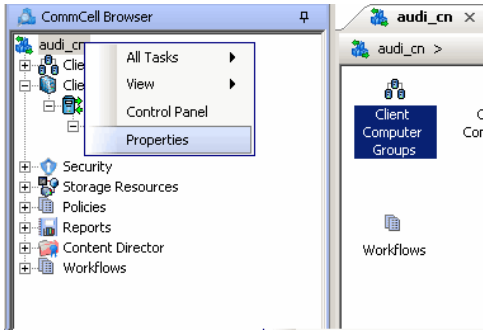
In this configuration the client establishes connection with the CommServe using one or more ports. To install the client across a firewall in this setup, you will have to specify the path to reach the CommServe computer. During installation of the client, use one of the following firewall configuration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

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, 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.

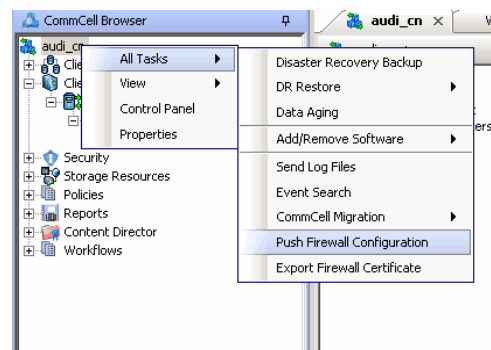
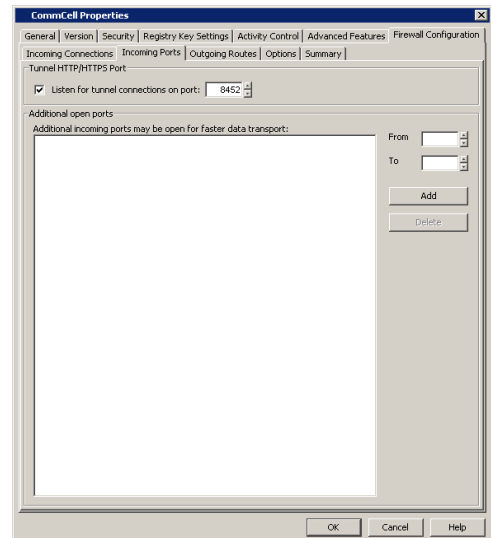
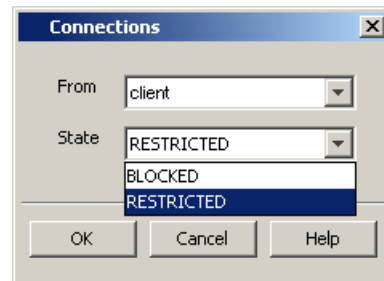
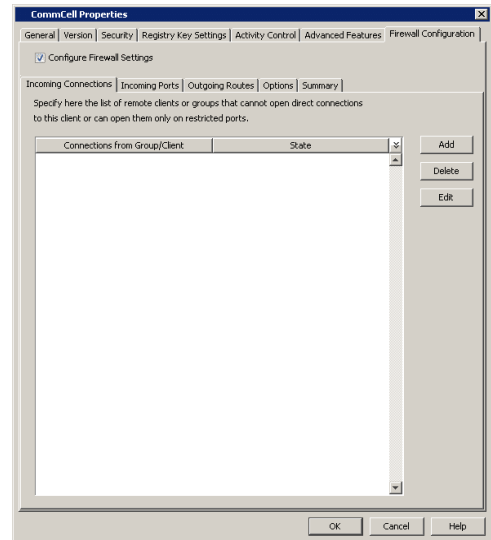
Review the following recommendations.

- 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.

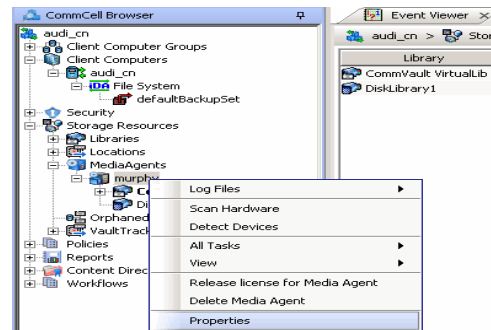
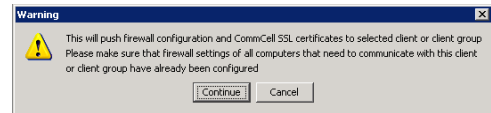
7. Click **Continue**.



The CommServe is configured to receive communication from the client.

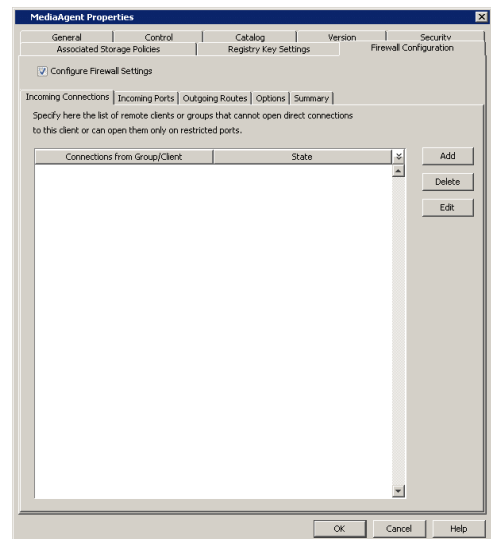
Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.

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



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

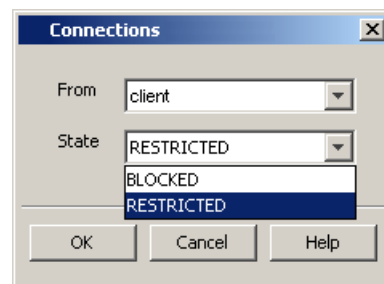
10. From the **Incoming Connections** tab, click **Add**.



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.

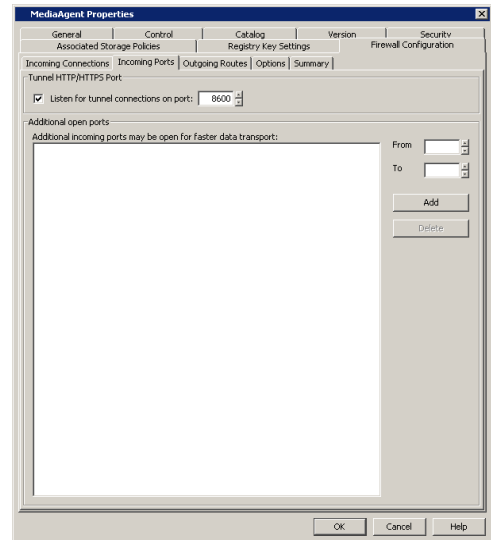
Review the following recommendations.

- 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

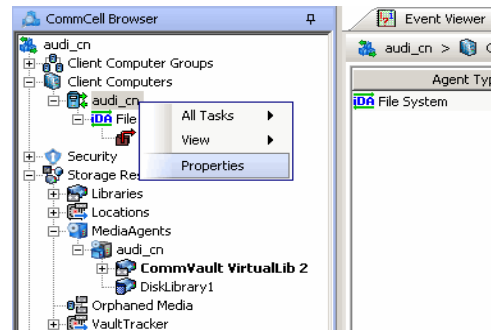
improves the backup performance.

- 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.

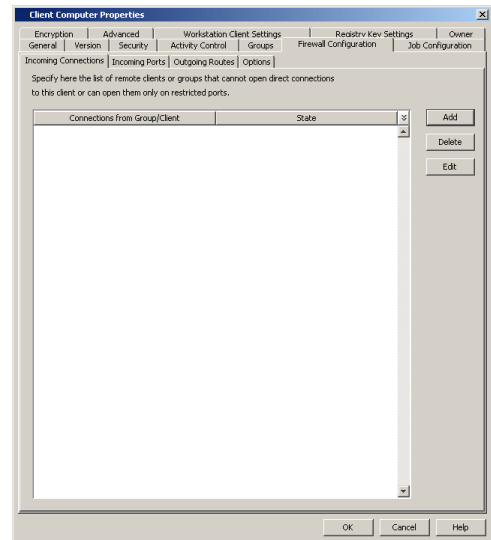


13. To configure the Client, right-click the client computer from the CommCell Console and click **Properties**.

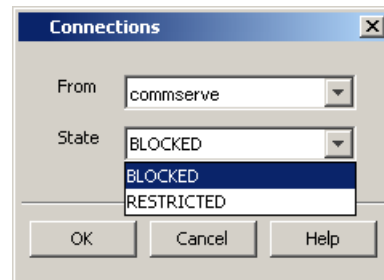


14. Click the **Firewall Configuration** tab.

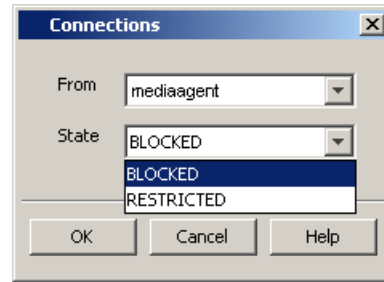
15. From the **Incoming Connections** tab, click **Add**.



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**.



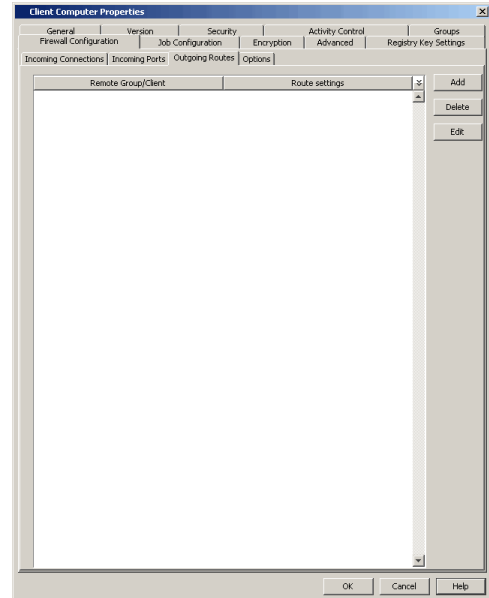
- 17.
- Click **Add** again to specify the MediaAgent connection details.
  - In the **From** field, specify the name of the MediaAgent computer.
  - In the **State** field, select **Blocked**, since the MediaAgent cannot open connections to the Client.
  - Click **OK**.



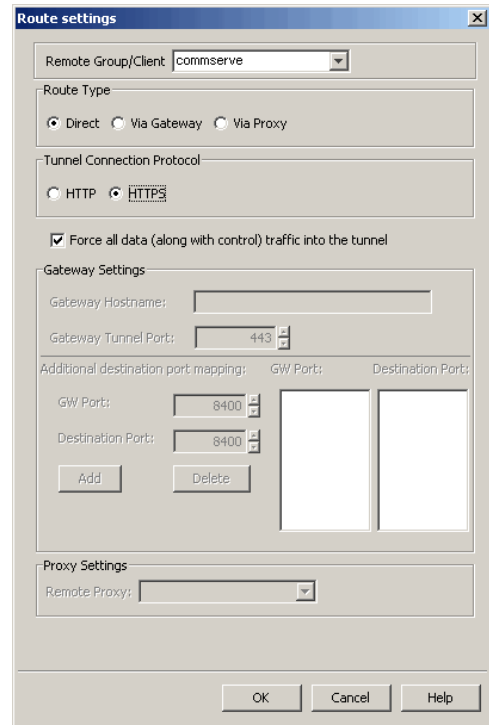
- 18.
- Click the **Outgoing Routes** tab.
  - Click **Add**.

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**.

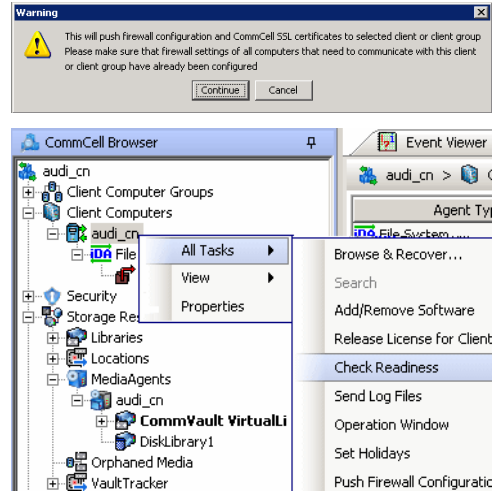


20. From the CommCell Console, right-click the client computer and click **All Tasks | Push Firewall Configuration**. This updates the firewall configuration files on the client computer.

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.

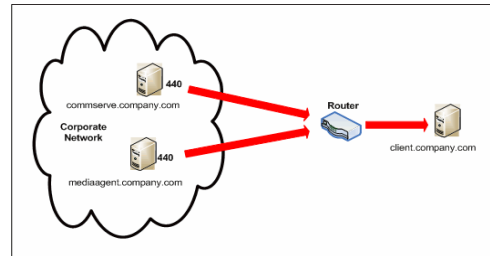


Connectivity between CommServe, MediaAgent, and the client is now established.

### 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.



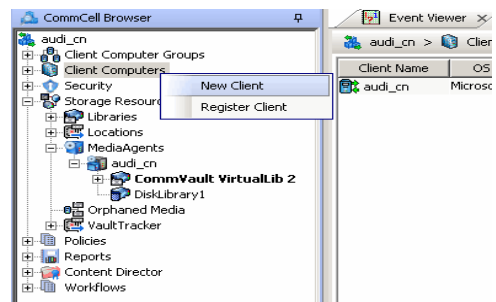
Review the following considerations before you begin.

- 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.

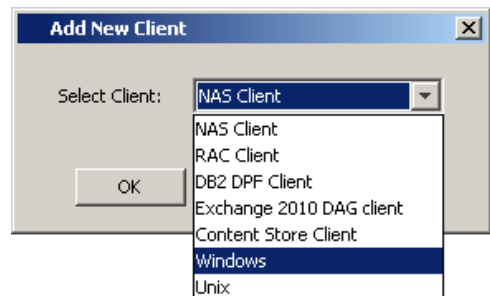
### SETUP CONNECTION TO THE COMMSERVE

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**.

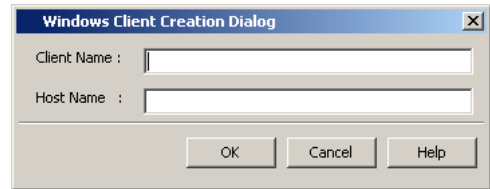


- Select **Windows** or **Unix** as applicable.





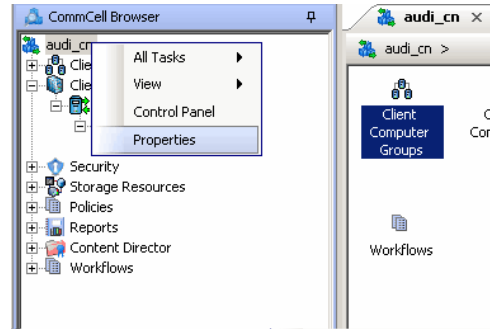
3. Provide the **Client Name** and the **Host Name** of the client computer to be installed.
  - The Client Name must be the same client name that you will provide during the client installation — the name by which the client will be identified in the CommCell Browser after installation. Ensure to provide 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**.

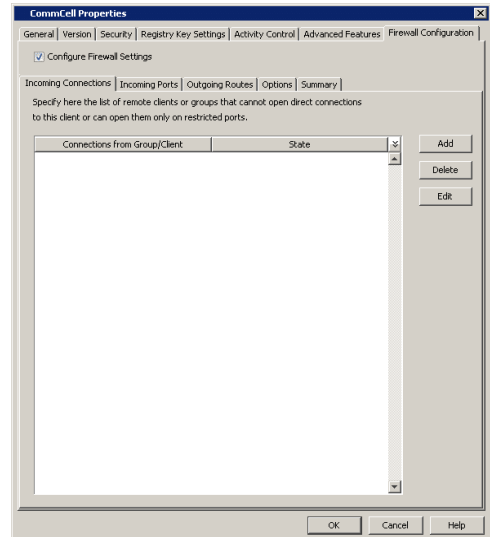
A placeholder client is created for firewall configuration use.

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

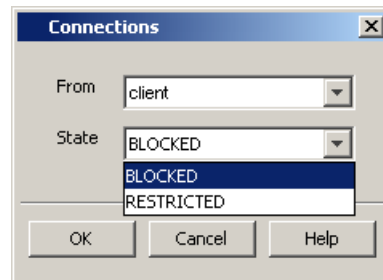


5. Click the **Firewall Configuration** tab.

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**.



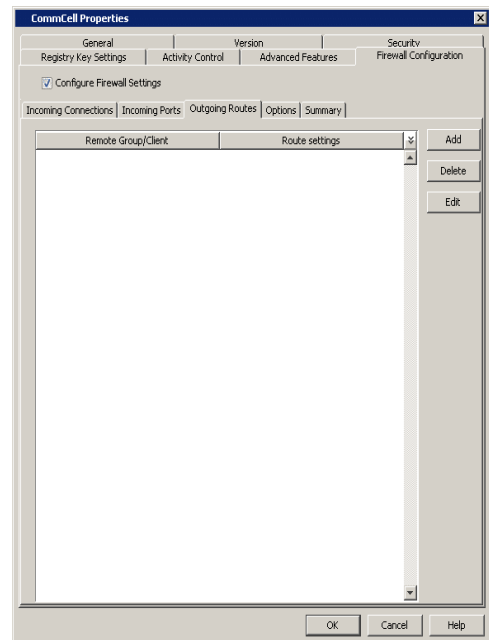
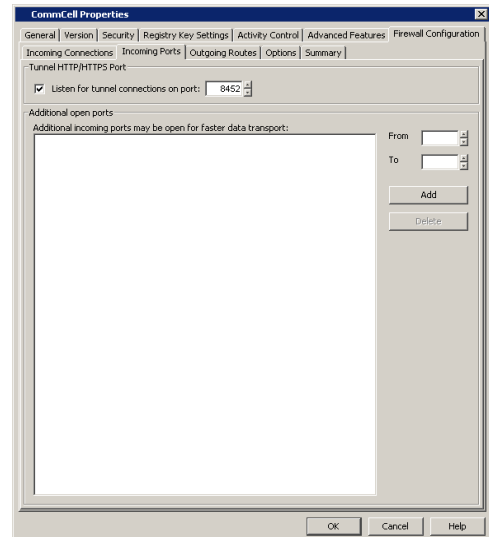
8.
  - Click the **Incoming Ports** tab.
  - As the CommServe does not receive connections from the client, not need to select **Listen for tunnel connections on port**.

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.

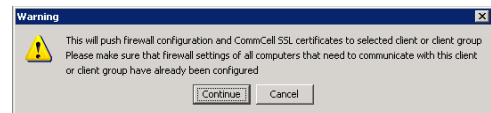
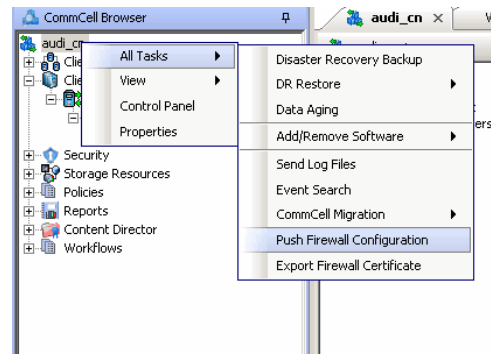
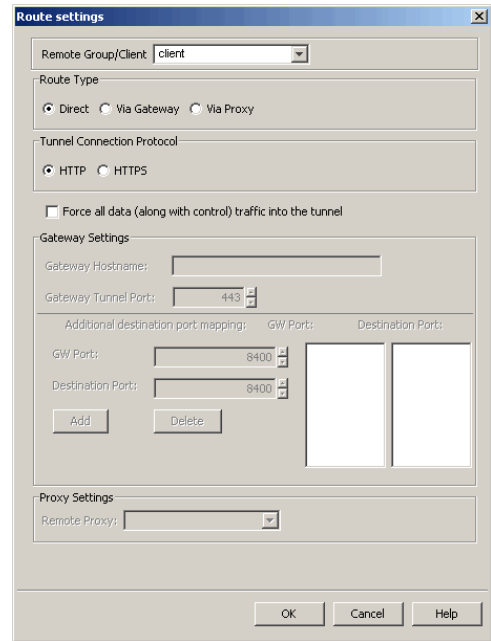
- Select the name of the placeholder client in **Remote Group/Client**.
- Select **Direct**.
- Select **HTTP**.
- **Force all data (along with control) traffic into the tunnel** option is not required as this route is not toward MediaAgent.
- Click **OK**.

- 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)

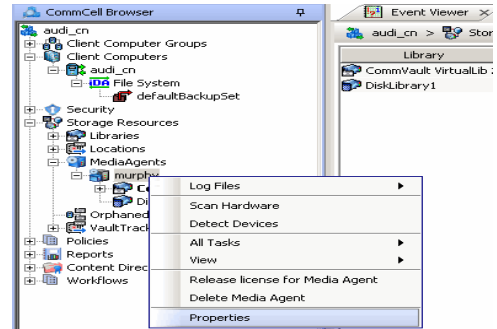
### CONFIGURE THE COMMSERVE, MEDIAAGENT AND CLIENT

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**.

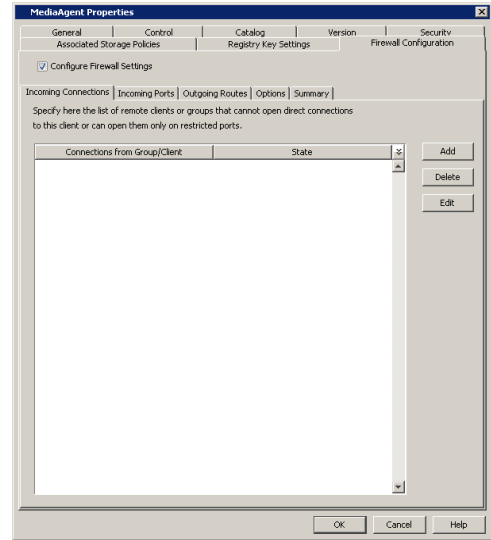
2. Click the **Firewall Configuration** tab.
3. From the **Incoming Connections** tab, click **Add**.



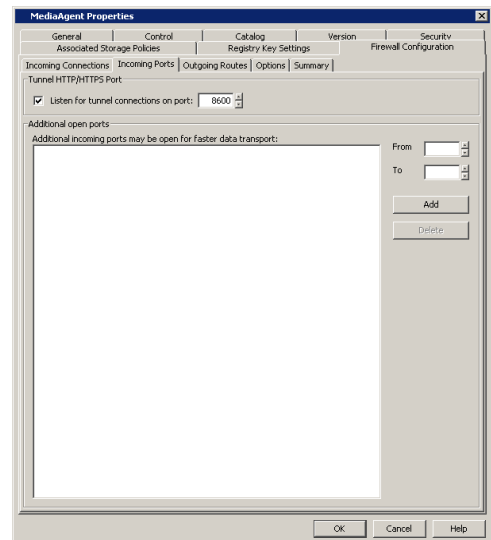
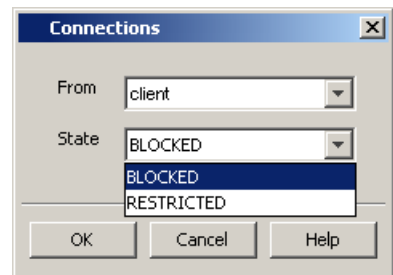
4.
  - In the **From** field, select the name of the client you just installed.
  - In the **State** field, select **Blocked**, since the MediaAgent does not open tunnel connection to the client.

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

  - Click **OK** to continue.



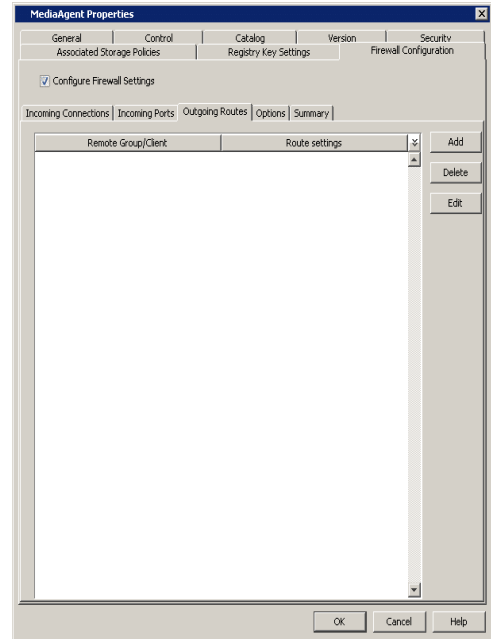
5.
  - Click the **Incoming Ports** tab.
  - Assuming that the MediaAgent opens tunnel connection to the client, there is no need to select **Listen for tunnel connections on port**.
  - Click **OK**.



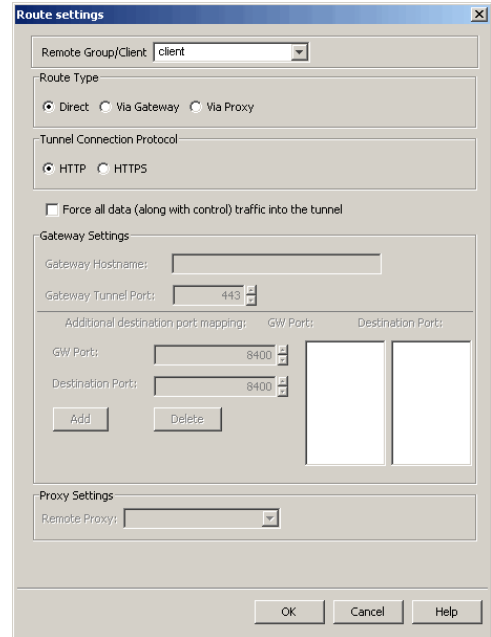
6.
  - Click the **Outgoing Routes** tab.
  - Click **Add** to specify the outgoing route toward the proxy.

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.

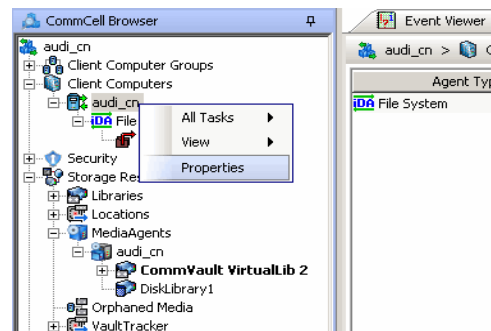
  - Enable HTTPS encryption for the tunnel or data traffic.
  - Encrypt the data connections by forcing the connections into the tunnel. However, consider the following before using this option.
    - Direct connections always work faster. Forcing data connections into the tunnel might degrade performance 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**.

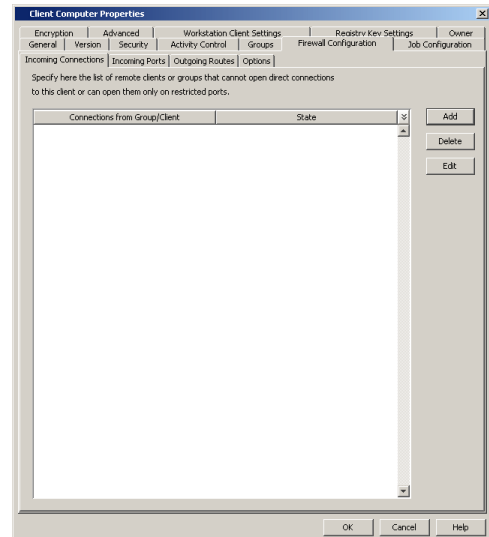


8. From the **Outgoing Routes** tab, click **OK**.  
The MediaAgent is now configured to communicate with the client.
9. To configure the Client, right-click the client computer from the CommCell Console and click **Properties**.

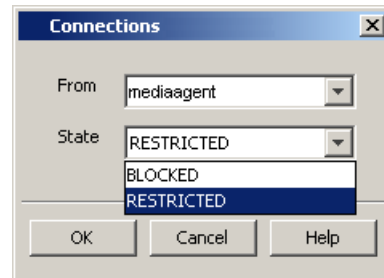
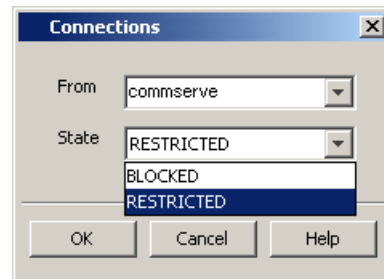


10. Click the **Firewall Configuration** tab.
11. From the **Incoming Connections** tab, click **Add**.

- 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**.



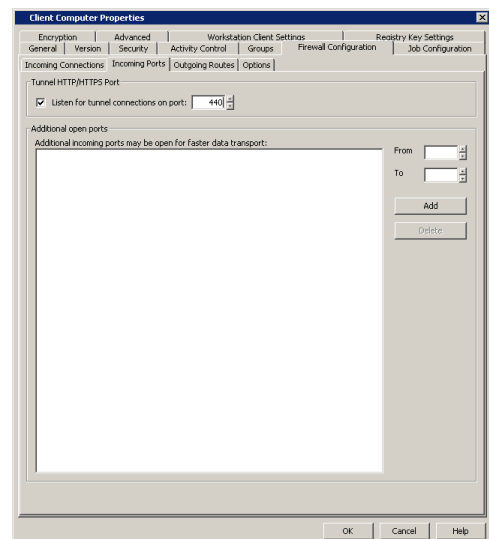
- 13.
- Click **Add** again to specify the MediaAgent connection details.
  - In the **From** field, select the name of the MediaAgent computer.
  - In the **State** field, select **Restricted**, since the MediaAgent will connect to the Client through a port.
  - Click **OK**.



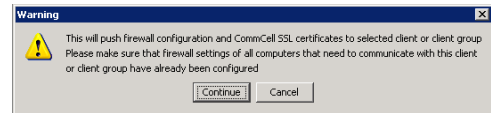
- 14.
- Click the **Incoming Ports** tab.
  - Select **Listen for tunnel connections on port** and specify the incoming port number on which the firewall will allow connections from the CommServe and the MediaAgent.
  - **Additional Open Ports:** You can speed up the data transfer by opening additional 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.

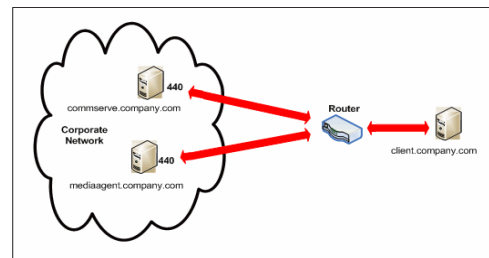


Connectivity between CommServe, MediaAgent, and the client is now established.

### 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.



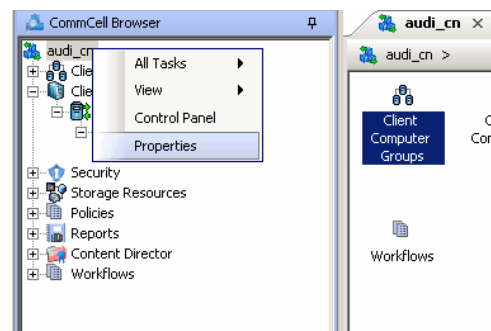
Review the following considerations before you begin.

- 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.

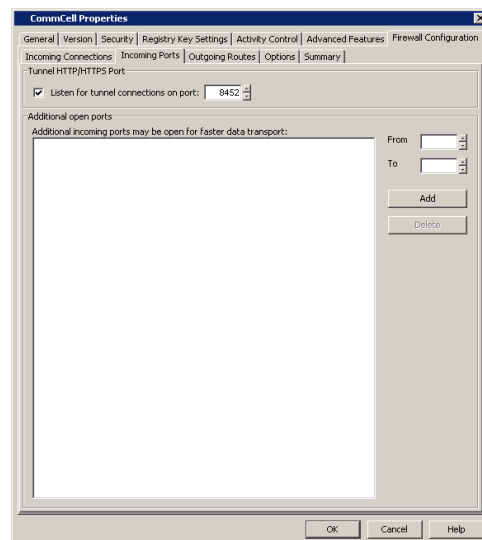
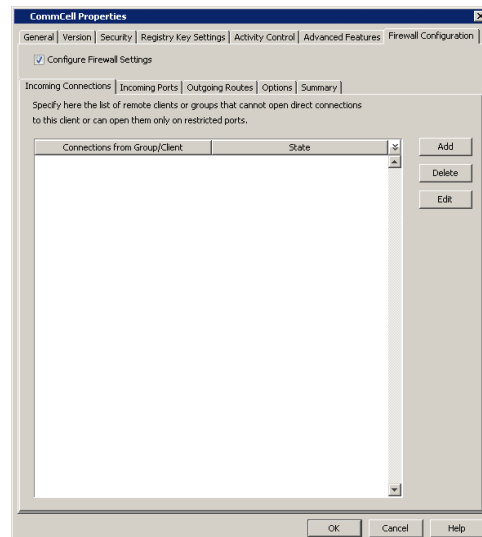
### SETUP CONNECTION TO THE COMMSERVE

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.

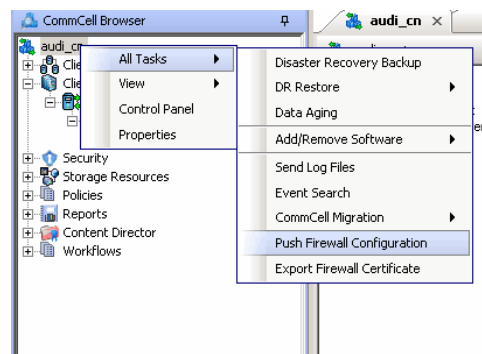
1. From the CommCell Console, right-click the CommServe computer and click **Properties**.
2. Click the **Firewall Configuration** tab.



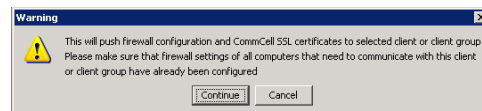
3.
  - Click the **Incoming Ports** tab.
  - Select **Listen for tunnel connections on port** and specify the port number on which the incoming tunnel connection is received.
  - Click **OK**.



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)

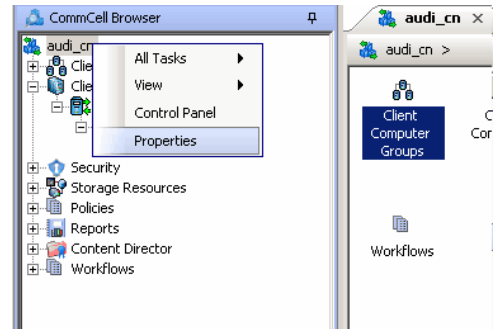


- Client/MediaAgent and CommServe can reach each other (Unix clients)

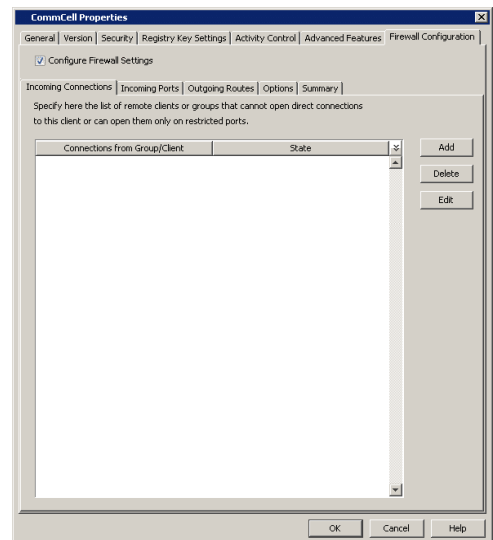
**CONFIGURE THE COMMSERVE, MEDIAAGENT AND CLIENT**

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

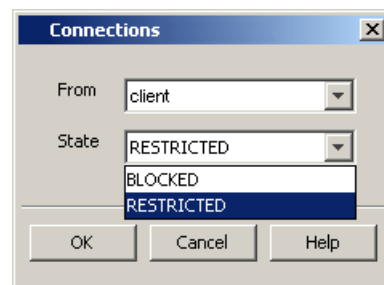
1. To configure the CommServe, right-click the CommServe computer from the CommCell Console and click **Properties**.



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**.



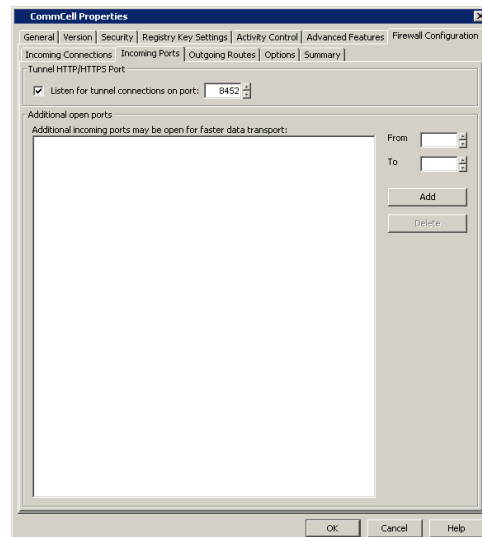
5.
  - Click the **Incoming Ports** tab. You will see the tunnel port already specified on the CommServe.
  - **Additional Open Ports:** For components that handle data transfer (for example, MediaAgent, File System iDataAgent, etc.), you can speed up the data transfer by opening additional ports on 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.

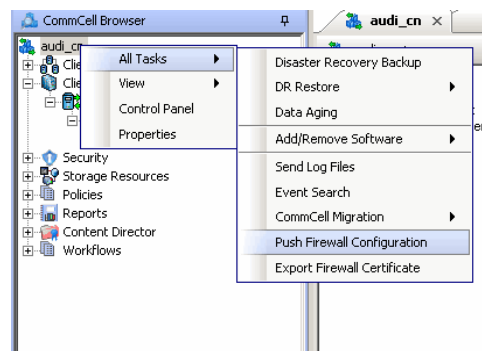
- For MediaAgents involving multi-stream restores, opening additional ports increases the restore performance. The number of open ports should correspond to the number of simultaneously running restore streams.
- For MediaAgents with **Optimize for concurrent LAN backups** option enabled, opening the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



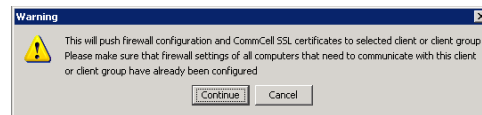
6. From the CommCell Console, right-click the CommServe computer and click **All Tasks | Push Firewall Configuration**.



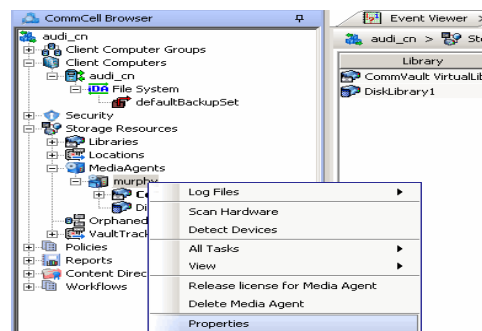
7. Click **Continue**.

The CommServe is configured to receive communication from the client.

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



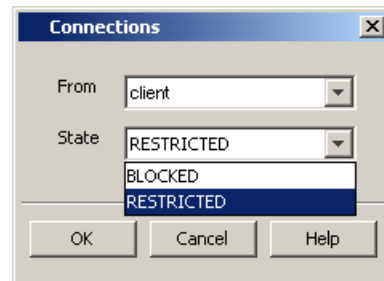
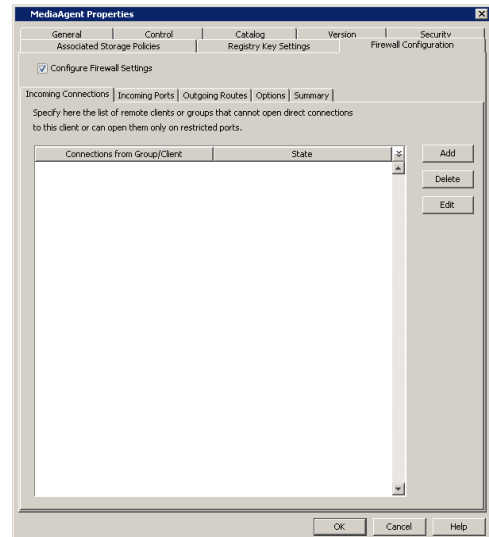
8. To configure the MediaAgent, right-click the MediaAgent computer from the CommCell Console and click **Properties**.



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.

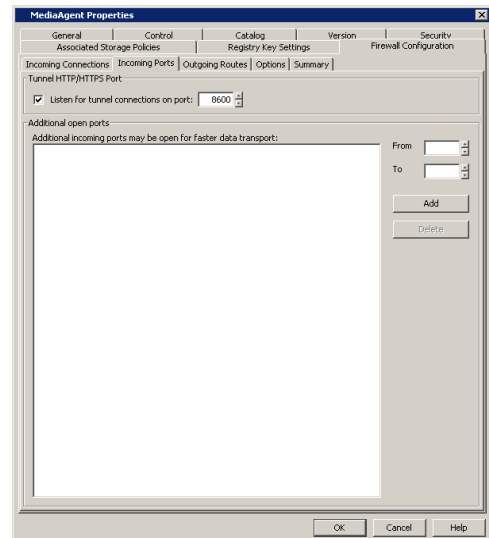
Review the following recommendations.

- 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**.

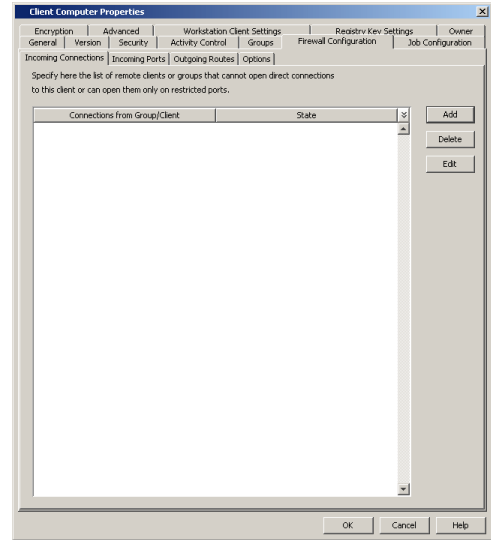
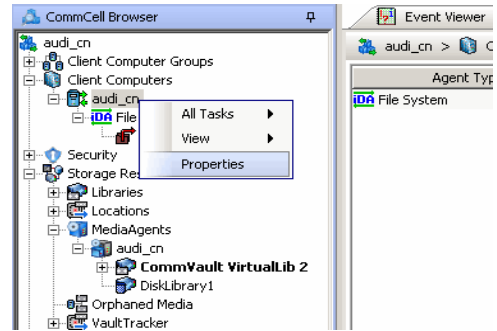
The MediaAgent is now configured to receive communication from the client.

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

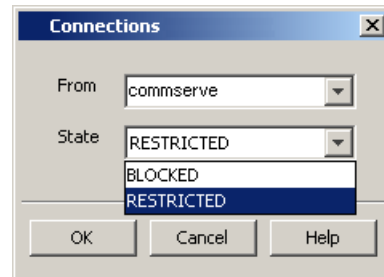


14. Click the **Firewall Configuration** tab.

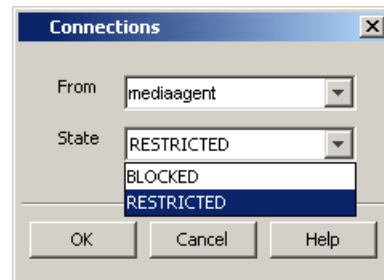
15. From the **Incoming Connections** tab, click **Add**.



- 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**.



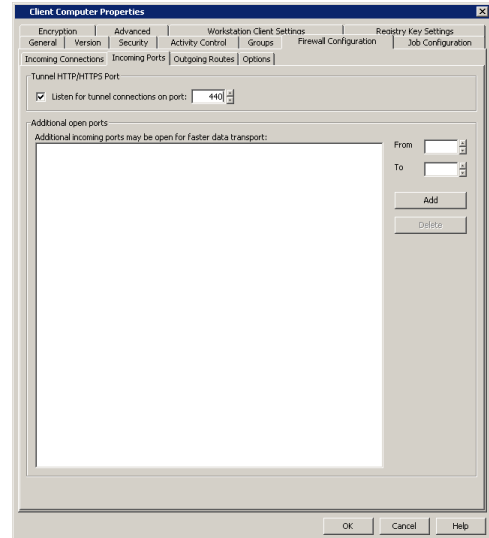
- 17.
  - Click **Add** again to specify the MediaAgent connection details.
  - In the **From** field, specify the name of the MediaAgent computer.
  - In the **State** field, select **Restricted**, since the Client can connect to the MediaAgent.
  - Click **OK**.



- 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.

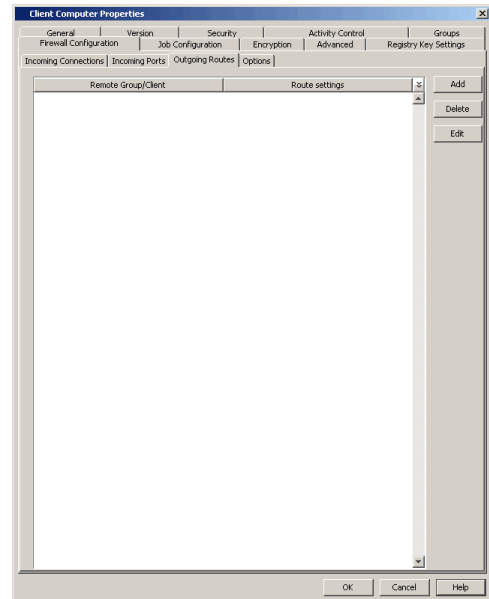
- For backups to MediaAgents with **Optimize for concurrent LAN backups** option unchecked, opening additional incoming ports improves the backup performance. The number of open ports should correspond to the number of simultaneously running backup streams.
- For ContinuousDataReplicator and Workstation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



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

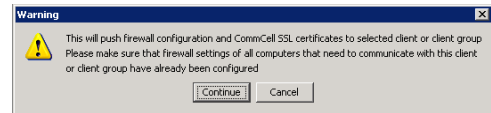
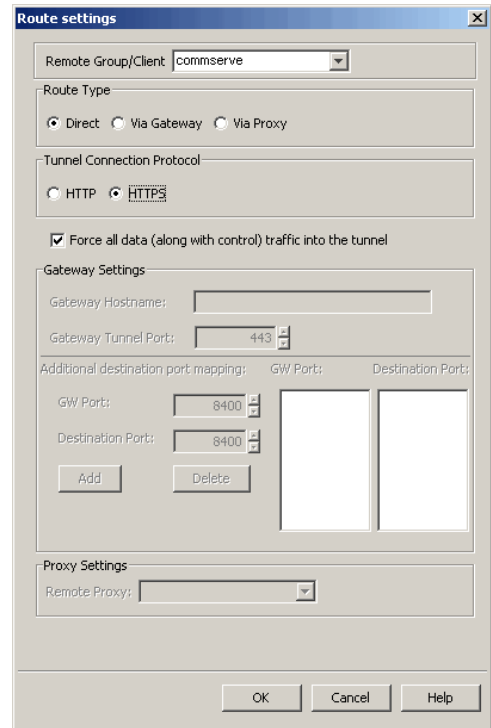
Outgoing routes are automatically created in the direct connectivity setup — manual entry is not required. However, you might want to create an entry if you wish to achieve one of the following.

- 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.



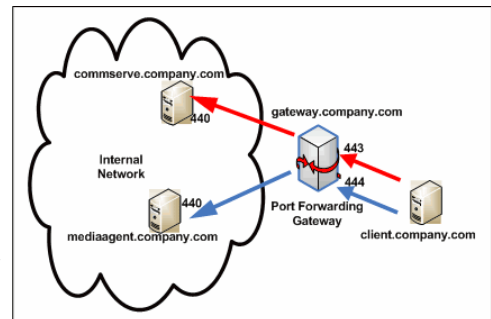
Connectivity between CommServe, MediaAgent, and the client is now established.

## 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.

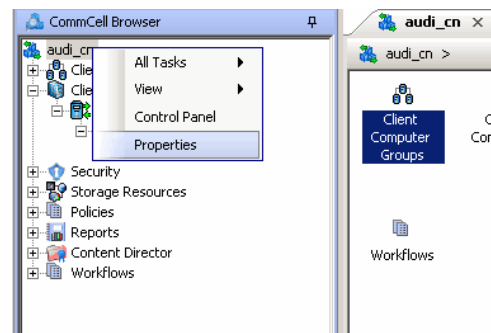
Note that there is no restriction on the internal port numbers. They need not be the same as shown in the illustration. Also, for machines in the internal network, neither the IP addresses nor the names have to be reachable or resolvable from outside.

---

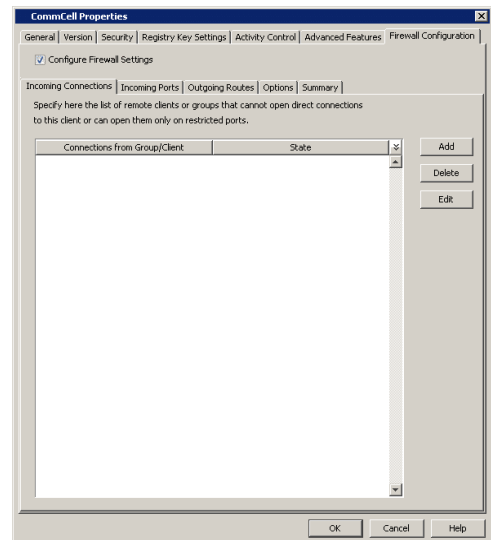
## SETUP CONNECTION TO THE COMMSERVE

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.

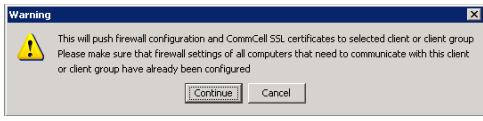
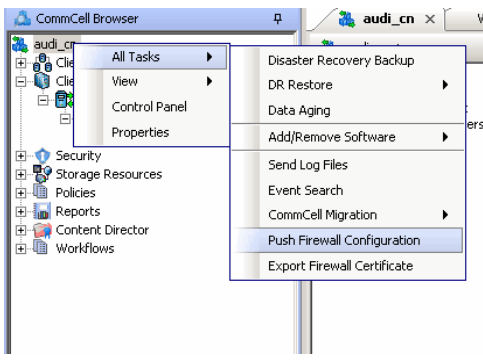
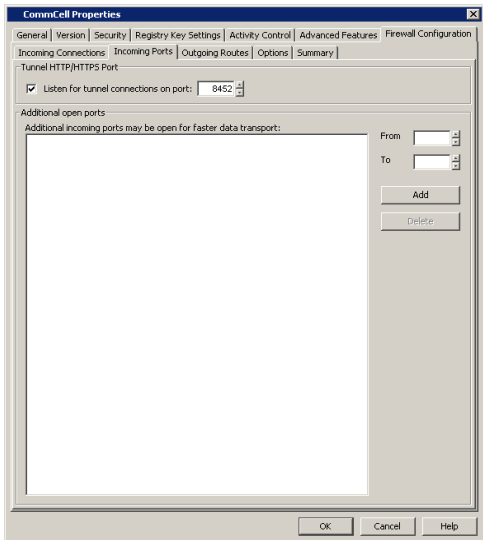
1. From the CommCell Console, right-click the CommServe computer and click **Properties**.



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**.



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**

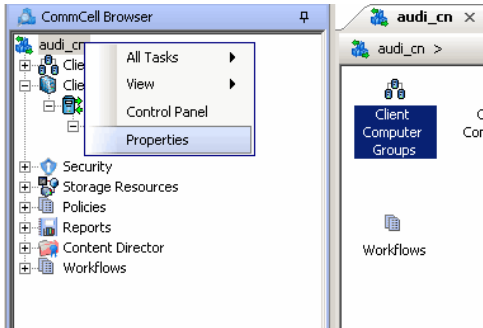
See Installation for step-by-step installation procedures to install the client.  
During installation, provide the gateway information through which the CommServe computer can be reached. The install program communicates to the CommServe using this information. Use one of the following firewall configuration 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**

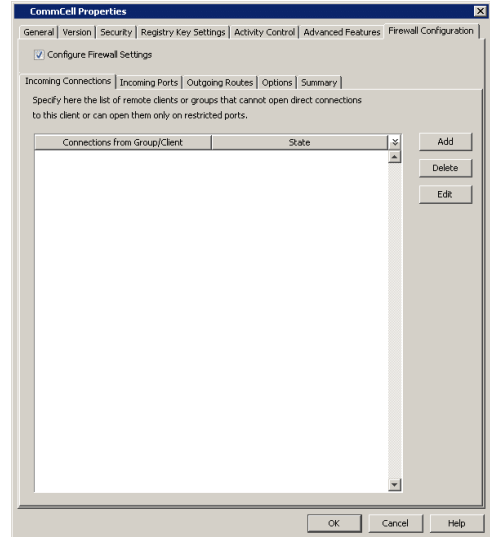
The previous configurations provided a path to reach the CommServe for installation purposes. To enable data protection operations between the two computers, you will have to establish the communication path between them. Perform the following steps to establish the communication route.

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

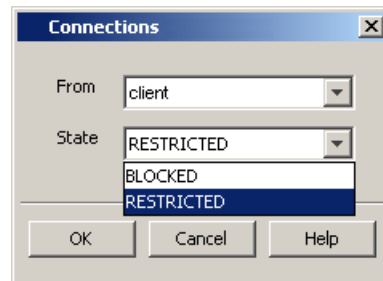




2. Click the **Firewall Configuration** tab.
3.
  - Click the **Incoming Connections** tab.
  - Click **Add**.



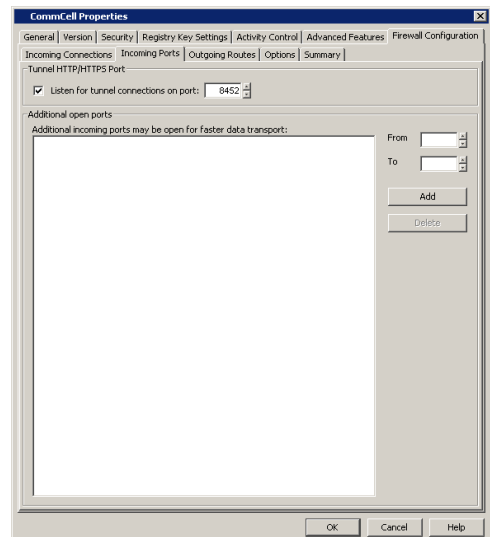
4.
  - In the **From** field, specify the name of the client outside the gateway you just installed.
  - In the **State** field, specify the status of the connection from the client. Since the connection is restricted through a gateway, select **Restricted**.
  - Click **OK**.



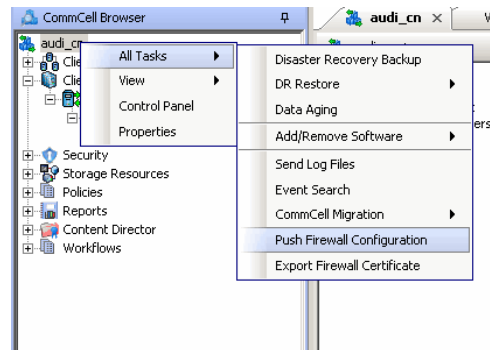
5.
  - Click the **Incoming Ports** tab.

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

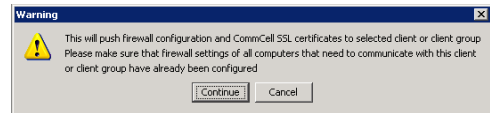
  - Click **OK**.



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



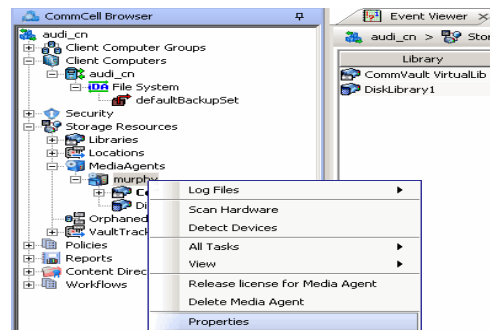
7. Click **Continue**.  
The CommServe is configured to receive communication from the client.  
Verify if your firewall configuration was pushed successfully in the **Event Viewer** window.



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.

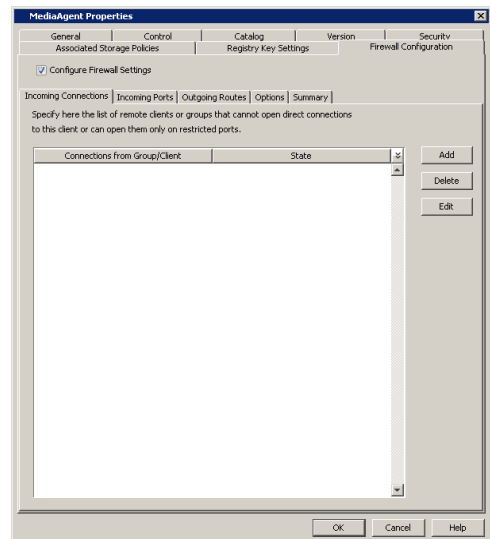


9. To configure the MediaAgent, right-click the MediaAgent computer from the CommCell Console and click **Properties**.

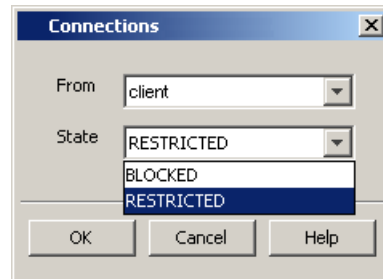


10. Click the **Firewall Configuration** tab.

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.

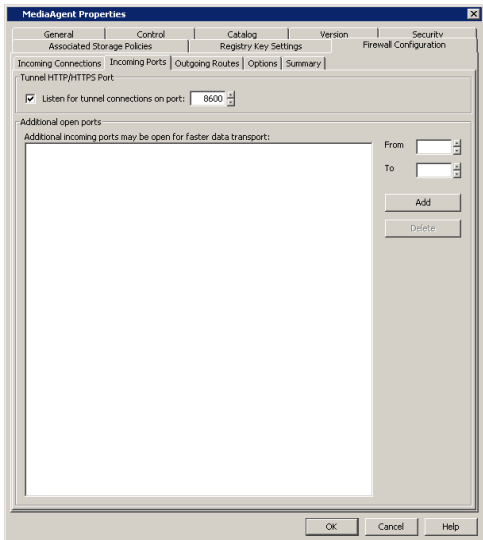
- Select **Listen for tunnel connections on port** and enter **440** as the port number. The gateway will forward connections to **mediaagent.company.com:440** when the gateway receives them from outside on port 444.
- **Additional Open Ports:** For components that handle data transfer (for example, 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.

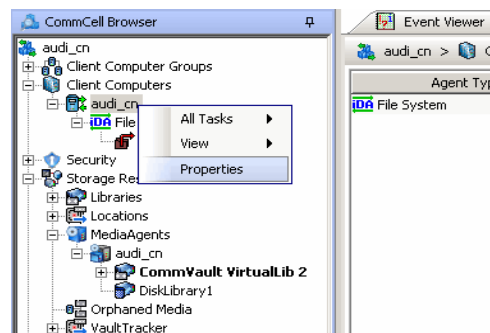


14. From the CommCell Console, right-click the client computer and click **All Tasks | Check Readiness**. The results are displayed in **Client Connectivity** dialog box.

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



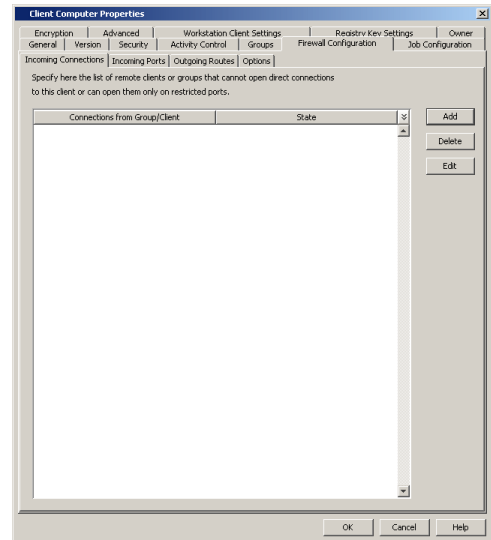
15. To configure the Client, right-click the client computer from the CommCell Console and click **Properties**.



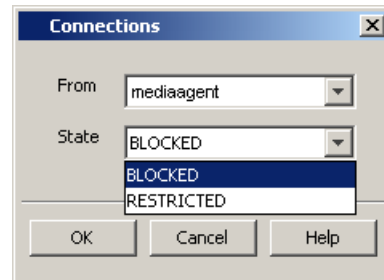
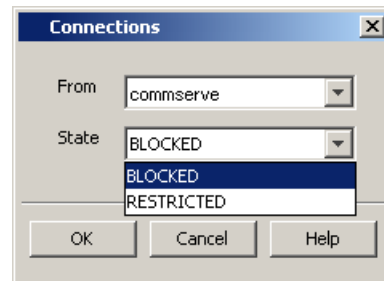
16. Click the **Firewall Configuration** tab.

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

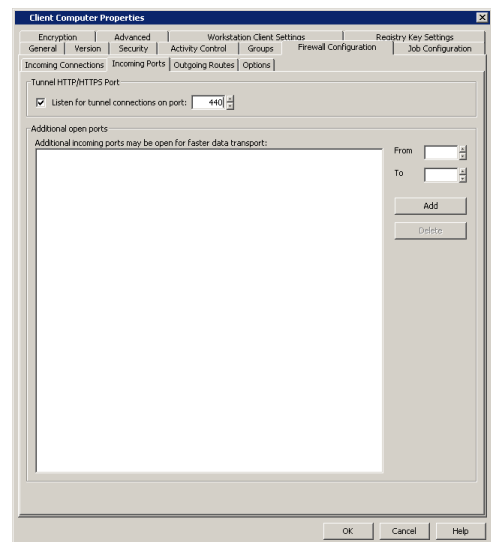
- 18.
- In the **From** field, specify the name of the CommServe computer behind the gateway.
  - In the **State** field, specify the status of the connection from the CommServe. Since CommServe does not open connections towards the client, select **Blocked**.
  - Click **OK**.



- 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**.

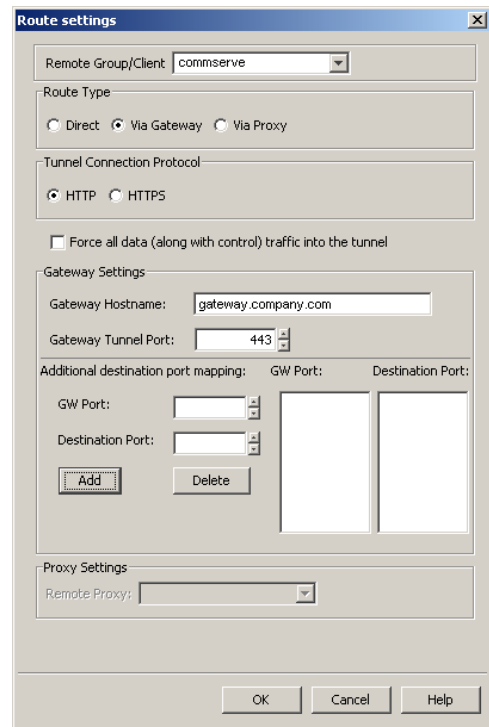
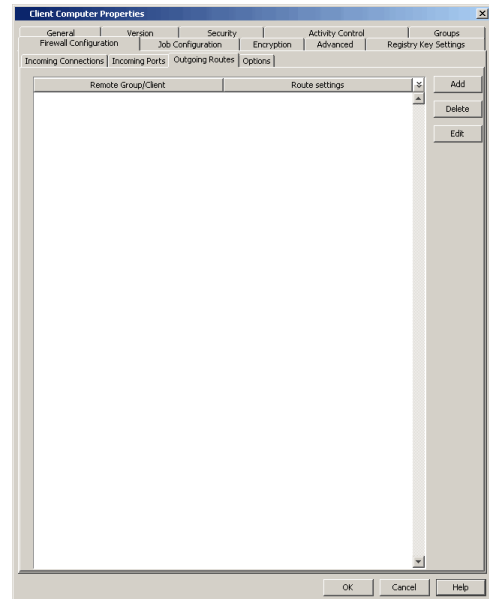


- 20.
- Click the **Incoming Ports** tab.
  - As the client does not receive incoming connections from the CommServe or MediaAgent, there is no need to select **Listen for tunnel connections on port**.
  - Click **OK**.



- 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**.

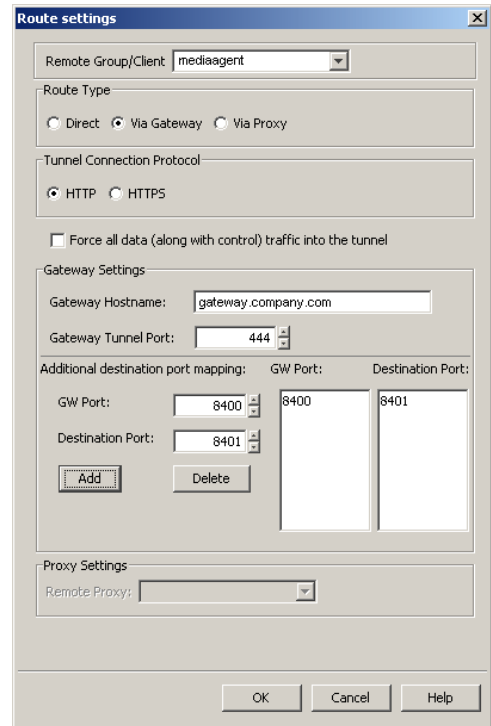


- 23.
- Click **Add** again to specify the outgoing connection route from this client towards the MediaAgent.
  - Select the MediaAgent in **Remote Group/Client**.
  - Select **Via Gateway**.
  - Select **Force all data (along with the control) traffic into the tunnel** to force the data traffic into 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**.

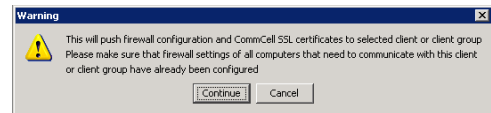
25. Click **Continue**.

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.

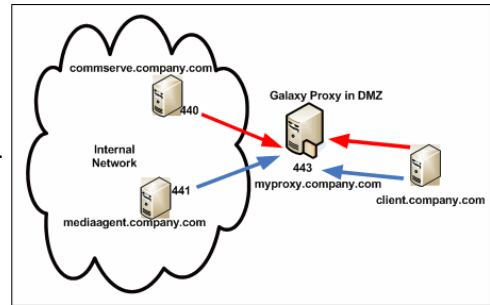
## OPERATING THROUGH A DMZ USING CALYPSO PROXY

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.

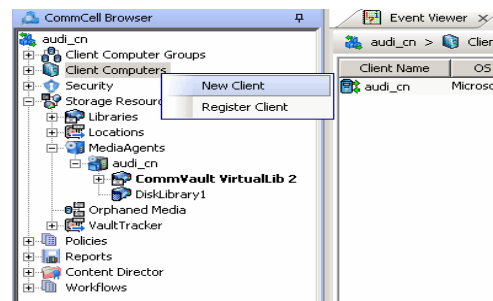
## SET UP THE CALYPSO PROXY

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

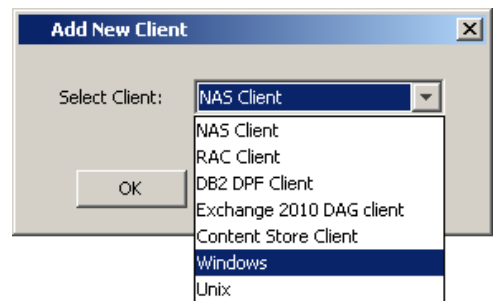
### PRECONFIGURE THE CALYPSO PROXY

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

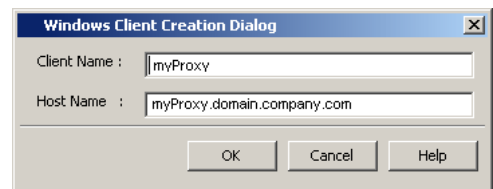
1. From the CommCell Console, right-click on the client computer node, and click **New Client**.



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

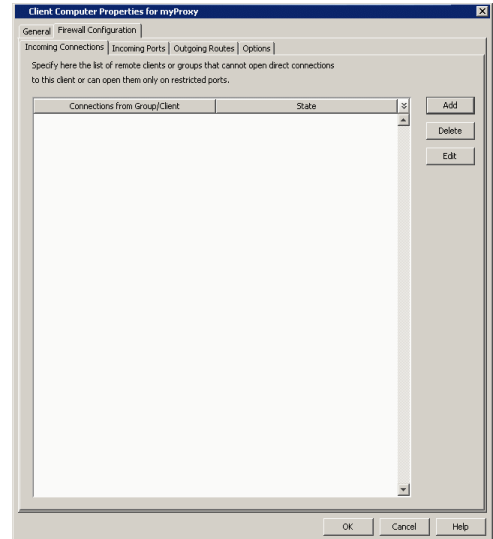
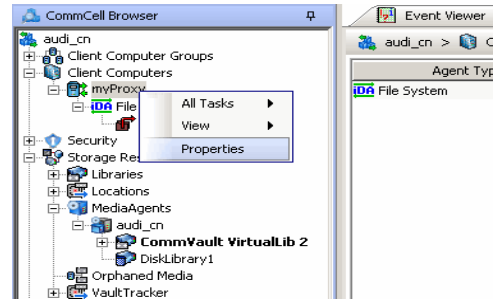


3.
  - Provide the **Client Name** and the **Host Name** you will use during your Calypso proxy installation.
  - Click **OK**.

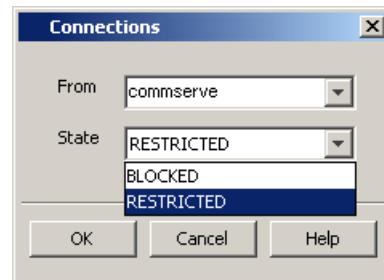


4. From the CommCell Console, right-click the client you just created, and click **Properties**.

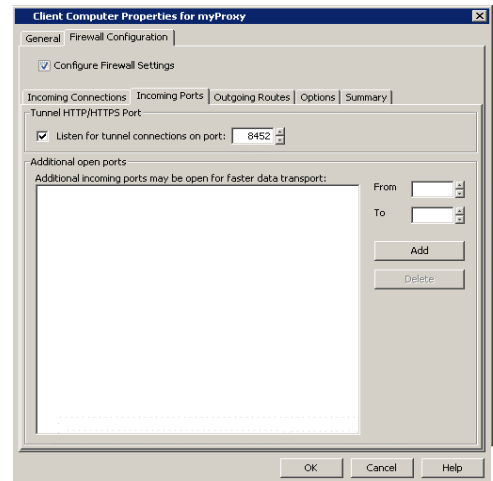
5.
  - Click the **Firewall Configuration** tab.
  - Click **Add**.



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.



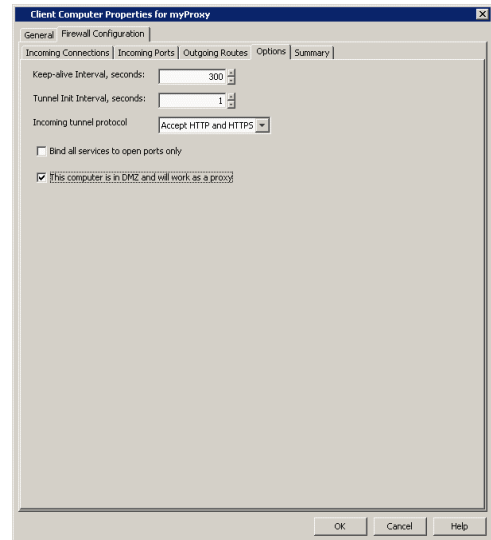
7.
  - Click the **Incoming Ports** tab.
  - Select **Listen for tunnel connections on port** and enter port number on which the Calypso proxy will listen from the CommServe.
 Write down the port number used as it will be needed during the Calypso proxy installation.



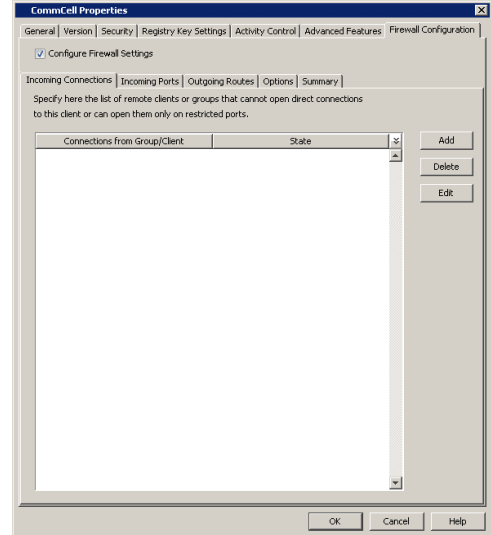
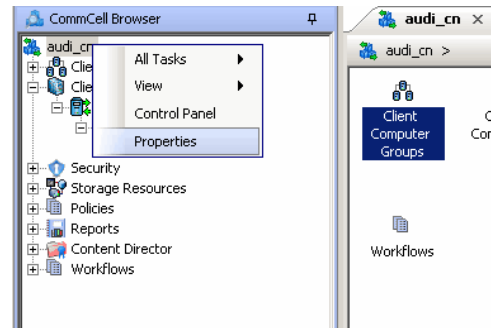
8.
  - Click the **Options** tab.
  - Select **This computer is in DMZ and will work as a proxy**.
  - Click **OK**.



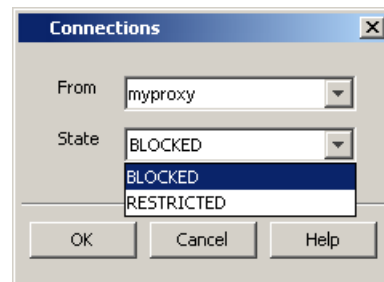
9. From the CommCell Console, right-click the CommServe computer and click **Properties**.



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

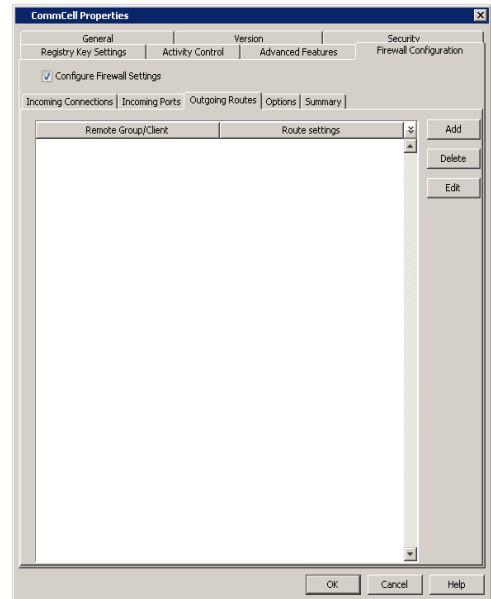


11.
  - In the **From** field, select the Calypso proxy computer.
  - In the **State** field, select **Blocked**.
  - Click **OK**.

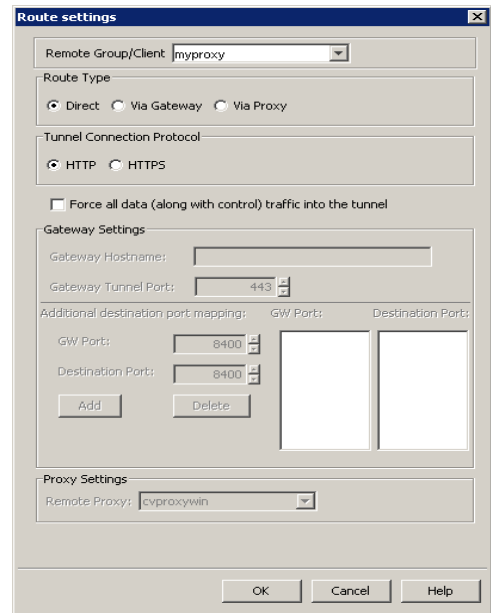


12.
  - Click the **Outgoing Routes** tab.

- Click **Add**.

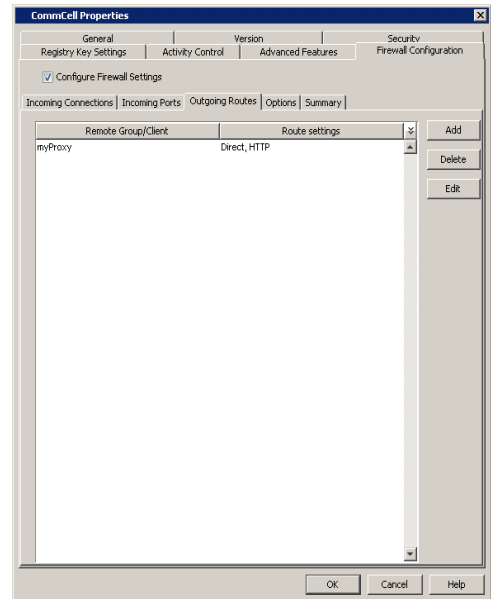


- 13.
- Select the Calypso proxy in **Remote Group/Client**.
  - Select **Direct**.
  - Click **OK**.

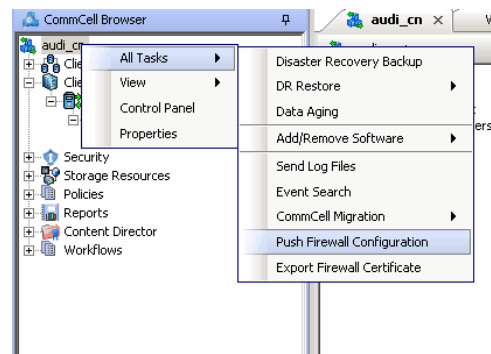


14. Click **OK**.

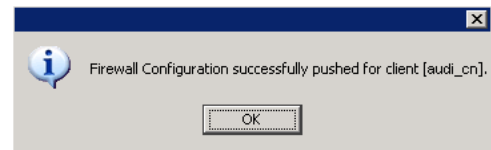
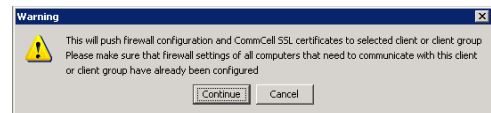
15. From the CommCell Console right-click the CommServe computer, click **All Tasks**, and click **Push Firewall Configuration**.



16. Click **Continue**.



17. 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:

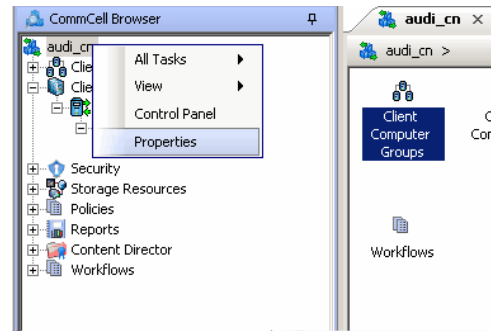
- CommServe can be Reached through a Proxy (Windows clients)

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

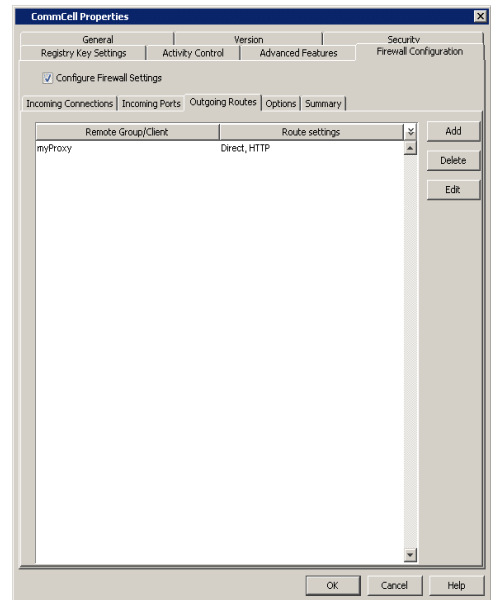
## CONFIGURE THE COMMSERVE, MEDIAAGENT AND CLIENT

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

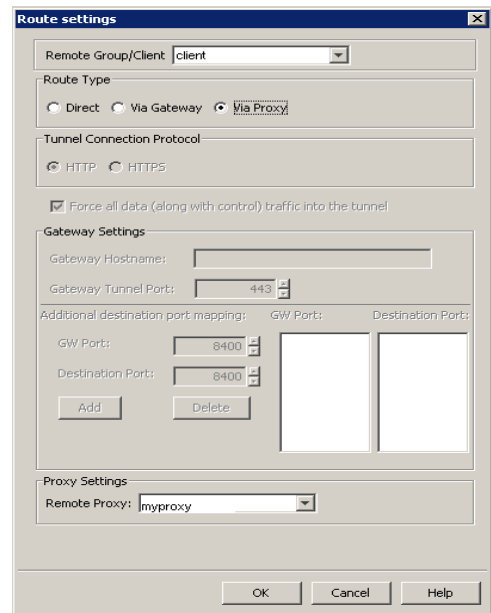
1. To configure the CommServe, right-click the CommServe computer from the CommCell Console and click **Properties**.



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.



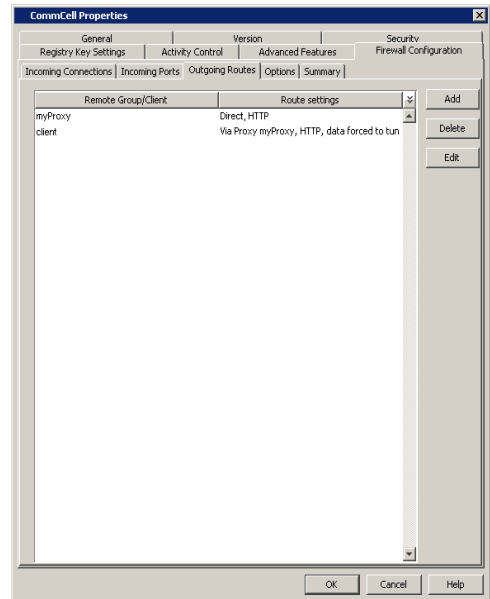
3.
  - Select the client computer in **Remote Group/Client**.
  - Select **Via Proxy**.
  - Select the Calypso proxy in **Remote Proxy**.
  - Click **OK**.



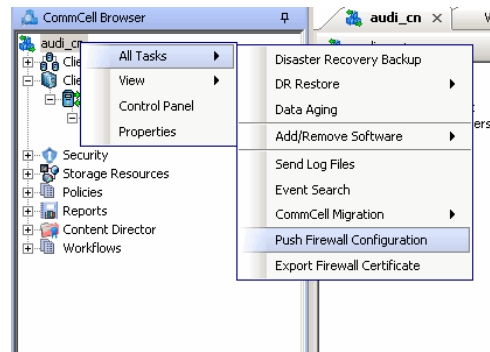
4. Click **OK**.

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.

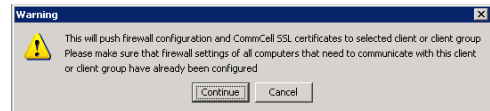
Note that when two computers are communicating with each other through a proxy, two routes need to be configured in each computer's Firewall preferences: one route to describe the connectivity of the computer with the proxy, and another route to describe the connectivity of the computer with the remote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



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

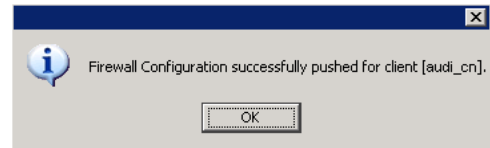


- Click **Continue**.



- 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.



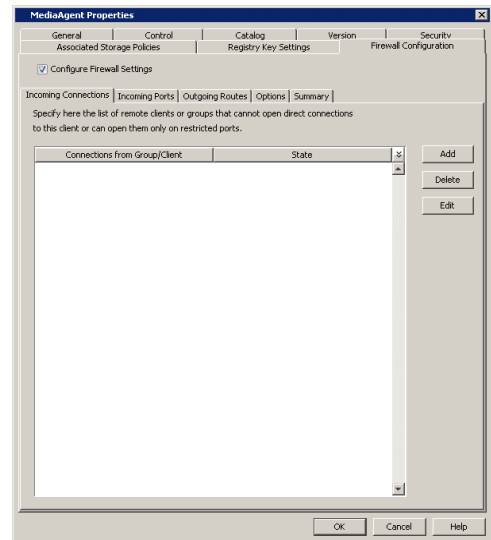
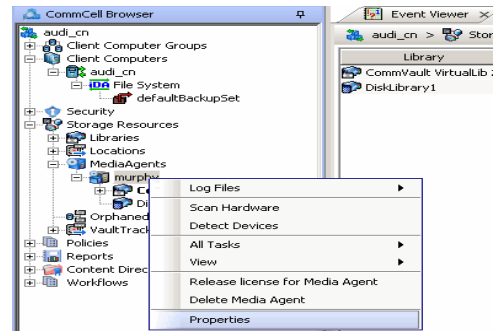
- From the CommCell Console, right-click the client computer and click **All Tasks | Check Readiness**. The results are displayed in **Client Connectivity** dialog box.

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

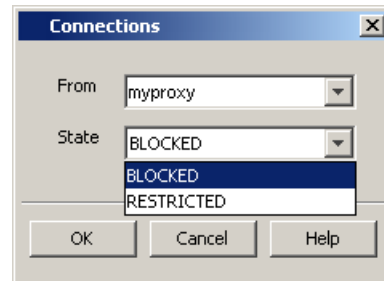


- To configure the MediaAgent, right-click the MediaAgent computer from the CommCell Console and click **Properties**.

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

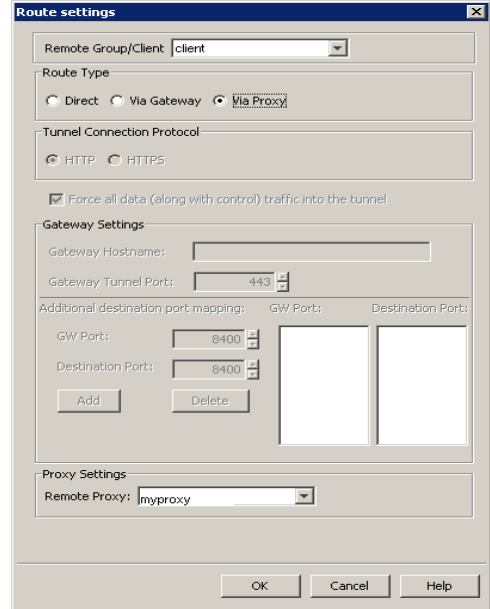
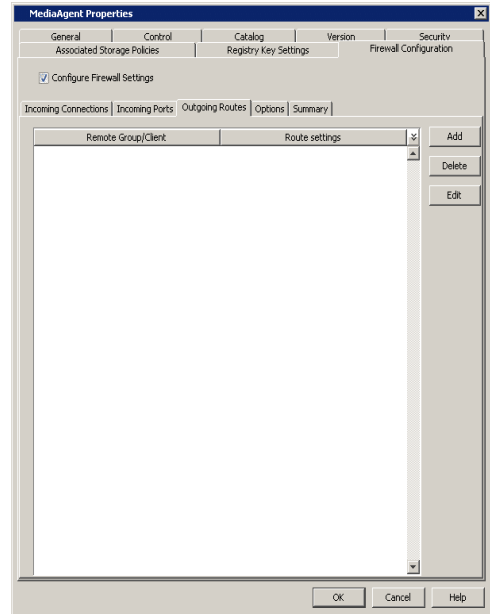


- 11.
- In the **From** field, select the Calypso proxy computer.
  - In the **State** field, select **Blocked**.
  - Click **OK**.

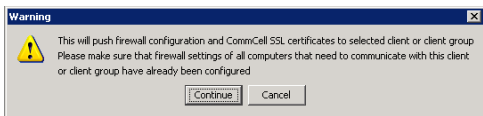
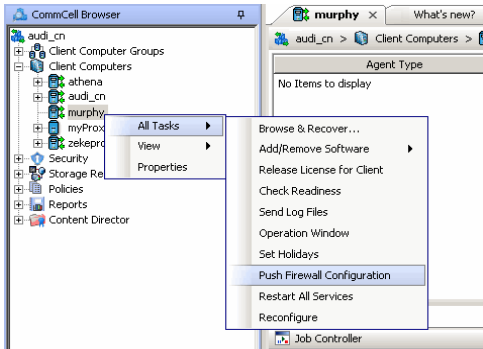
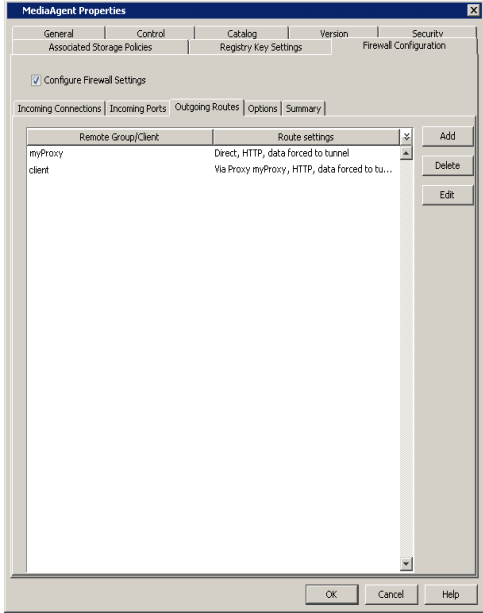
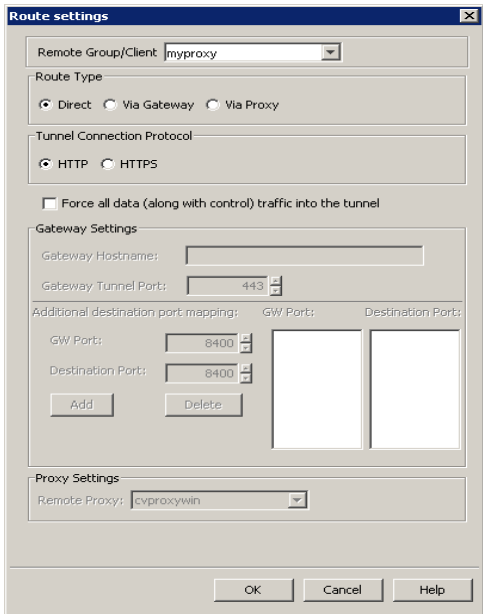


- 12.
- Click the **Outgoing Routes** tab.
  - Click **Add** to specify the outgoing connection route from the MediaAgent to the Client through the Calypso proxy.

- 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**.

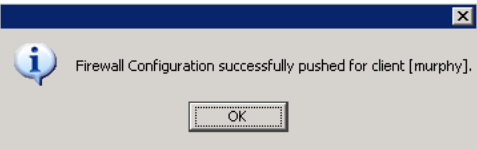
17. Click **Continue**.

18. Click **OK**.



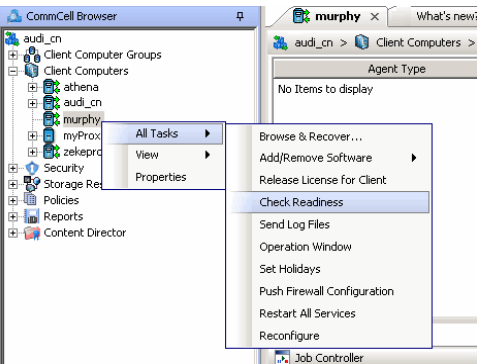
The MediaAgent is configured to receive communication from the client through the Calypso proxy.

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

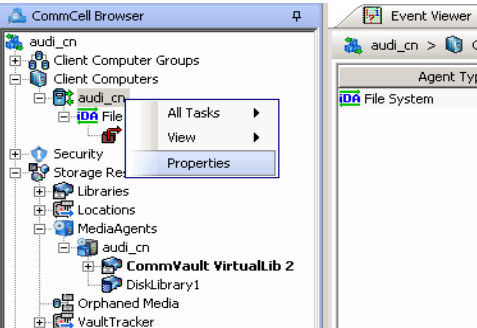


- 19. From the CommCell Console, right-click the MediaAgent computer and click **All Tasks | Check Readiness**. The results are displayed in **Client Connectivity** dialog box.

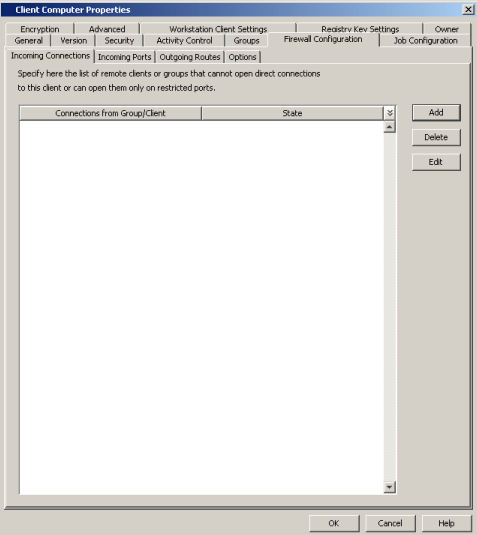
If the MediaAgent computer is not ready, verify your settings with the above recommendations and revise the settings if required.



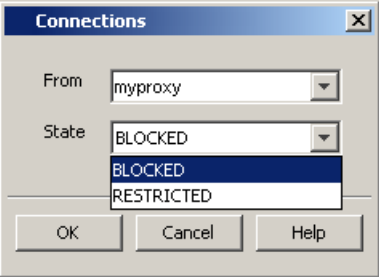
- 20. To configure the Client, right-click the client computer from the CommCell Console and click **Properties**.



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

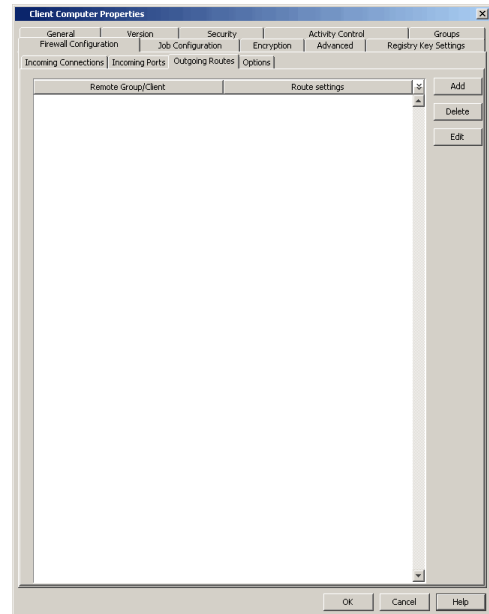


- 22.
  - In the **From** field, select the Calypso proxy computer.
  - In the **State** field, select **Blocked**. Since there are no incoming connections from the proxy to the client, the connection status is **Blocked**.
  - Click **OK**.



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

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

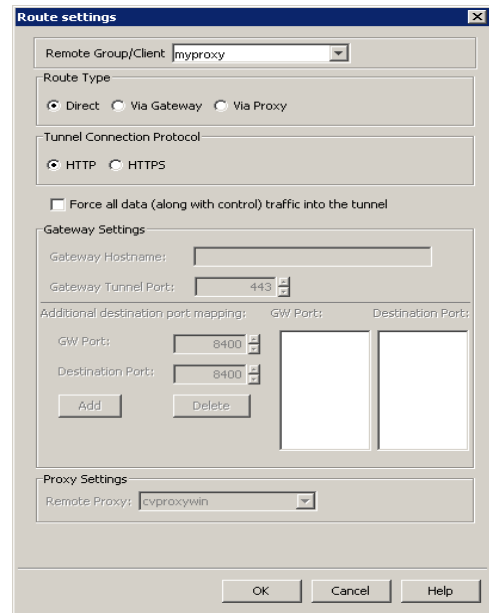


- 24.
- Select the Calypso proxy in **Remote Group/Client**.

- 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**.

The screenshot shows the 'Route settings' dialog box with the following configuration:

- Remote Group/Client:** commserve
- Route Type:**  Direct  Via Gateway  Via Proxy
- Tunnel Connection Protocol:**  HTTP  HTTPS
- Force all data (along with control) traffic into the tunnel
- Gateway Settings:**
  - Gateway Hostname: [Empty]
  - Gateway Tunnel Port: 443
- Additional destination port mapping:**

GW Port:	Destination Port:
8400	8400
- Proxy Settings:** Remote Proxy: myproxy

Buttons: OK, Cancel, Help

The screenshot shows the 'Route settings' dialog box with the following configuration:

- Remote Group/Client:** mediaagent
- Route Type:**  Direct  Via Gateway  Via Proxy
- Tunnel Connection Protocol:**  HTTP  HTTPS
- Force all data (along with control) traffic into the tunnel
- Gateway Settings:**
  - Gateway Hostname: [Empty]
  - Gateway Tunnel Port: 443
- Additional destination port mapping:**

GW Port:	Destination Port:
8400	8400
- Proxy Settings:** Remote Proxy: myproxy

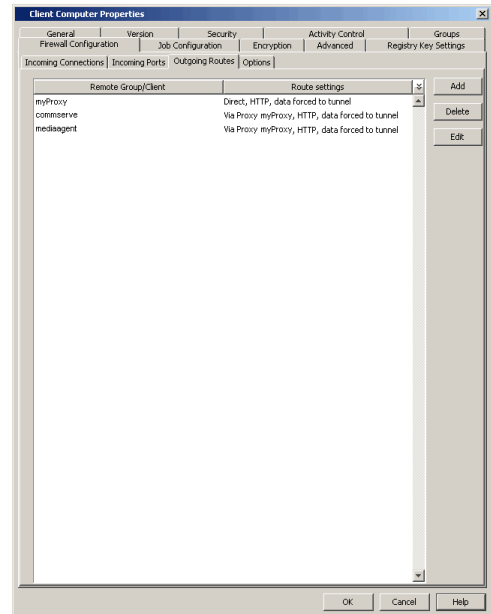
Buttons: OK, Cancel, Help

27. Click **OK**.

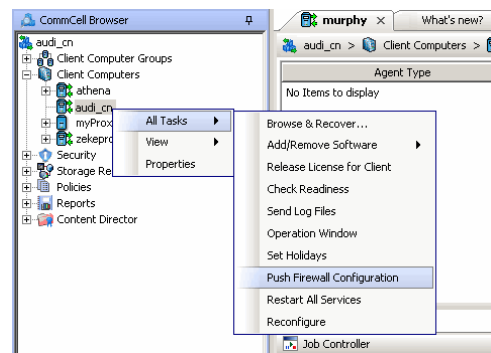
The **Outgoing Routes** tab should display three routes: the routes from the client to the proxy, client to to the MediaAgent, and client to the CommServe.

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**.



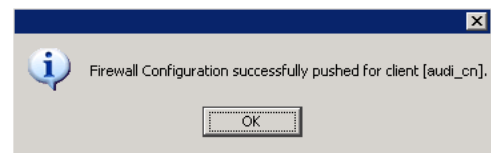
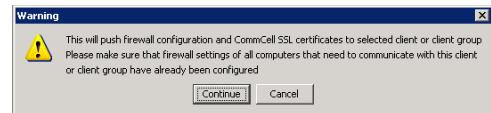
29. Click **Continue**.



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.

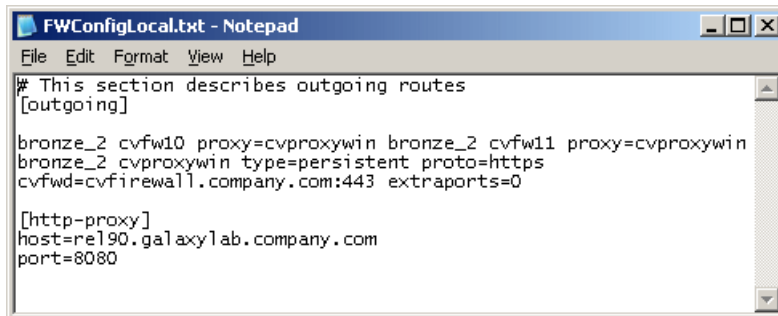
2. Locate the `[http-proxy]` section at the end of the file and remove the comment tag (`#`) from the section and its body. The section and its contents will appear as follows.

```
# [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

<a href="#">Setup</a>	<a href="#">Advanced</a>	<a href="#">Troubleshooting</a>	<a href="#">Best Practices</a>
-----------------------	--------------------------	---------------------------------	--------------------------------

### 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

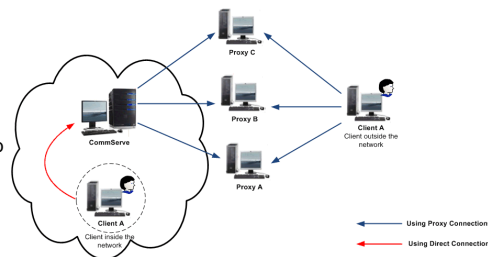
You can define the following routes for a client group or client computer:

- 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.

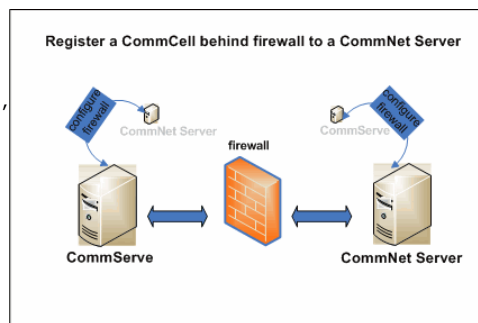
## REGISTERING A COMMSERVE TO A COMMNET SERVER

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.

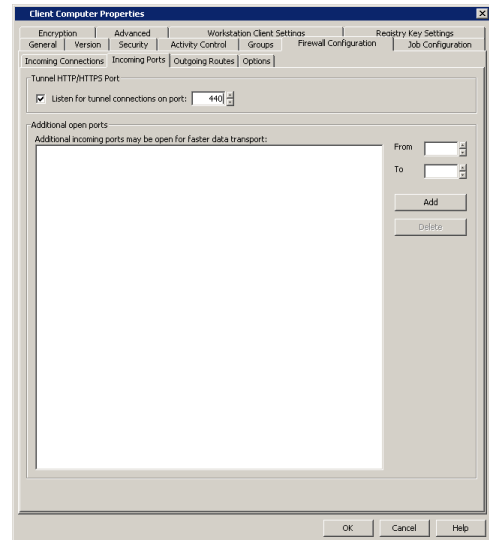
1. From the CommCell Console, right-click on the client computer node, and click **New Client**.
2. In the **Add New Client** window, select **Windows** and click OK.
3.
  - In the **Windows Client Creation** window, enter the **Client Name** and the **Host Name** of the CommNet Server computer on the 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.

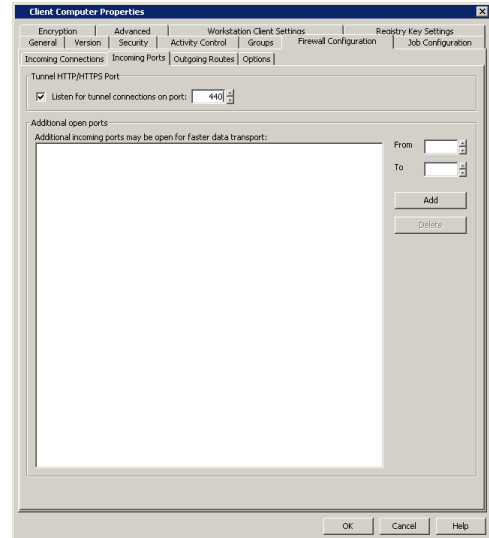
9. From the CommCell Console, right-click the client computer node, and click **New Client**.
10. In the **Add New Client** window, select **Windows** and click **OK**.
11.
  - In the **Windows Client Creation** window, enter the **Client Name** and the **Host Name** of the CommServe computer on the 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](#)

# Global Filters

Topics | How To | Support | Related Topics

## Overview

### How To Setup Global Filters

- CommNet Global Filters
- CommCell Global Filters

### Important Considerations

- General
- CommNet

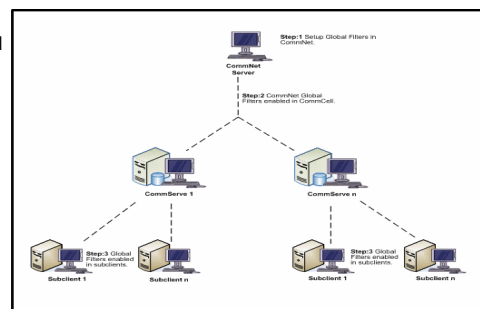
## OVERVIEW

Global Filters are exclusions that can be set to filter out data from data protection operations on all agents of a certain type. This is useful in cases where certain files, folders or entities need to be excluded from data protection operations.

Global Filters can be configured as follows:

- CommNet level to easily and quickly exclude data from data protection operations on multiple CommCells at once.
- CommCell level to exclude data from data protection operations on all clients residing within the CommCell.

CommNet Global Filters represent the top-level of a filtering hierarchy such that filters defined at the CommNet level can be propagated downward to CommCells within a CommNet domain, which can then be propagated down to specified subclients on those CommCells. The inheritance of Global Filters by subordinate objects within the filtering hierarchy is illustrated in the simple image.



For example, Company A decided to save money on storage and reduce the backup window by not backing up a folder commonly found on computers in their organization called `C:\temp`. To accomplish this goal using Global Filters, that path was specified as an exclusion filter entry in CommNet, then the Global Filters were enabled on each CommCell in the CommNet domain, and enabled on each file system subclient for those CommCells so that the CommNet filter entry was inherited by the selected CommCells and subclients. Using this approach, typing in that filter path for 100 subclients across 10 CommCells can be avoided. Also, the next time backups were run for those subclients it took less time and fewer tapes because `C:\temp` was successfully filtered out of the backups.

Global Filters are configured separately for each agent type both at the CommNet and CommServe level, and support the use of regular expressions (or wildcards).

To set up global filters for CommCell, use the Control Panel from the Tools menu on CommCell console.

## HOW TO SETUP GLOBAL FILTERS

### COMMNET GLOBAL FILTERS

Perform the following steps to setup Global Filters at the CommNet level:

1. Define the Global Filters in CommNet.  
See Setup Global Filters in CommNet for step-by-step instructions.
2. Enable the Global Filters in the CommCell.  
See Enable/Disable Global Filters for a CommCell for step-by-step instructions.
3. Enable Global Filters in the subclients.  
See Enable/Disable Global Filters on a Subclient for step-by-step instructions.

### COMMCELL GLOBAL FILTERS

Perform the following steps to setup Global Filters at the CommCell level:

1. Define the Global Filters in the CommCell.  
See Setup Global Filters for a CommCell for step-by-step instructions.
2. Enable Global Filters in the subclients.  
See Enable/Disable Global Filters on a Subclient for step-by-step instructions.

---

## IMPORTANT CONSIDERATIONS

---

### GENERAL

- Global Filters are disabled by default at the subclient level of each client, and the supported wildcards vary for each agent type. Be sure to use only the wildcards that work with the operating system or application for which you are creating a filter. Refer to the following:
  - For File System data see Wildcards
  - For Lotus Noted Document data see Wildcards
  - For Exchange data see Wildcards
- Job Results files cannot be filtered from backup operations.
- To configure Global Filters for an OES File System *iDataAgent* you must create and associate the subclient with Unix File System global filters.
- Do not change the Global Filter for subclients in a CommCell that have a data protection operation in progress.
- Performing a full backup after changing Global Filters is recommended.
- When you change a Global Filter, the change is effective the next time a data protection operation is run on the applicable subclients.

---

### COMMNET

- Global Filters configured in the CommNet environment are stored in the CommServe database of the CommCell for which they were created. Note that these filters can only be deleted utilizing the CommNet software, and will be removed from the CommServe database after CommCell Synchronization. Therefore, if a connection does not exist between the CommNet server and the CommServe, these Global Filters will continue to exist on the CommCell.
- When the following configurations are modified, the changes are immediately pushed to the active CommCell(s); cell synchronization is not required to propagate this information to the cells.
  - Global Filters
  - Billable Entities
  - Cost Categories
  - Data Collection Policy
  - Comments (Note that Comments made using the CommCell Console are pushed to the CommNet Server only during cell synchronization. For more information, see Comments.)

This information will be pushed accordingly when services (CommNet Server or Bull Calypso Server Event Manager) are restarted as well.

---

[Back to Top](#)

## Global Filters - How To

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

---

[Setup Global Filters in CommNet](#)

[Delete Global Filters exclusion from CommNet](#)

[Setup Global Filters for a CommCell](#)

[Delete Global Filters exclusion from CommCell](#)

[Enable/Disable Global Filters for a CommCell](#)

[Enable/Disable Global Filters on a Subclient](#)

---

## SETUP GLOBAL FILTERS IN COMMNET

*Required Capability:* See Capabilities and Permitted Actions

▶ To setup Global Filters:

1. On the **Setup** menu, click **Global Filters**.
2. From the Global Filters dialog, click the appropriate agent tab at the bottom of the window for the exclusions list you want to define.
3. For File System *iDataAgents*, perform one of the following actions:

- To add a file, folder or pattern that will be excluded from backups, click **Add**, and in the Enter Path dialog box, type the complete path (including drive letter) of the file, folder, or wildcard pattern that you want to exclude. Click **OK**.
- To modify an existing filter entry, select the entry in the display pane, then click **Modify**. In the Enter Path dialog box, type in your modification to the complete path (including drive letter) of the file, folder, or wildcard pattern that you want to exclude. Click **OK**.

See Wildcards for a list of supported wildcards for File System *iDataAgents*. Repeat this step if you want to add or modify more files and/or folders for the filter.

4. For Exchange Mailbox-based agents, perform one of the following actions:

- To add a mailbox folder that will be excluded from data protection operations, on the **Exclude Folder** tab, click **Add**, and in the Enter Folder Name (or Enter Path) dialog box, type in the mailbox folder path that you want to exclude. Click **OK**.
- To add a mailbox folder pattern that will be excluded from data protection operations, click the **Exclude Folder Patterns** tab, click **Add**, and in the Enter Folder Name (or Enter Path) dialog box, type in the wildcard pattern of the mailbox folders that you want to exclude. Click **OK**.
- To modify an existing filter entry on either the **Exclude Folder** tab or **Exclude Folder Patterns** tab, select the entry in the display pane and click **Modify**. In the Enter Folder Name (or Enter Path) dialog box, type in your modification to the mailbox folder name or wildcard pattern that you want to exclude. Click **OK**.

See Wildcards for a list of supported wildcards for Exchange Mailbox-based agents. Repeat this step to add or modify more mailbox folders and/or wildcard patterns for the filter.

5. To save your changes to the global filter, click **OK**.

Ensure that you have selected the **Use CommNet Global Filters** checkbox at the CommServe level, and the **Include CommCell Level Global Filters** or **Global Filter** checkbox for each subclient that you would like to inherit the CommNet filters. For step-by-step instructions, [Enable/Disable Global Filters on a Subclient](#).

## DELETE GLOBAL FILTERS EXCLUSION FROM COMMNET

*Required Capability:* See Capabilities and Permitted Actions

▶ To setup Global Filters by deleting an exclusion from the exclusions list:

1. On the **Setup** menu, click **Global Filters**.
2. From the Global Filters dialog, click the appropriate agent tab at the bottom of the window for the exclusions list you want to delete.
3. Select the file, folder path, mailbox folder or wildcard expression from the Exclusions list you wish to delete, and then click **Delete**. (Repeat this step for each entry that you want to delete.)
4. To save your changes to the global filter, click **OK**.

## SETUP GLOBAL FILTERS FOR A COMMCELL

*Required Capability:* Capabilities and Permitted Actions

▶ To setup Global Filters by adding/modifying an exclusion to the exclusions list:

1. From the CommCell Browser, right-click the CommServe, click **Control Panel**, and then click **Global Filters**.
2. From the Global Filters window, select the appropriate agent option from the **Global Filter Category** windowpane for the exclusions list you want to define.
3. For File System *iDataAgents*, perform one of the following actions:
  - To add a file or folder that will be excluded from backups, click **Browse** and select the desired path. Click **OK**.
  - To add a file, folder or pattern that will be excluded from backups, click **Add**, and in the Enter Path dialog box, type the complete path (including drive letter) of the file, folder, or wildcard pattern that you want to exclude. Click **OK**.
  - To modify an existing filter entry, select the entry in the display pane, then click **Modify**. In the Enter Path dialog box, type in your modification to the complete path (including drive letter) of the file, folder, or wildcard pattern that you want to exclude. Click **OK**.

See Wildcards for a list of supported wildcards for File System *iDataAgents*. Repeat this step if you want to add or modify more files and/or folders for the filter.

4. For Exchange Mailbox-based agents, perform one of the following actions:

- To add a mailbox folder that will be excluded from data protection operations, on the **Exclude Folder** tab, click **Add**, and in the Enter Folder Name (or Enter Path) dialog box, type in the mailbox folder path that you want to exclude. Click **OK**.
- To add a mailbox folder pattern that will be excluded from data protection operations, click the **Exclude Folder Patterns** tab, click **Add**, and in the Enter Folder Name (or Enter Path) dialog box, type in the wildcard pattern of the mailbox folders that you want to exclude. Click **OK**.
- To modify an existing filter entry on either the **Exclude Folder** tab or **Exclude Folder Patterns** tab, select the entry in the display pane and click



**Modify.** In the Enter Folder Name (or Enter Path) dialog box, type in your modification to the mailbox folder name or wildcard pattern that you want to exclude. Click **OK**.

See Wildcards for a list of supported wildcards for Exchange Mailbox-based agents. Repeat this step to add or modify more mailbox folders and/or wildcard patterns for the filter.

5. To save your changes to the global filter, click **OK**.
- 

## DELETE GLOBAL FILTERS EXCLUSION FROM COMMCELL

*Required Capability:* Capabilities and Permitted Actions

▶ To delete an exclusion from the exclusions list:

1. From the CommCell Browser, right-click the CommServe, click **Control Panel**, and then click **Global Filters**.
  2. From the Global Filters window, select the appropriate agent option from the **Global Filter Category** windowpane for the exclusions list you want to delete.
  3. Select the file, folder path, mailbox folder or wildcard expression from the Exclusions list you wish to delete, and then click **Delete**. (Repeat this step for each entry that you want to delete.)
  4. To save your changes to the global filter, click **OK**.
- 

## ENABLE/DISABLE GLOBAL FILTERS FOR A COMMCELL

*Required Capability:* Capabilities and Permitted Actions

▶ To setup Global Filters for a CommCell:

1. From the CommCell Browser, right-click the CommServe, click **Control Panel**, and then click **Global Filters**.
  2. From the Global Filters window, select the **Use CommNet Global Filter** checkbox.
  3. To save your changes to the global filter, click **OK**.
- 

## ENABLE/DISABLE GLOBAL FILTERS ON A SUBCLIENT

### Before You Begin

- Make sure that CommCell Level Global Filters are defined or CommNet Global Filters are enabled. See Setup Global Filters in CommNet or Setup Global Filters for a CommCell for step-by-step instructions.

*Required Capability:* Capabilities and Permitted Actions

▶ To enable/disable the Global Filter on a subclient:

1. From the CommCell Browser, right-click the subclient whose Global Filter you want to enable, and then click **Properties** from the shortcut menu.
  2. Click the Filters tab of the Subclient Properties dialog box.
  3. To enable/disable Global Filters on this subclient, select one of the following values from the **Include Global Filters** list:
    - **ON** - select this option to disable Global Filters for this subclient.
    - **OFF** - select this option to enable Global Filters for this subclient.
    - **Use Cell Level Policy** - select this option to enable or disable Global Filters for this subclient only when the **Use Global Filters on All Subclients** option is enabled on the **Control Panel (Global Filters)** dialog.
  4. Click **OK** to save your changes.
- 

[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

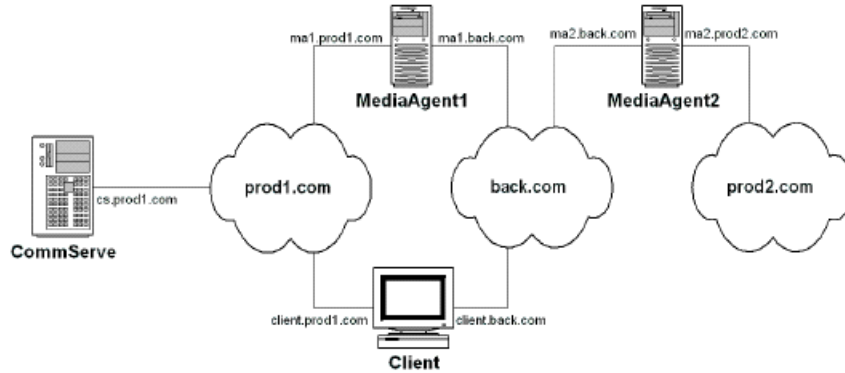
When you have multi-homed computers that has two or more network interface cards (NICs) in both the CommNet Server as well as the CommCell computer, you can configure the software to communicate across a specific NIC using the following procedures:

- 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:



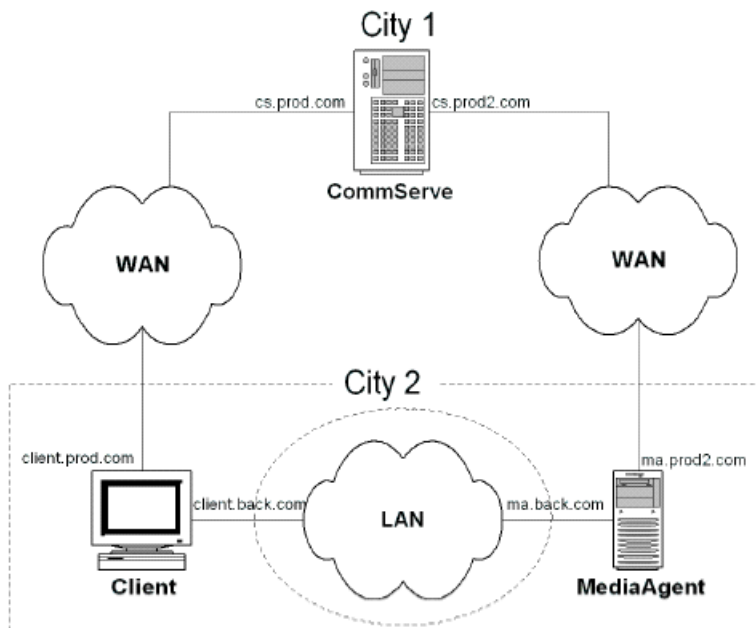
In the above scenario all data is conducted through the *backup* domain `back.com`, thereby reducing network traffic on the production domains. The following data interface pairs have to be defined to accomplish this goal:

- `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`

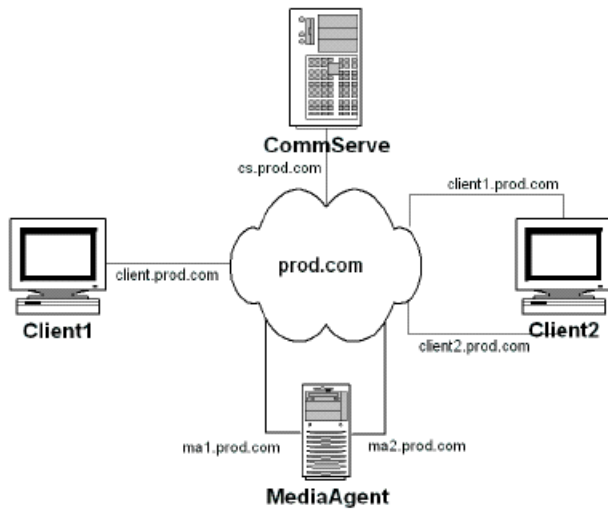


In the above scenario, the CommServe is located in one geographic domain, while the Client and MediaAgent are located in another different geographic domain. In such a situation, adding a third domain and defining the following pipeline pair between the Client and MediaAgent would result in efficient 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



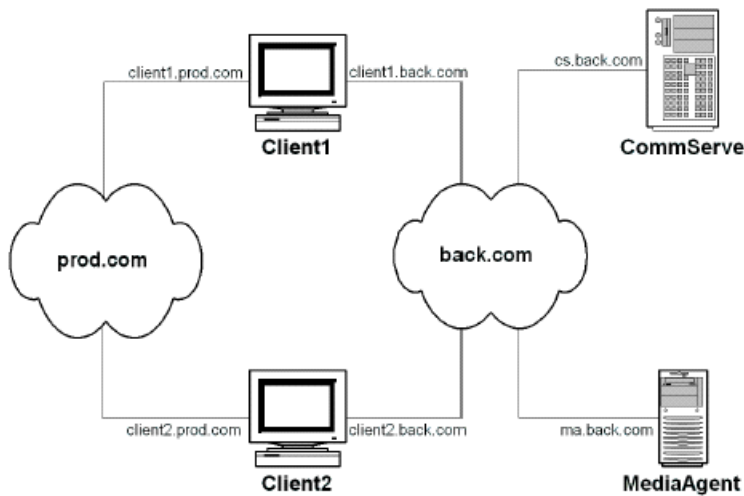
In the above scenario, although all the components are in the same domain, (they could be in a different subnet) defining the following pipeline pair between Client2 and MediaAgent would result in better network communication:

- 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.

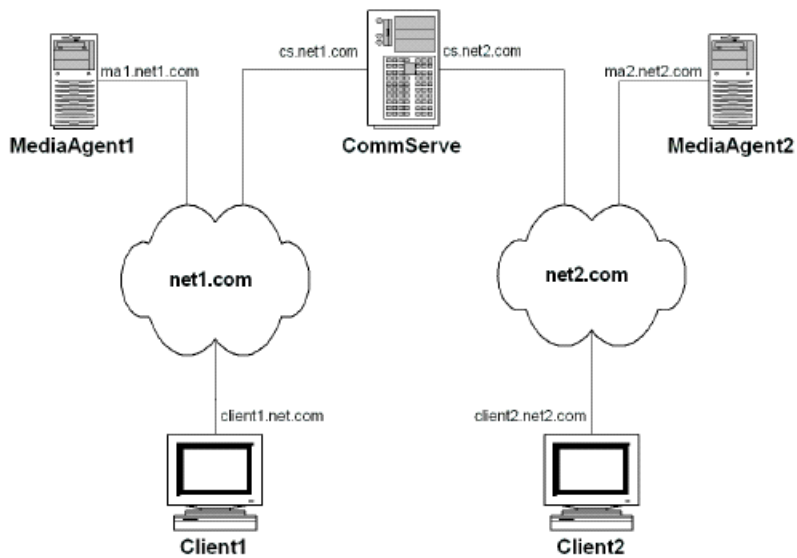


In the above scenario, all the client computers are in the production domain while the MediaAgent and CommServe are attached to the *backup* domain back.com. By using the client1.back.com and client2.back.com as the default interface names for the clients, all the data protection operations and communication 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

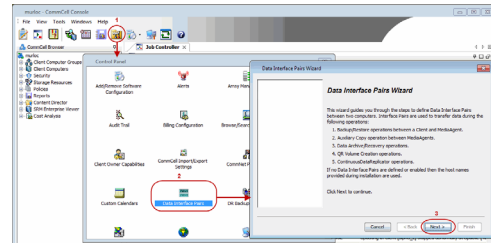
- When you create a data interface between two computers, you must ensure that there is a network path between the two computers. If there is no network path between the two computers all operations will fail. If necessary, check with your network administrator to determine whether a given interface pair is valid.

*Required Capability:* Capabilities and Permitted Actions

▶ To configure data interface pairs:

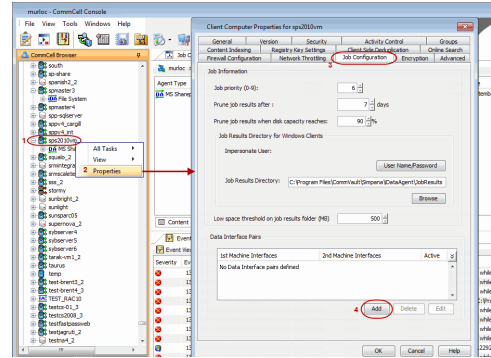
1. From the **Tools** menu in the CommCell Console, click **Control Panel** and then double-click **Data Interface Pairs**.

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](#)



# SLA

Topics | How To | Troubleshoot | Related Topics

The Data Protection SLA (Service Level Agreement) report displays the overall performance of backup operations across multiple clients and their respective entities based on the admissible SLA value configured in the CommNet Browser. This performance rating helps in detecting the acceptable levels of the data protection operations for CommCells, clients, applications, or subclients.

Based on this rating, you can then determine if you need to take any corrective action such as modifying the retention policies, schedule patterns, or by fixing problems that may exist in the network or hardware.

The SLA is calculated by taking various short-term and long-term data protection coverage data into account as defined in the SLA Setup dialog box.

The following coverage data categories are included:

- existence of full coverage
- existence of any level of coverage
- redundancy in coverage
- failure rate.

You may also set a benchmark level called the admissible SLA. This is used to compare against the benchmark level when the SLA is calculated, to determine if the CommCells, Clients, or applications are adequately covered. An SLA above this benchmark reflects adequate data protection coverage, however an SLA below this benchmark reflects inadequate coverage.

The SLA for any entity at a level higher than a subclient is computed by taking the average of the SLAs for all associated subclients. If the SLA for a particular entity is below the benchmark level, then analyze all the associated subclients to determine if the problem is uniform across all subclients or a particular subclient.

SLA averages can be viewed from the Client SLA window and the Data Protection SLA Report.

## SLA - How To

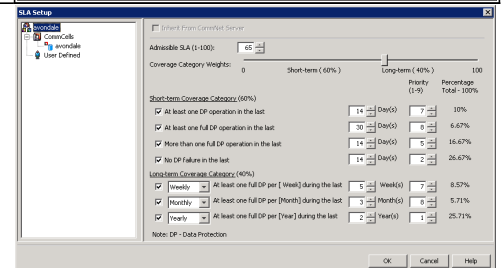
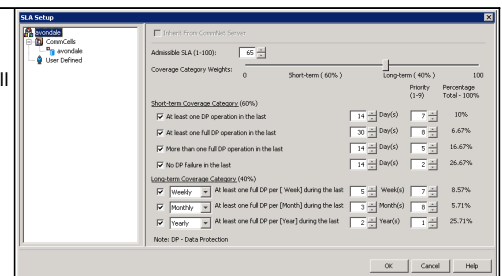
Topics | How To | Troubleshoot | Related Topics

### CONFIGURE THE SLA FOR THE COMMNET SERVER OR A COMMCELL

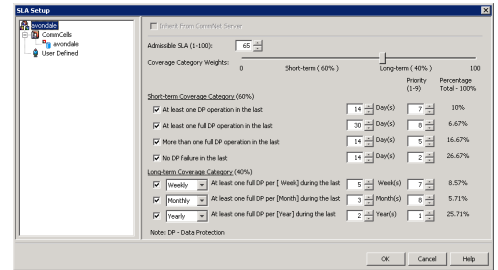
*Required Capability:* See Capabilities and Permitted Actions

▶ To set up the SLA for the CommNet Server or a CommCell:

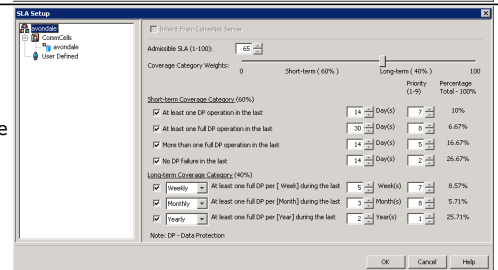
- From the CommNet menu bar, select the **Setup** menu, and click **SLA Configuration**.
- From the SLA Setup dialog box, select the CommNet Server or a specific CommCell.  
Note that if you want parameters for the CommCell to be different from what is configured for the CommNet Server, then de-select the **Inherit From CommNet Server** field and select a CommCell from the drop-down tree.
- Assign a benchmark SLA level in the **Admissible SLA** field from 1 to 100.  
Determine the coverage category weights for the short-term and long-term coverage category by sliding the percentage weight bar to the left or right. Based on the position of the slider, the percentage is assigned to each category totaling the percentage, e.g., if the short term is set at 60%, the coverage categories percentage will total 60%, and the long term categories would total 40%. Each category within the short term and long term coverage categories are weighted differently depending on their priority.
- From the **Short Term Coverage Category** pane:
  - Select the categories to be included in the SLA calculation.
  - Select a number days for each coverage category.



- Assign a relative weight priority from 1 to 9 for each coverage category. Based on this and the coverage category weight assigned, a weight percentage is assigned to each short term coverage category.



- From the **Long Term Coverage Category** pane:
  - Select the categories to be included in the SLA calculation.
  - Select a number of weeks, months, or years for each coverage category.
  - Assign a relative weight priority from 1 to 9 for each coverage category. Based on this and the coverage category weight assigned, a weight percentage is assigned to each long term coverage category.



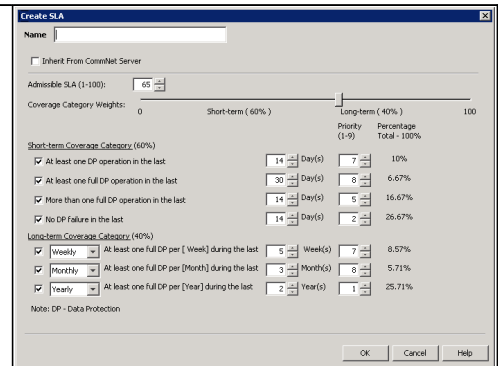
- Click **OK**.

## CONFIGURE THE SLA FOR A CLIENT COMPUTER

*Required Capability:* See Capabilities and Permitted Actions

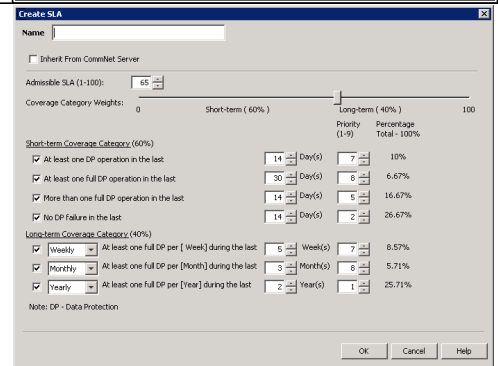
▶ To set up the SLA for a client:

- From the CommNet menu bar, select the **Setup** menu, and click **SLA Configuration**.
- From the SLA Setup dialog box, right-click on **User Defined**, and select **Create SLA**.

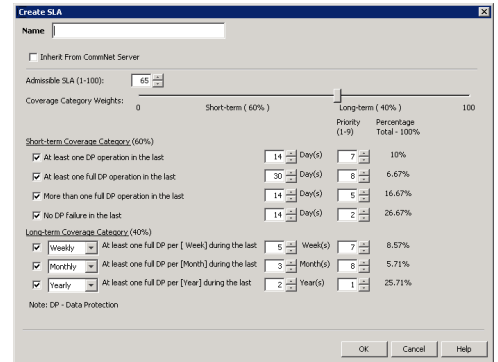


Enter a Name for the User Defined SLA.  
 Note that if you want parameters for the Client to be the same as what is configured for the CommNet Server, then select the **Inherit From CommNet Server** field.

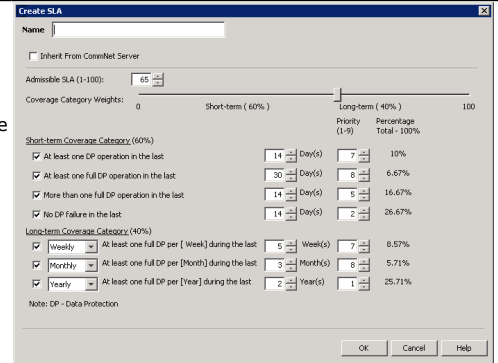
- Assign a benchmark SLA level in the **Admissible SLA** field from 1 to 100.
- Determine the coverage category weights for the short-term and long-term coverage category by sliding the percentage weight bar to the left or right. Based on the position of the slider, the percentage is assigned to each category totaling the percentage, e.g., if the short term is set at 60%, the coverage categories percentage will total 60%, and the long term categories would total 40%. Each category within the short term and long term coverage categories are weighted differently depending on their priority.



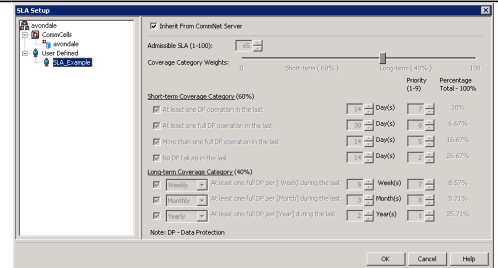
- From the **Short Term Coverage Category** pane:
  - Select the categories to be included in the SLA calculation.
  - Select a number days for each coverage category.
  - Assign a relative weight priority from 1 to 9 for each coverage category. Based on this and the coverage category weight assigned, a weight percentage is assigned to each short term coverage category.



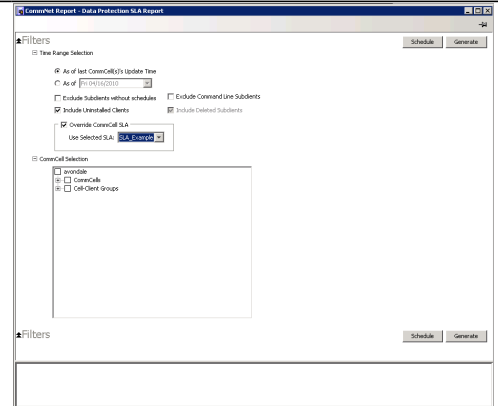
4. From the **Long Term Coverage Category** pane:
- Select the categories to be included in the SLA calculation.
  - Select a number of weeks, months, or years for each coverage category.
  - Assign a relative weight priority from 1 to 9 for each coverage category. Based on this and the coverage category weight assigned, a weight percentage is assigned to each long term coverage category.
- Click **OK**.



5. The User Defined SLA will appear on the **SLA Setup** dialog. Click **OK**.



6. Run an SLA Report.
- To use a user defined SLA rating:
- Select the **Override CommCell SLA** option, and select the SLA you wish to use for the client.
- In the **CommCell Selection** windowpane, select the client to run the report against.
- Click **Generate**. The SLA report will be generated for the specified client.



# CommNet - Log Files

Topics | How To

---

Overview

Log File Pruning

---

## OVERVIEW

Log files are used by the software to record processing details of operations that have occurred on the CommNet Server and CommNet Agent and can be viewed for troubleshooting purposes. The log files are recorded to the following locations:

- On the CommNet Server computer: `<CommNet software installation directory>\Log files\CommNetServer.log`
  - On the CommNet Agent computer: `<CommServe software installation directory>\Log files\CommNetAgent`
- 

## LOG FILE PRUNING

The default size of each log file is 5MB. The system prunes the log files every 10 minutes if the size of the `Log Files` directory is over 100 MB. This is done by pruning the older files until the size of the `Log Files` directory is 80% of the maximum size established for the log files directory (by default, 80% of 100 MB, which is 80MB).

Older log files are copied to the following directory:

- `<CommNet software installation directory>\Log files\Old Log Files\`

The log files stored in the `Old Log Files` directory have a starting timestamp and ending timestamp as a part of the filename.

---

# CommNet - Log Files - How To

Topics | How To

---

## CHANGE MAXIMUM SIZE OF LOG FILES DIRECTORY

### WARNING

Incorrectly editing the registry may severely damage your system. Before making changes to the registry, it is strongly recommended that you back up any valued data on the computer. For information about how to backup and restore the registry, refer to the appropriate Registry Help Topic provided in **Regedit.exe** or **Regedt32.exe**.

*Required Capability:* See Capabilities and Permitted Actions

▶ To change the maximum size of the log files directory:

1. Open the Registry Editor.
2. Navigate to the following registry key:

```
QNet\Platform Information\<vmname>\Debug
```

3. Create the following entry as a DWORD value:

```
nDEBUGDIRMAXSIZE
```

4. Assign a value (in MB) to indicate the maximum size of the log files directory.
  5. Close Registry Editor.
-

# CommNet Disaster Recovery

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

---

Overview

[Planning for Disaster Recovery of the CommNet Server](#)

[Building a Standby CommNet Server Using Log Shipping](#)

---

## OVERVIEW

In the case of disaster recovery, where a full system restore is required, you must rebuild the system to exactly the state as it existed before the problem. In some cases, where the SQL Server is corrupted, the SQL Server software must be reloaded and the server rebuilt.

---

## PLANNING FOR DISASTER RECOVERY OF THE COMMNET SERVER

Schedule Disaster Recovery Backups regularly to protect CommNet Server database as described in [Disaster Recovery Backups](#).

---

## BUILDING A STANDBY COMMNET SERVER USING LOG SHIPPING

You could also setup a standby server for disaster recovery purposes. See [Building a Standby CommNet Server Using Log Shipping](#) for step-by-step instructions.

---

# CommNet Disaster Recovery - How To

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

---

[Recover the CommNet Server in the Event of a Disaster](#)

[Building a Standby CommNet Server Using Log Shipping](#)

---

## RECOVER THE COMMNET SERVER IN THE EVENT OF A DISASTER

The following procedures assume that you have planned for disaster recovery as described in [Planning for Disaster Recovery of the CommNet Server](#).

*Required Capability:* See [Capabilities and Permitted Actions](#)

### To recover the CommNet Server computer:

Use the following procedure to recover the CommNet Server to the same computer or to a different computer.

1. Rebuild the CommNet Server computer.
  - o Install the operating system with all the necessary service packs.
  - o Install the CommNet Server software.

The install program will also install Microsoft SQL Server Enterprise Edition, with the CommNet instance. It is NOT necessary to install all these components in the same drives and folders in which they were previously installed.
2. From the CommServe computer, Stop Services on Windows for CommNet.
3. Using the CommServe Disaster Recovery Tool, Restore a Disaster Recovery Backup.
4. From the CommServe computer, Start Services on Windows for CommNet.
5. If the software is restored to another computer or to the same computer with a new name, perform the following steps on all the CommCells that were registered in this CommNet Server:
  - o Contact your software provider's representative to obtain a new license.

If original license included a Disaster Recovery IP address, there is no need to update the license, please move to

the Cell Registration step.

- From the CommNet Browser, on the Cell Registration dialog box, select each CommCell then click **Modify**.
  - From the Modify CommCell dialog box, type a new CommNet interface name in the CommNet Interface Name field.
  - Click **OK**.
  - After all the cells have been changed, click **Close** from the Cell Registration dialog box.
6. Synchronize the CommCell in the CommNet Browser to obtain up-to-date information about the CommCell.

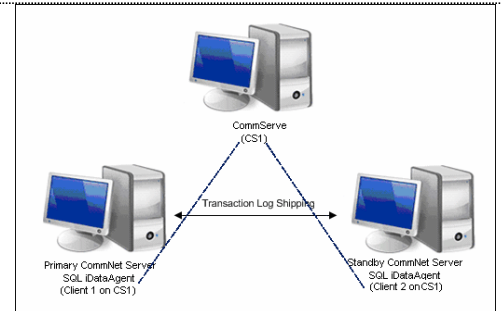
## BUILDING A STANDBY COMMNET SERVER USING LOG SHIPPING

If the CommNet Server is installed in the primary production environment, a standby CommNet Server can be built as described in the following sections.

### REQUIREMENTS

Review the following requirements before setting up the primary and standby CommNet Server and the Microsoft SQL Server Database Engine on separate computers:

- Primary and Standby CommNet Servers
  - Setup the primary and standby CommNet Servers by installing the CommNet Server and the SQL Server *iDataAgent* software.
- Two CommNet Server licenses
  - One each for the primary and standby CommNet servers
- Two licenses for SQL Server *iDataAgents*
  - One each for the primary and standby CommNet servers



### PROCEDURE

#### Setting up the Primary CommNet Server

1. Install the CommNet Server software on the primary CommNet Server computer. See Deployment - CommNet Server, for more information.
2. Install the SQL Server *iDataAgent* on the primary CommNet Server computer. (Client 1 of CS1 in the above illustration.) See **Deployment - Microsoft SQL Server *iDataAgent*** for more information.

#### Setting up the Standby CommNet Server

3. Install the CommNet Server software on the standby CommNet Server computer. See Deployment - CommNet Server, for more information.  
Make sure that all the updates installed in the primary CommNet Server are also installed on the standby CommNet Server
4. Stop all Services on the standby CommNet Server. See Services for more information.  
You cannot have services running on both the primary and standby computers.
5. Install the SQL Server *iDataAgent* on the standby CommNet Server computer. (Client 2 of CS1 in the above illustration.) See **Deployment - Microsoft SQL Server *iDataAgent*** for more information.

#### Setting up the Standby CommNet Server Database

6. Using the SQL Server *iDataAgent*, perform a full backup of the SQL database in the primary CommNet Server and restore it to the SQL Server in the standby CommNet Server. The database must be in the standby state after the restore.
  - See Start a Full/Incremental/Differential Backup for step-by-step instructions on performing a full backup using the SQL Server *iDataAgent*. This can be found in the **Backup - Microsoft SQL Server** section.
  - See **Restore a Single Database Without Browsing** for step-by-step instructions on restoring data using the SQL Server *iDataAgent*. This can be found in the **Restore - Microsoft SQL Server** section.
7. Using the SQL Server *iDataAgent*, schedule frequent backups of the Transaction Logs in the primary server. It is recommended to schedule backups every 30 minutes. See **Start a Transaction Log Backup** for step-by-step instructions. This can be found in the **Backup - Microsoft SQL Server** section.  
Schedule a restore of the transaction logs to be run after each backup. The database must be in the standby state after every Transaction Log restore.
  - If possible, choose a disk storage policy for performance reasons.
  - Make sure to periodically verify the scheduled jobs to ensure that the transaction log backup and restore

#### See Also:

**Warm Database Restore** for more information on the performing this type of restore.

complete successfully.

#### Switching the CommNet Server from Primary to Standby in Case of failures

1. If the primary CommNet Server is still active stop all services on the CommNet Server computer. See Services for more information.
2. In the standby computer, using the **SQL Server Management Studio**, bring the **CommNet** database online. See the **SQL Server Management Studio** help for information on bringing the database online.
3. In the Standby CommNet Server, start the services. See Start Services on Windows for step-by-step instructions.
4. Open the CommNet Console and re-apply the permanent license associated with the standby CommNet Server. See License Administration for more information.
5. Perform the following steps on all the CommCells that are registered with this CommNet Server: See Register a Cell for step-by-step instructions.
  - From the CommNet Browser, open the Cell Registration dialog box, select each CommCell then click **Modify**.
  - From the Modify CommCell dialog box, type a new CommNet interface name in the CommNet Interface Name box.
  - Click **OK**.
  - After all the cells have been changed, click **Close** from the Cell Registration dialog box.
6. Synchronize the CommCell in the CommNet Browser to obtain up-to-date information about the CommCell. See Synchronize Cells for step-by-step instructions.
7. Disable all scheduled job and kill running jobs associated with the SQL Server *iDataAgent* in the primary CommNet Server.

#### Switching the CommNet Server Back From Standby to Primary When the Failure Condition is Cleared

1. Stop all services on the standby CommNet Server. See Services for more information.
2. In the standby CommNet Server, using the **SQL Server Management Studio**, backup the **CommNet** database and create a .dmp file. See the **SQL Server Management Studio** help for information on creating the dump file.
3. In the primary CommNet Server, using the **SQL Server Management Studio**, restore the **CommNet** database. See the **SQL Server Management Studio** help for information on restoring a database.
4. In the primary CommNet Server, start the services. See Start Services on Windows for step-by-step instructions.
5. Open the CommNet Console and re-apply the permanent license associated with the primary CommNet Server. See License Administration for more information.
6. Perform the following steps on all the CommCells that are registered with this CommNet Server: See Register a Cell for step-by-step instructions.
  - From the CommNet Browser, open the Cell Registration dialog box, select each CommCell then click **Modify**.
  - From the Modify CommCell dialog box, type a new CommNet interface name in the CommNet Interface Name box.
  - Click **OK**.
  - After all the cells have been changed, click **Close** from the Cell Registration dialog box.
7. Synchronize the CommCell in the CommNet Browser to obtain up-to-date information about the CommCell. See Synchronize Cells for step-by-step instructions.
8. Enable all schedules including the Backup Schedule for the SQL Server *iDataAgent*.

Back to Top