



Laptop Backup - Administrator Guide (Linux)

Laptop Backup - Administrator Guide (Linux)

TABLE OF CONTENTS

OVERVIEW

PREPARE COMMCELL

SETUP FIREWALL USING PROXY

SETUP FIREWALL WITHOUT PROXY

CREATE INSTALLATION PACKAGE

SETUP SELF SERVICE

ADVANCED OPTIONS

Scheduling Automatic Updates

Modifying The Contents Of The Subclient For Specific Laptop User

Configuring Network Bandwidth Throttling

Configuring Automatic Backup Schedules

Assigning Laptop Owners

Defining The Capabilities For Laptop Users

Defining Download Privilege to Laptop Owners

Modifying the Documentation Link for Backup Monitor

Enabling Secured Access for Web Search Client

License Requirements

Overview - Laptop Backup (DLO)

Overview

Prepare CommCell

Firewall Using Proxy

Firewall Without Proxy

Create Installation Package

Web Access

< Previous

Next >

The Laptop Backup (DLO) feature enables you to protect data residing on laptops and desktops used in remote locations. Laptop Backup offers the following key features:

- **Quick & Automated Backups:** Seamless backups using automatic schedules based on network connectivity.
- **Improved Resource Utilization:** Deduplication technology, coupled with intelligent backup scheduling dramatically improves the ability to protect distributed data with optimized disk resources.
- **Network Optimized Backups:** Backups over any network – LAN, WAN or VPN with dynamic bandwidth throttling.
- **Anytime, Anywhere Access:** Instant access to data using any web browser.
- **Integrated Security Features:** Full encryption at all stages and secured network access (HTTPS) used together for data security.
- **Automated Customization Based on Business Rules:** Ability to configure additional settings, such as encryption, content indexing before performing the backups.



< Previous

Next >

Prepare CommCell - Laptop Backup

Perform the following configurations on CommServe to enable laptop backup:

1. Create Storage Policy
2. Create a Client Group for Laptops
3. Configure Additional Settings Before Laptops Execute The First Backup
4. Create a Client Group for MediaAgent
5. Create a Schedule Policy
6. Create a Subclient Policy

PRE-REQUISITES

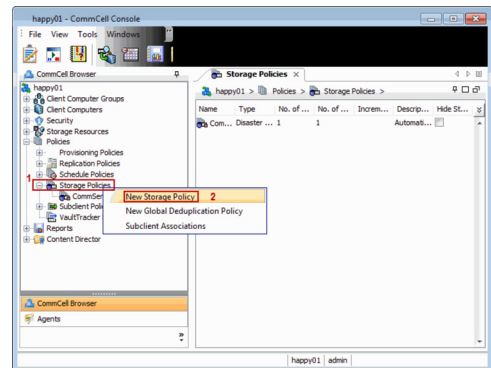
Ensure you have the following before performing the configuration:

- CommServe and MediaAgent software must be installed on the computer.
- Service Pack 12 (or higher) installed on the CommServe and MediaAgent.
- Disk Libraries must be configured.

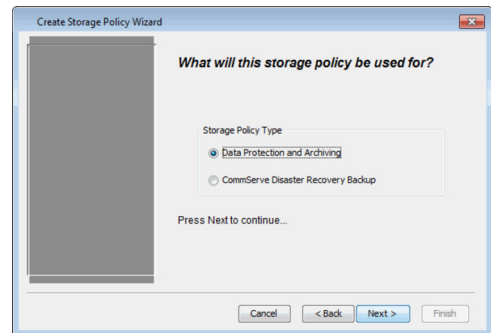
CREATE STORAGE POLICY

The Storage Policy act as a channel for backup and restore operations. It will map data from its original location to the physical media. Follow the steps given below to create a storage policy for the laptop backup:

1.
 - From the CommCell Browser, navigate to **Policies**.
 - Right-click the **Storage Policies** node and click **New Storage Policy**.



2. Click **Next**.



3.
 - Specify the name of the storage policy and in the **Storage Policy Name** box.
 - Click **Next**.

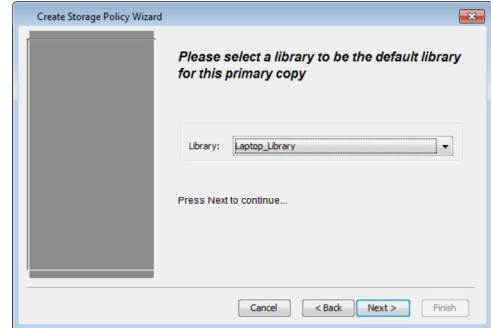
Note down the **Storage Policy** name.

This is needed later to assign storage policy to subclient during Create Subclient Policy.

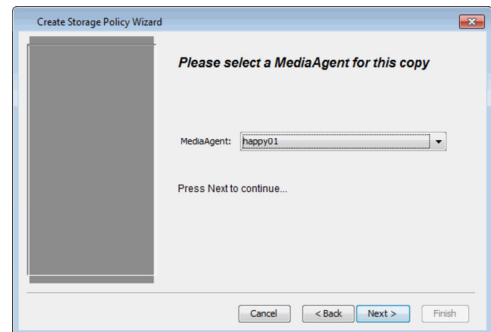
4.
 - In the **Library** list, select the default library to which the Primary Copy should be associated.
 - Click **Next**.



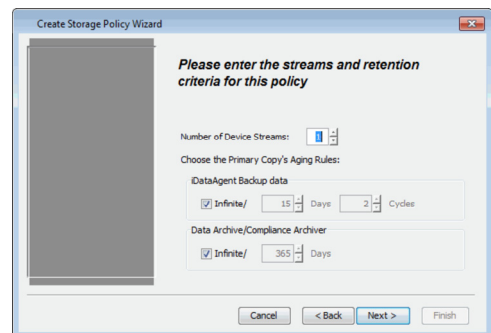
5. Select **MediaAgent** and click **Next**.



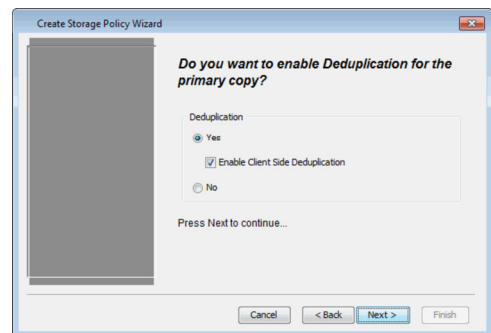
6. Click **Next**.



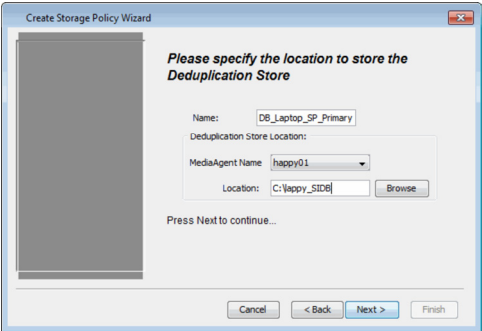
7. Click **Next**.
 Make Sure that **Enable Client Side Deduplication** is selected.



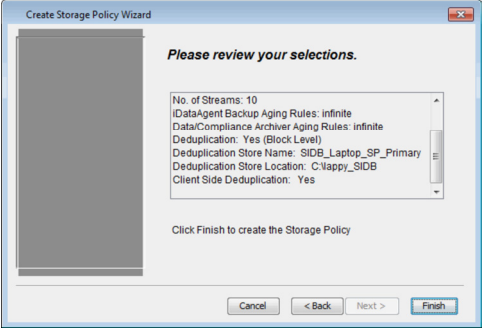
8. Verify **Name** and **MediaAgent Name**.
 Click **Browse** to specify location for **Deduplication Store**.



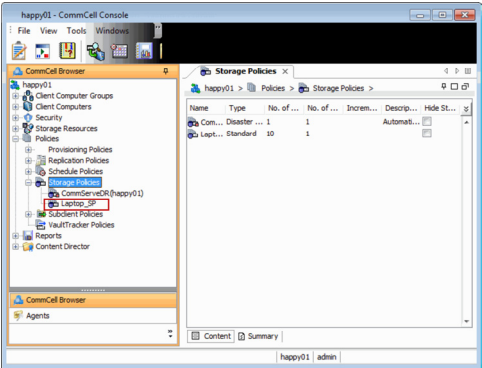
Click **Next**.



9. Review the details and click **Finish** to create the Storage Policy.



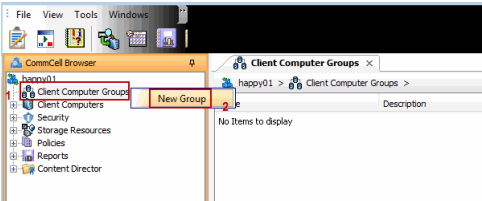
10. You can view the storage policy in the **Storage Policies** node.



CREATE A CLIENT GROUP FOR LAPTOPS

The client computer group is a logical grouping of client computers. Client Computer Group definition help to define options to the entire group instead of the individual clients. Follow the steps given below to create a client group for the laptops which you want to backup:

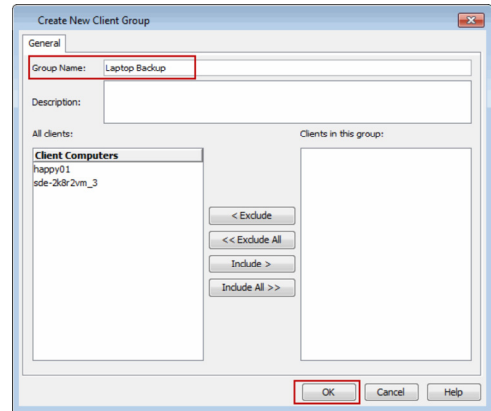
11. From the CommCell Browser, right-click **Client Computer Groups** node, and click **New Group**.



12.

- In the **Group Name** box, specify the name as **Laptop Backup**
- Click **OK**.

You can create an additional group and name it as **Waiting Room**. This group may be used as a staging area to configure any additional setting for the clients before performing the first backup. You can configure encryption, content indexing, client side deduplication etc for the client using command line scripts.



CONFIGURE ADDITIONAL SETTINGS BEFORE LAPTOPS EXECUTE THE FIRST BACKUP

You can configure several additional settings for laptops before allowing them to backup for the first time. For example:

- Enable Client Level Encryption
- Enable Content Indexing
- Enable Client Side Deduplication

Follow the steps given below to configure any additional settings:

13.
 - Use the following steps to download the script needed for this task:
 - Click the **Download Now** button located on the right.
 - Select a location to save the .zip file.
 - Navigate to the location of the .zip file and unzip the file.
 - Modify the script to select the additional settings which you want to configure.
 - Schedule a task to run this script after a specific time interval. You can use Windows Task Scheduler to schedule this task.

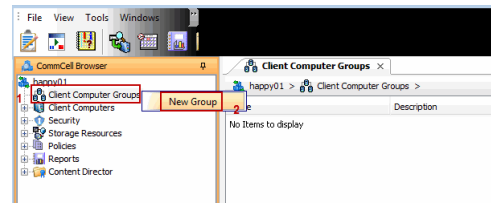


When the user installs the **Installation Package** on a laptop, the laptop will be added to the **Waiting Room** client group. This script will configure the additional settings for the laptops in the waiting room and then move the laptop from the **Waiting Room** group to **Laptop Backup** group. After the laptop moves to the **Laptop Backup** group, the backups will be performed as per the schedule policy.

CREATE A CLIENT GROUP FOR MEDIAAGENT

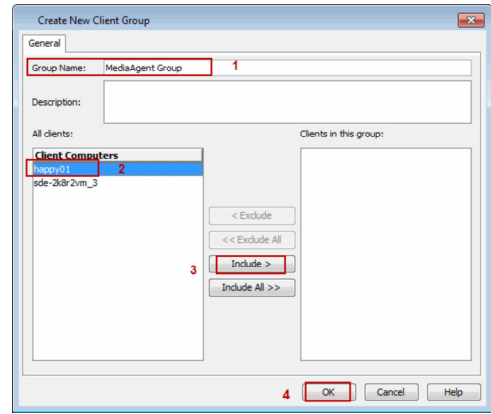
The MediaAgent monitors the transfer of data between client computer and media. Follow the steps given below to create a client group for all the MediaAgents which will be used for the backup and restore:

14. From the CommCell Browser, right-click **Client Computer Groups** node, and click **New Group**.



15. In the **Group Name** box, specify the name for the MediaAgent Group.
 - Add the MediaAgents to the group by clicking **Include** button.
 - Click **OK**.

Add the MediaAgents which are not installed on the same CommServe computer and used for backing up the clients data.

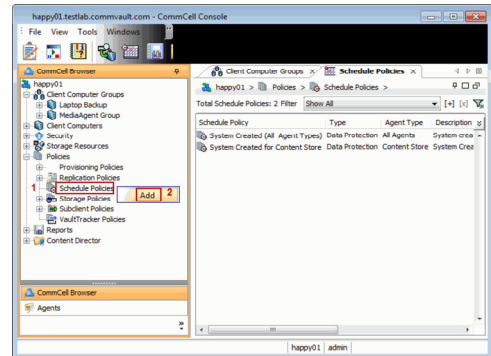


CREATE SCHEDULE POLICY

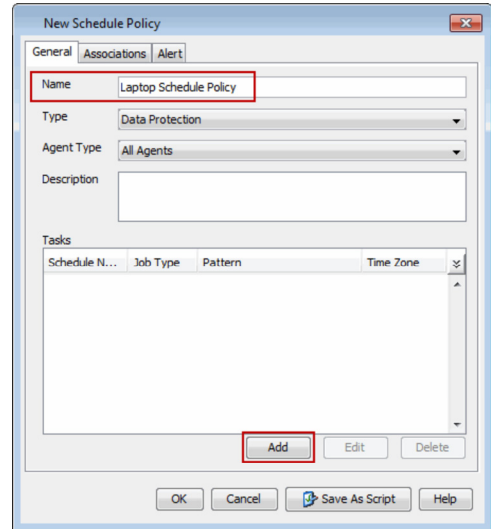
When multiple clients or tasks require similar operations to be scheduled you can create a schedule policy as a scheduling template and attach it to the respective client or task in the CommCell.

Use the following steps to create a schedule policy.

16.
 - From the CommCell Browser, navigate to **Policies**.
 - Right-click **Schedule Policies** node and then click **Add**.



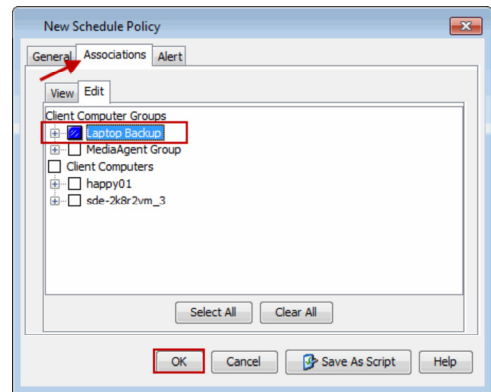
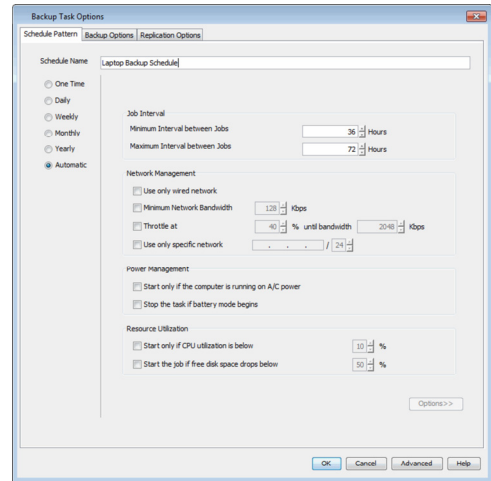
17.
 - In the **Name** box, specify the name of the Schedule Policy.
 - Click **Add** button.



18. In the **Schedule Name** box, enter a name of the schedule pattern. Select **Automatic** and Click **OK**.

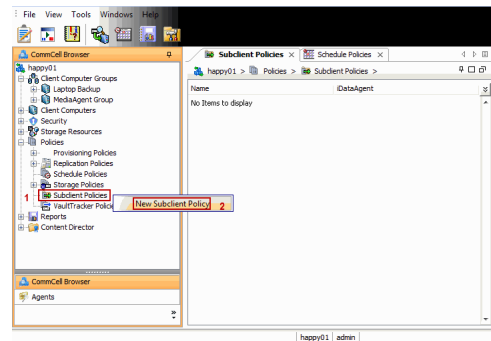
Automatic backup schedule does not perform synthetic full backups.

19.
 - Click **Associations** tab.
 - Select the **Laptop Backup** client group.
 - Click **OK**.

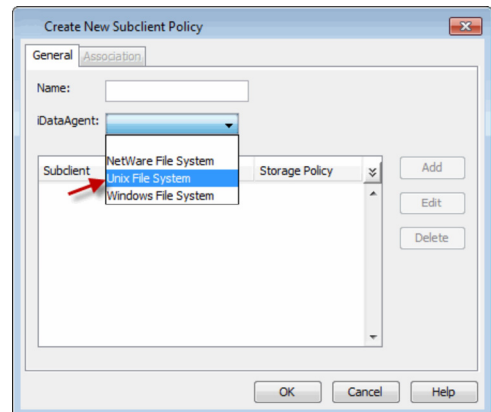


CREATE SUBCLIENT POLICY

20. From the CommCell Browser, navigate to **Policies** right-click **Subclient Policies** node, and click **New Subclient Policy**.

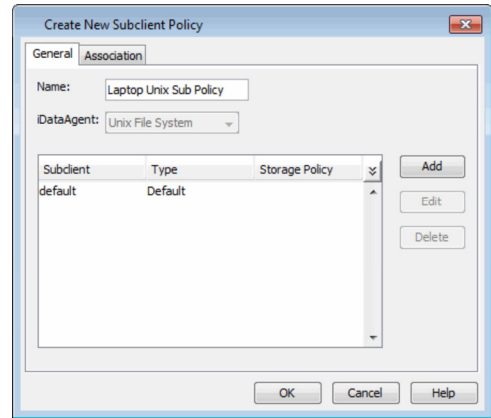


21.
 - In the **Name** box, enter the name of the subclient policy.
 - In the **iDataAgent** list, select **Unix File System**.
 - Note down the Subclient Policy **Name**.
 - This is needed later during Custom Package creation.

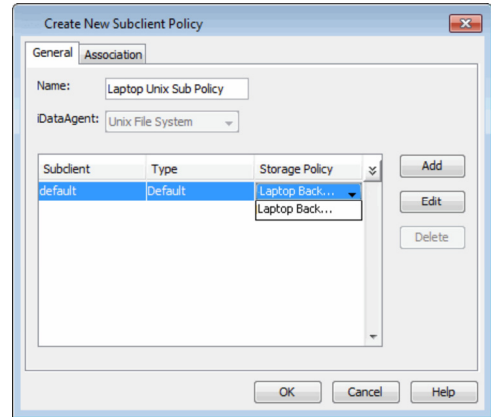


22. The display pane will display default subclient.

23. Assign a Storage Policy for a subclient created in step 3 during Create Storage Policy.



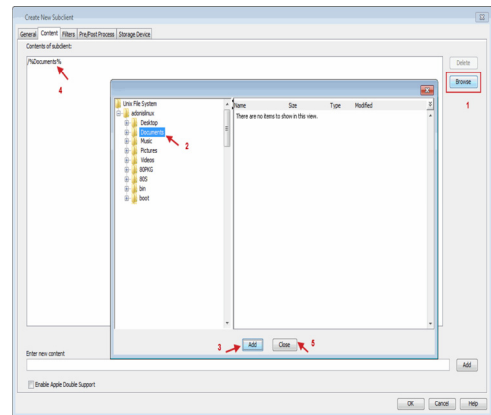
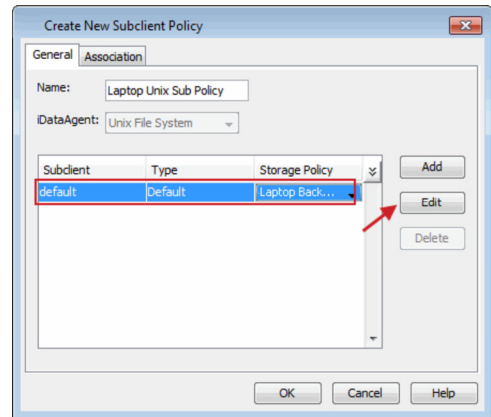
24. Select the subclient and then click **Edit**.



- 25.
- Click **Content** tab.
 - Click **Browse** and expand the **Unix File System** node.
 - Select the required backup content location, e.g. /Documents and click **Add**.
 - Click **Close**.

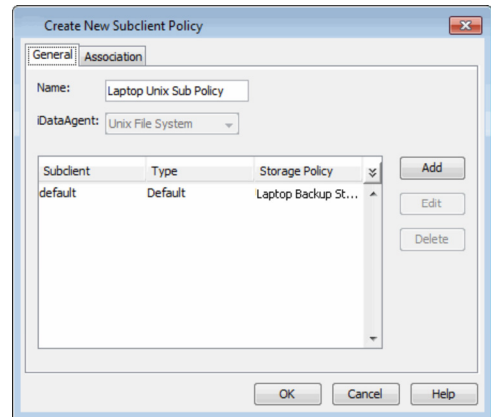
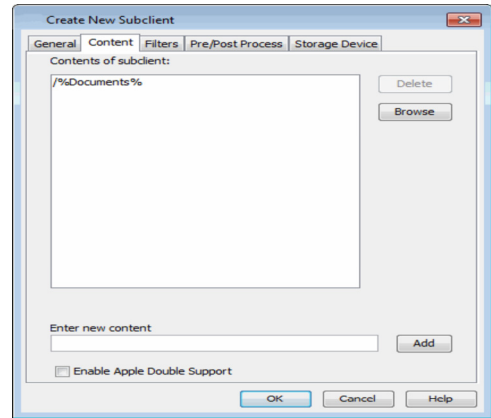
The contents (e.g. word processing documents, digital photos, music files and so on) of folders (e.g. Documents, Music, Videos, etc.,) specified in the above location will be backed up.

The Administrator must request the users to copy the files and folders to be backed up to this folder.



26. Click **OK**.

27. Click **OK**.



Setup Firewall Using Proxy - Laptop Backup

Overview

Prepare CommCell

Firewall Using Proxy

Firewall Without Proxy

Create Installation Package

Web Access

◀ Previous

Next ▶

SKIP THIS STEP IF YOU ARE NOT USING PROXY SERVER

Click **Next** ▶ to Continue.

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.

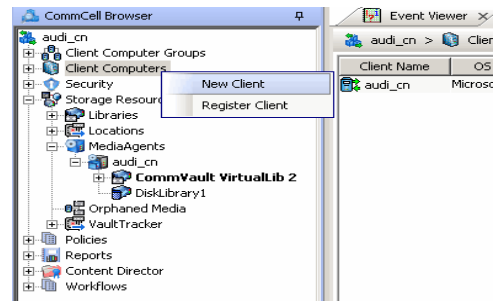
The following sections explain the steps involved in operating through a GatewayProxy:

1. Preconfigure the GatewayProxy
2. Configure Firewall on Client Group
3. Configure Firewall on CommServe
4. Configure Firewall on MediaAgent
5. Install on GatewayProxy
6. Verify the GatewayProxy

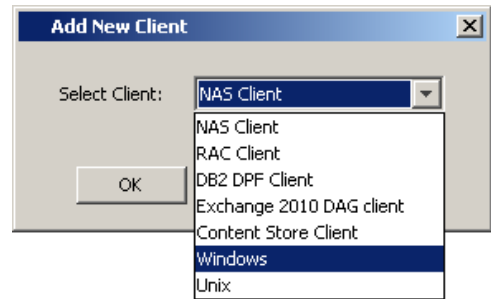
PRECONFIGURE THE GATEWAYPROXY

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

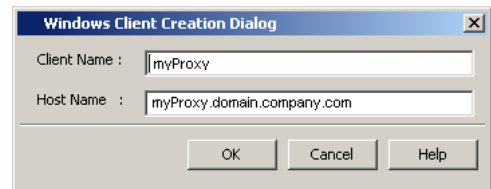
1. From the CommCell Console, right-click on the **Client Computers**, and click **New Client**.



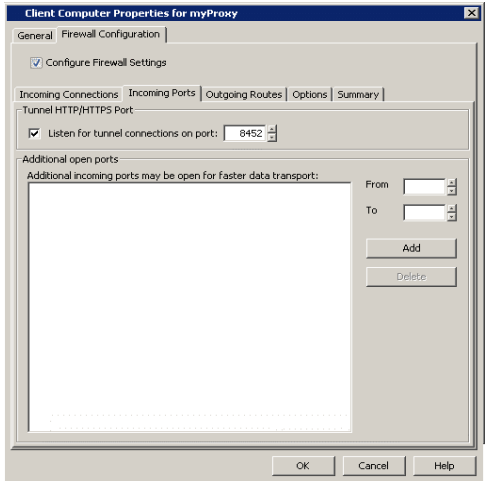
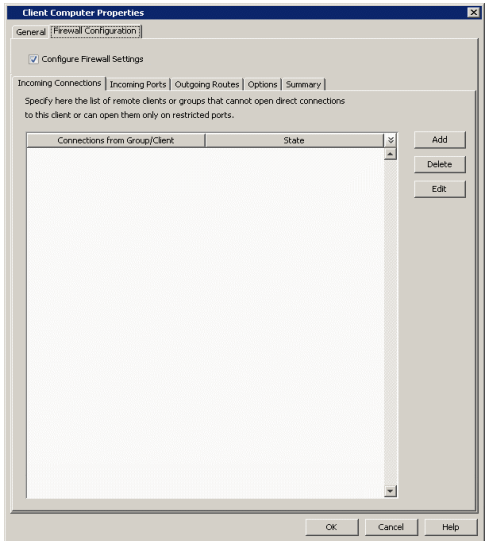
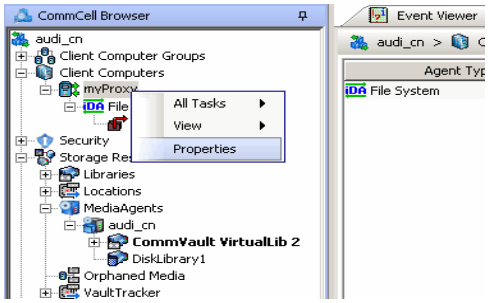
2. Select **Windows** or **Unix** as applicable from drop-down list.
Click **OK**.



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



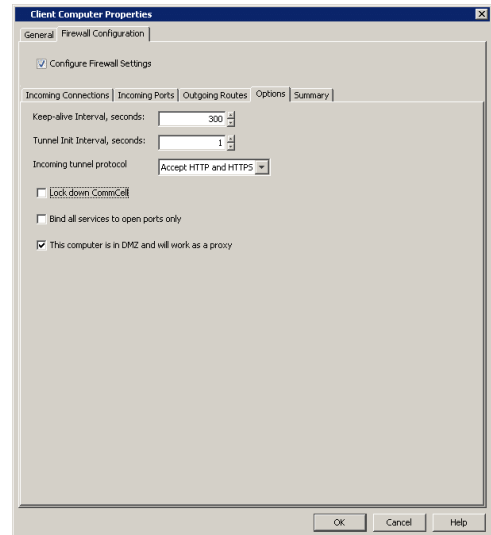
4. From the CommCell Console, right-click the client you just created, and click **Properties**.



- 5. Click the **Firewall Configuration** tab.
Select **Configure Firewall Settings** box.

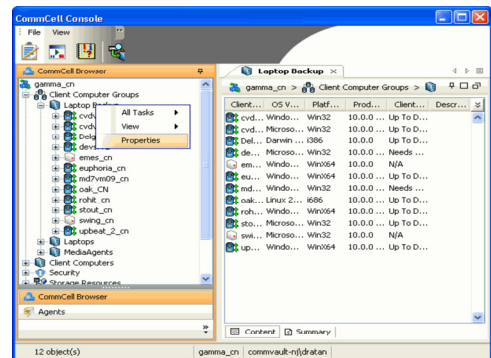
- 6. Click the **Incoming Ports** tab.
Select **Listen for tunnel connections on port** and enter port number on which the GatewayProxy will listen from the CommServe.

- 7. Click **Options** tab.
Clear **Lock down CommCell**.
Select **This computer is in DMZ and will work as proxy**.
Click **OK**.

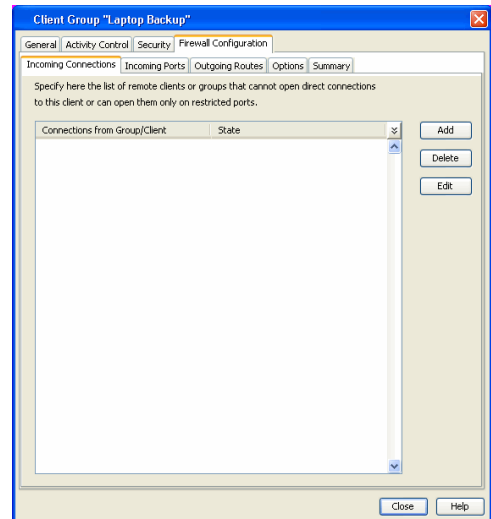


CONFIGURE FIREWALL ON CLIENT GROUP

8. From **CommCell Browser**, navigate to **Client Computer Groups**, select and right-click the **Laptop Backup** group and click **Properties**.

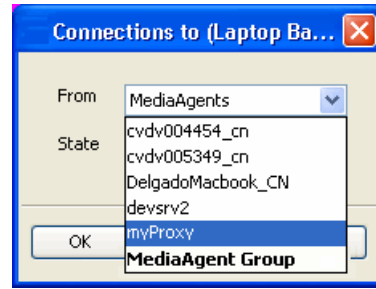


- 9.
- Click **Firewall Configuration** tab.
 - Select **Configure Firewall Settings** box.
 - Click **Add** button.



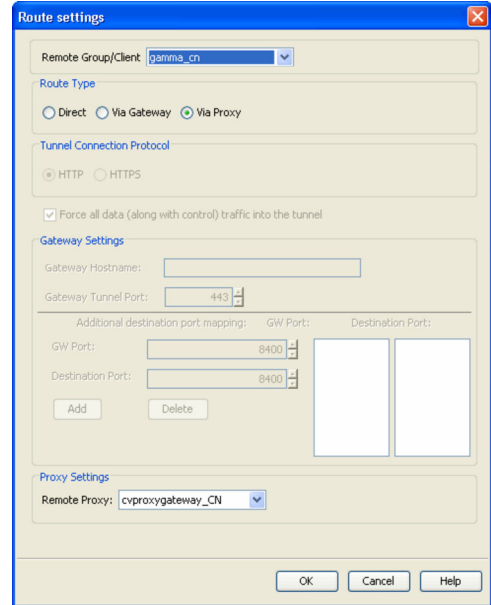
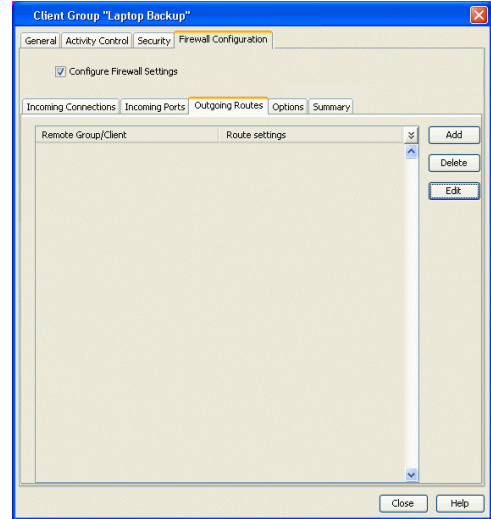
- 10.
- Select **GatewayProxy** computer from **From** drop-down list.
 - Select **Blocked** from **State** drop-down list.
 - Click **OK**.

11. Select **Outgoing Routes** tab.
Click **Add**.

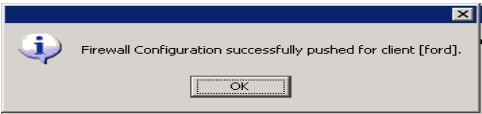
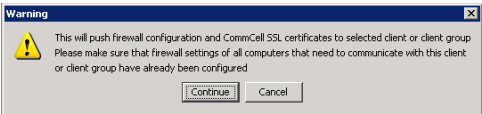
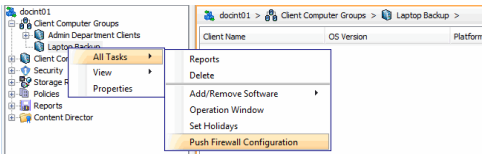
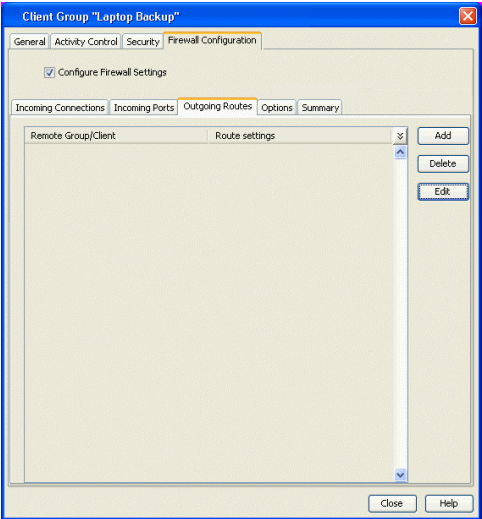


12.
 - Select the **CommServe** from the **Remote Group/Client** drop-down list.
 - Select **Via Proxy**.
 - Select **GatewayProxy** computer from **Remote Proxy** drop-down list.
 - Click **OK**.

If MediaAgents are installed on separate computer, repeat the steps described above and select the **MediaAgent group** in the **Remote Group/Client** list.



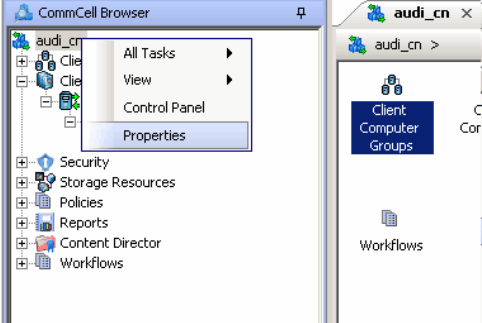
13. Click **OK**.



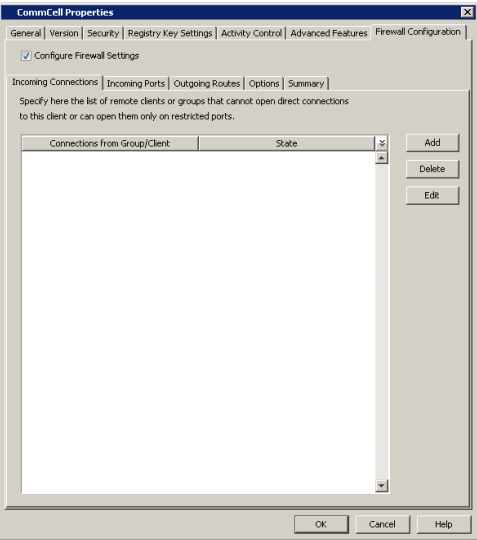
14.
 - From the CommCell Browser, navigate to **Client Computer Groups**.
 - Right-click the **Laptop Backup** group and point All Tasks and then click **Push Firewall Configuration**.
15. Click **Continue**.
16. The specified configuration is saved.
The firewall configuration was pushed successfully.
17. The newly added clients will automatically be registered in the client group and will hence inherit the firewall settings established in the client group.

CONFIGURE FIREWALL ON COMMSERVE

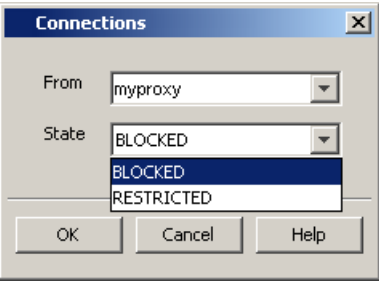
18. From the CommCell Console, right-click the CommServe computer and click **Properties**.



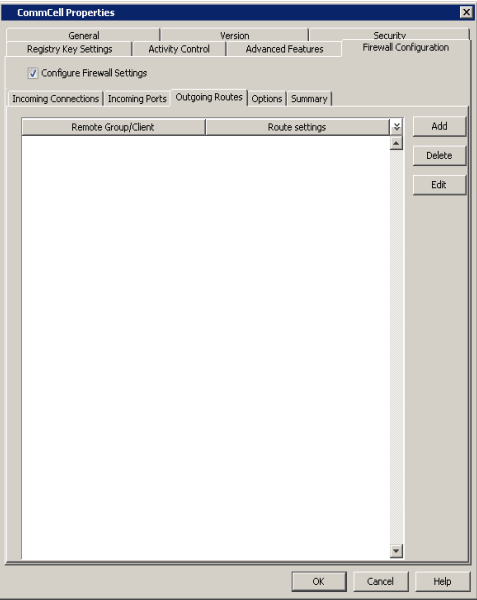
19.
 - Click the **Firewall Configuration** tab.
 - Select **Firewall Configuration Settings** box.
 - Click **Add**.



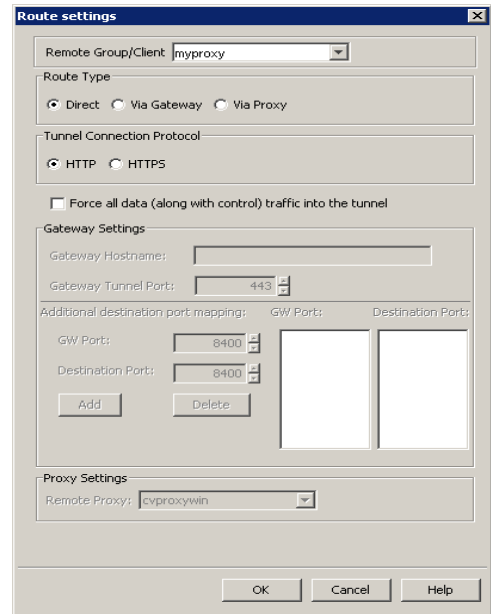
- 20.
 - Select **GatewayProxy** computer from **From** drop-down list.
 - Select **Blocked** from **State** drop-down list.
 - Click **OK**.



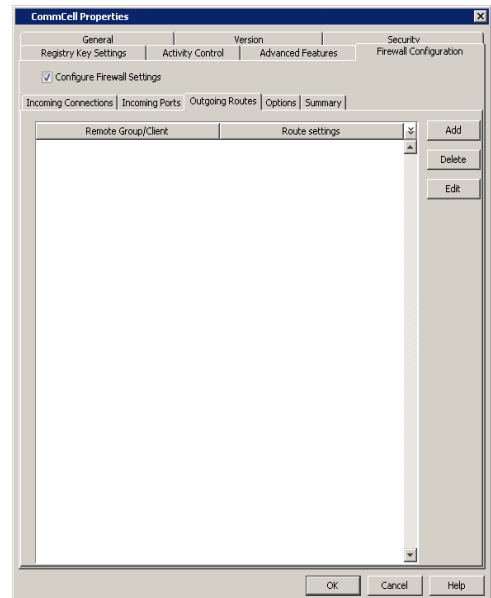
- 21.
 - Click the **Outgoing Routes** tab.
 - Click **Add**.



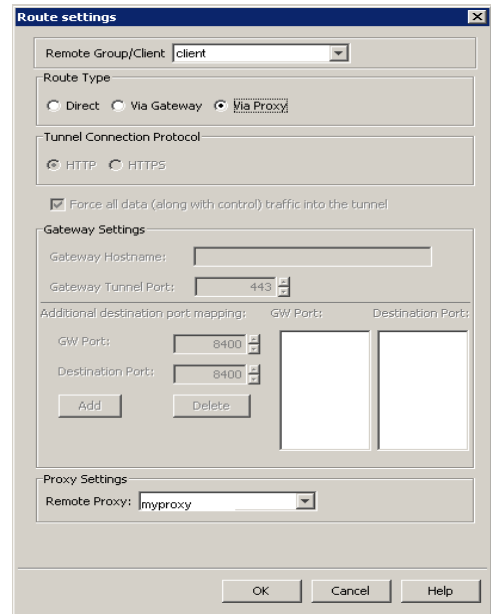
- 22.
 - Select the **GatewayProxy** computer in **Remote Group/Client**.
 - Click **OK**.



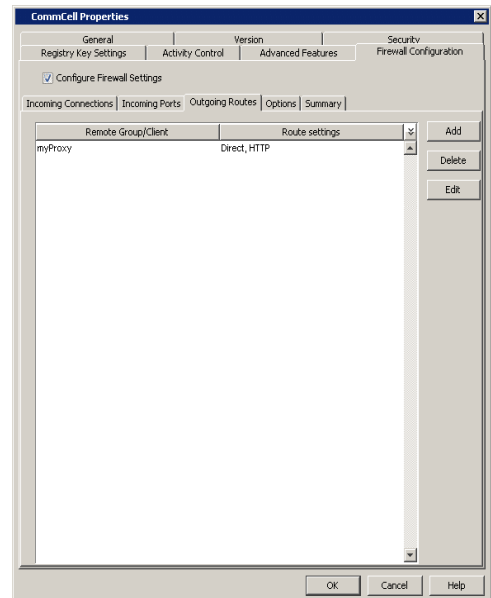
23. Click **Add**.



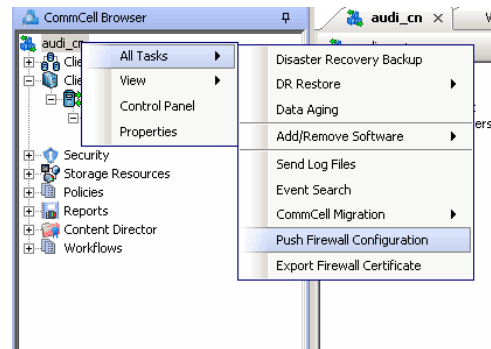
- 24.
- Select the **Laptop Backup** client group from the **Remote Group/Client** drop-down list.
 - Select **Via Proxy**.
 - Select **GatewayProxy** computer from **Remote Proxy** drop-down list.
 - Click **OK**.



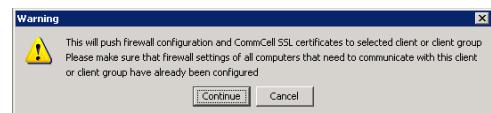
25. Click **OK**.



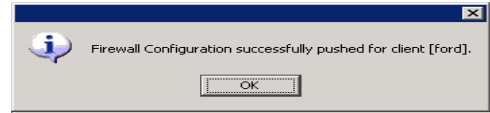
26. From the CommCell Console right-click the CommServe computer, click **All Tasks**, and click **Push Firewall Configuration**.



27. Click **Continue**.



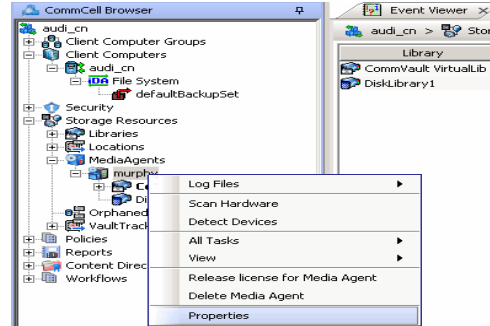
28. Click **OK**.



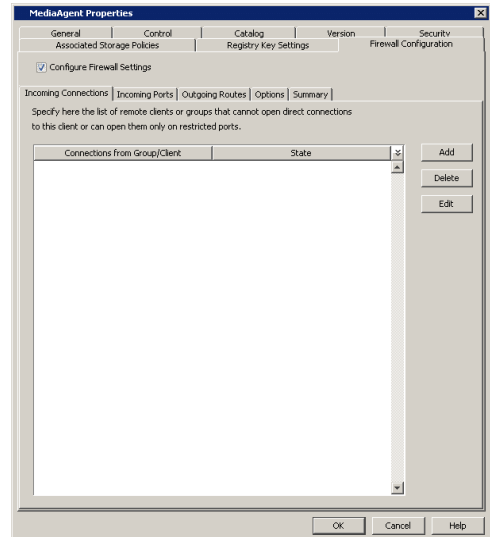
CONFIGURE FIREWALL ON MEDIAAGENT

SKIP THIS SECTION IF MEDIAAGENT IS SAME AS COMMSERVE

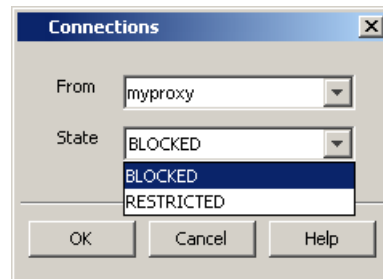
29. From the CommCell Console, navigate to **Storage-Resource | MediaAgents**, select and right-click **<media_agent>** and click Properties



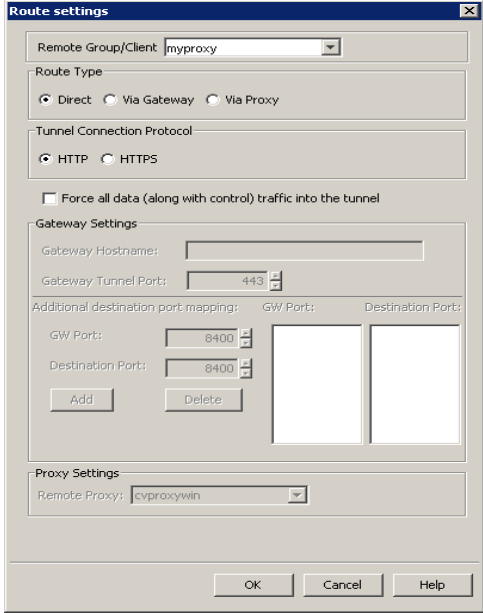
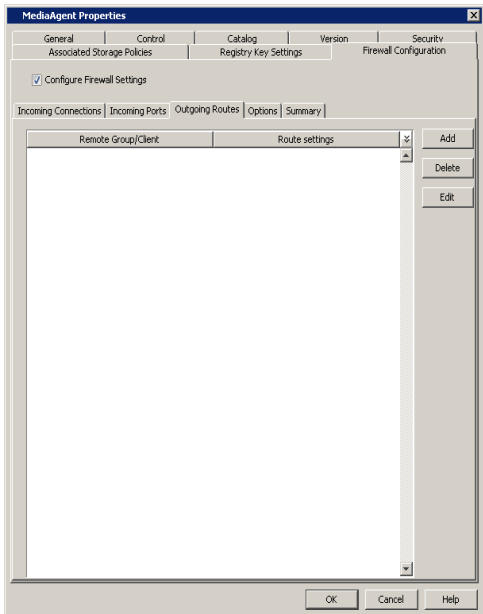
- 30.
- Click the **Firewall Configuration** tab.
 - Select **Configure Firewall Settings** box.
 - From the **Incoming Connections** tab, click **Add**.



- 31.
- In the **From** field, select the GatewayProxy computer.
 - In the **State** field, select **Blocked**.
 - Click **OK**.

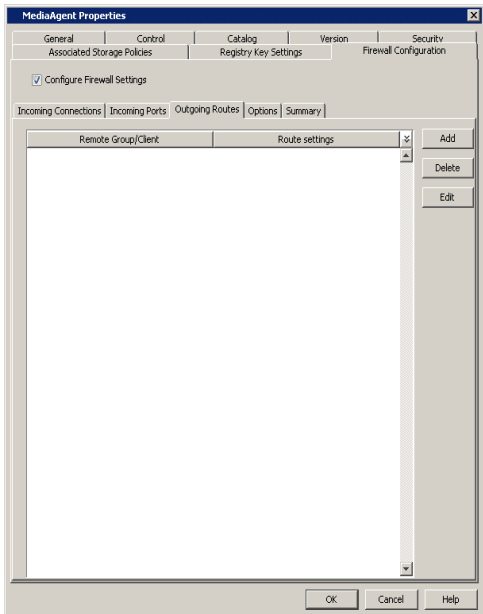


32. Click the **Outgoing Routes** tab.
Click **Add**.

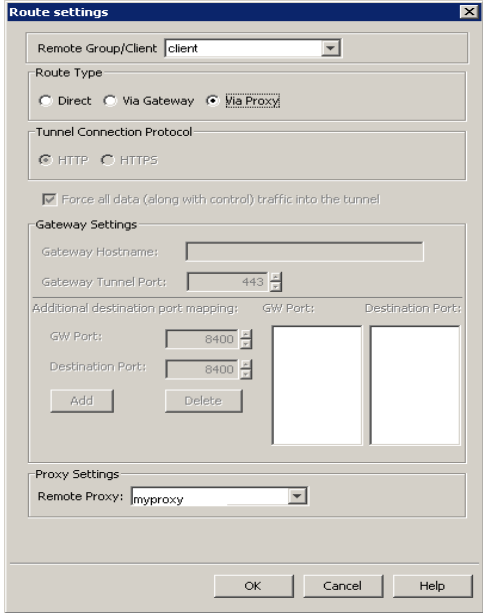


- 33.
- Specify the route from **MediaAgent Group** to the GatewayProxy in **Remote Group/Client** drop-down list.
 - Click **OK**.

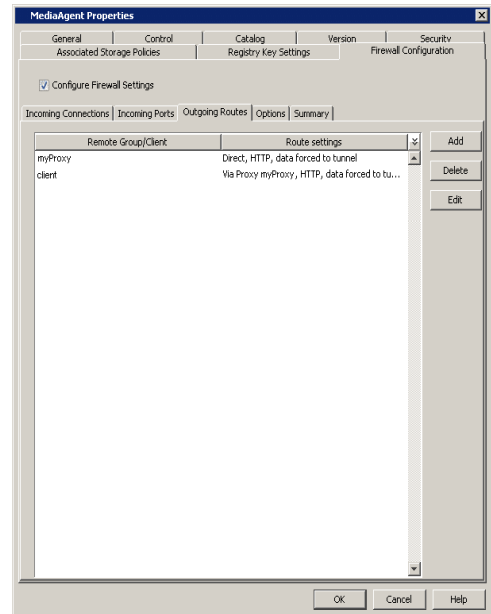
34. Click **Add**.



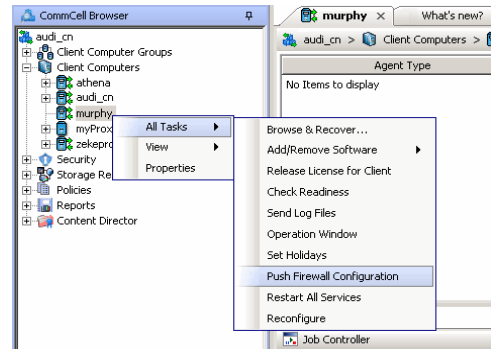
- 35.
- Select the client computer in **Remote Group/Client**.
 - Select **Via Proxy**.
 - Select the GatewayProxy in **Remote Proxy**.
 - Click **OK**.



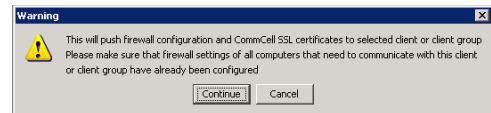
36. Click **OK**.
- The **Outgoing Routes** tab must display two routes: the route from MediaAgent to the proxy and the route from MediaAgent to the client through the proxy.
- The MediaAgent is configured to receive communication from the client through the GatewayProxy.



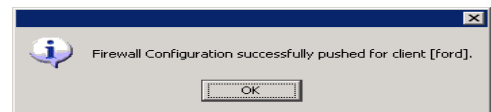
37. From the CommCell Console, right-click the MediaAgent computer and click **All Tasks | Push Firewall Configuration**.



38. Click **Continue**.
The MediaAgent is configured to receive communication from the client through the GatewayProxy.



39. Click **OK**.
You are now ready to install the **GatewayProxy**.



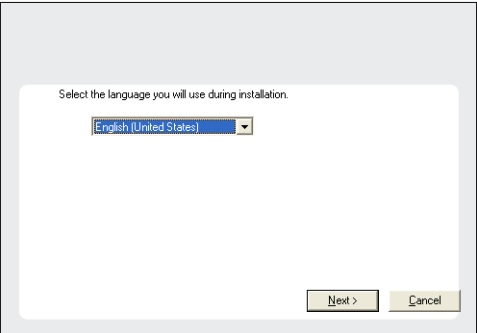
INSTALL ON GATEWAYPROXY

Install the CommCell client software using one of the following methods on GatewayProxy computer:

- Install GatewayProxy for Windows Client
- Install GatewayProxy for Unix Client

INSTALL GATEWAYPROXY FOR WINDOWS CLIENT

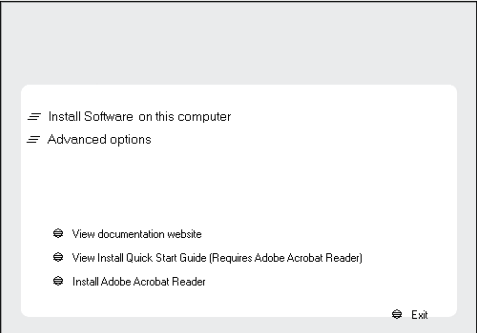
1. Run **Setup.exe** from the **Software Installation Disc** in the **GatewayProxy** computer.
2. Select the required language.
Click **Next**.



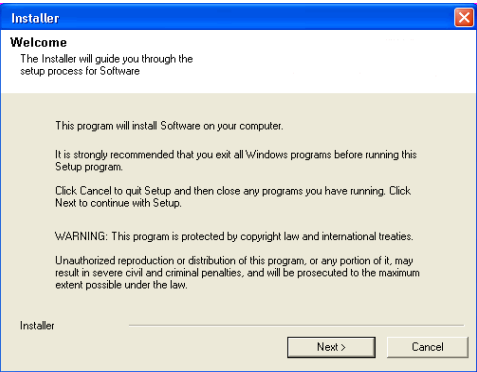
3. Select the option to install software on this computer.

NOTES

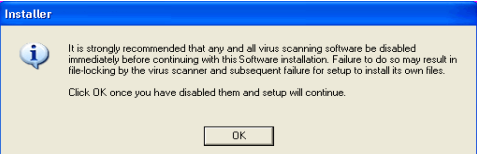
- The options that appear on this screen depend on the computer in which the software is being installed.



4. Click **Next**.

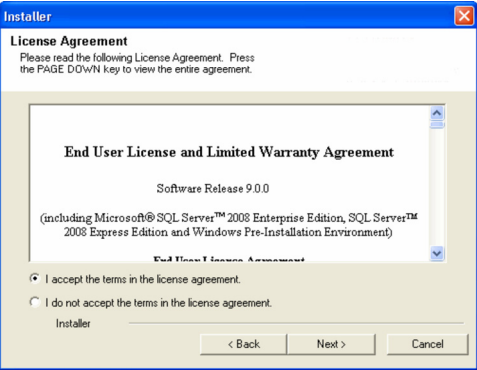


5. Click **OK**.



6. Select **I accept the terms in the license agreement**.

Click **Next**.



7. Expand **Client Modules | Backup & Recovery | File System** and select **Windows File System iDataAgent**.

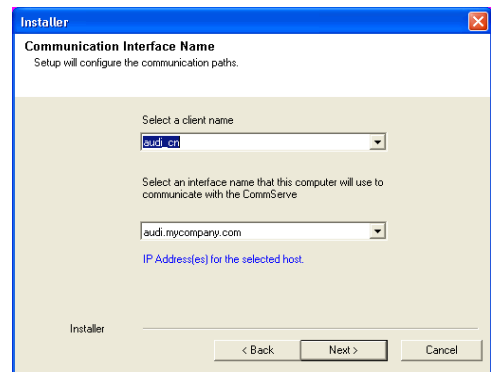
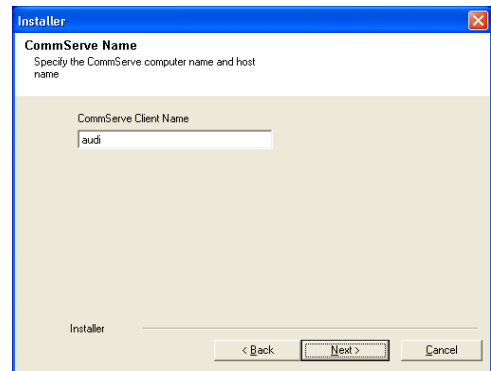
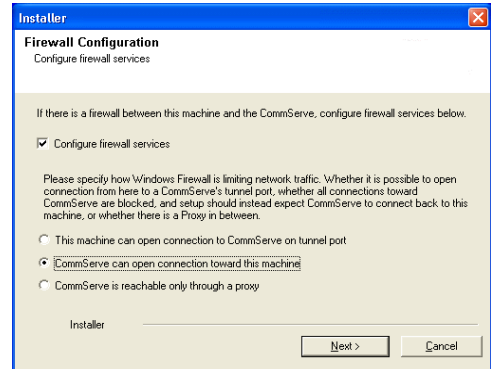
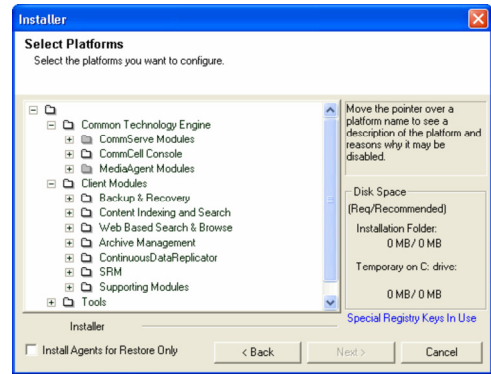
Click **Next**.

8. Select the **Configure Firewall Services** box.
Select **CommServe can open connection toward this machine** and click **Next**.

9. Enter the name of the computer in **CommServe client name** field.
Click **Next**.

10. Click **Next**.

11. Specify a local port number through which the Client/MediaAgent will receive communication from the CommServe.
Click **Next**.



12. Specify the port numbers to be used by the Bull Calypso Communications Service (CVD) and Bull Calypso Client Event Manager (EvMgr) Services.

Click **Next**.

- Valid range for the port number is between 1024 and 65000.
- Ensure that the port numbers specified here are within the valid range and are not used by any other services.

13. Click **Next**.

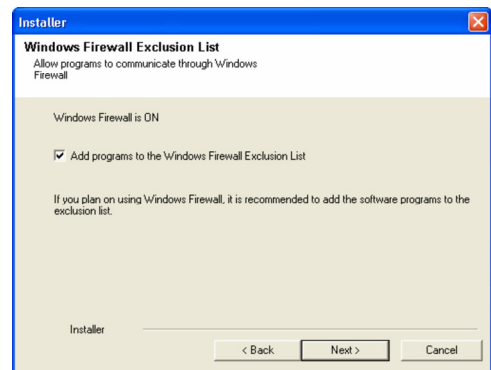
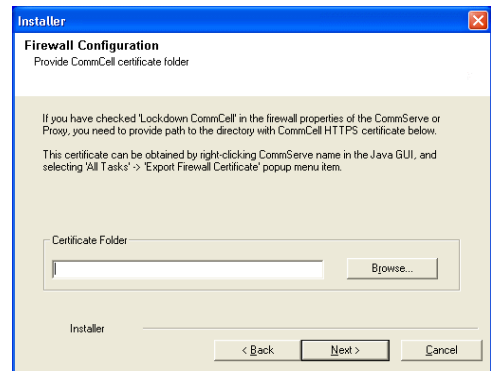
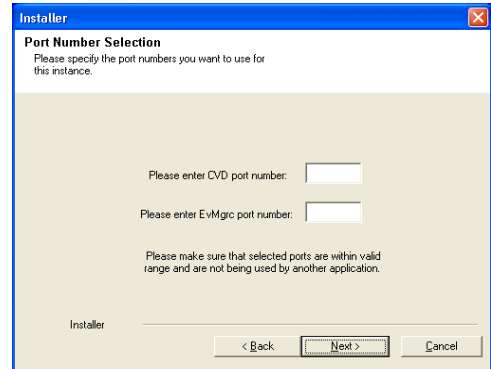
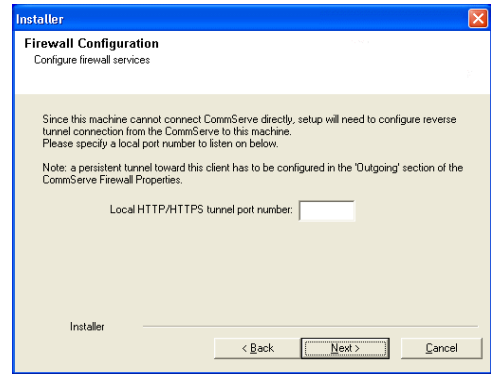
14. Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.

Click **Next**.

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

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

15. Click **Next**.



16. Verify the default location for software installation.

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

Click **Next**.

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

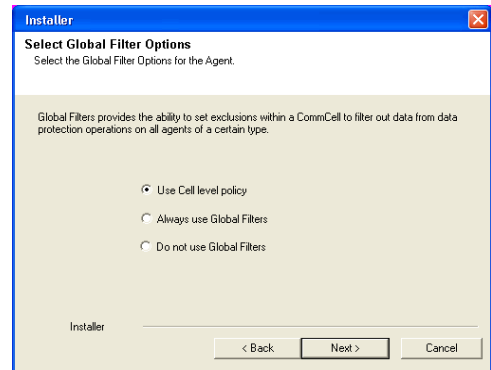
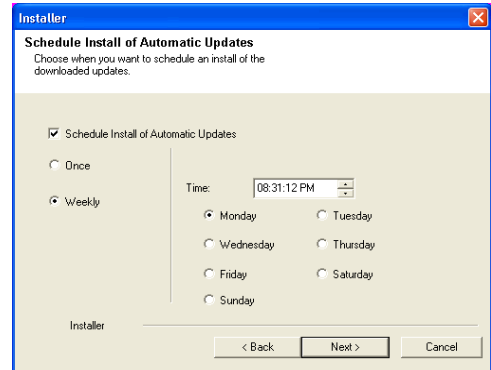
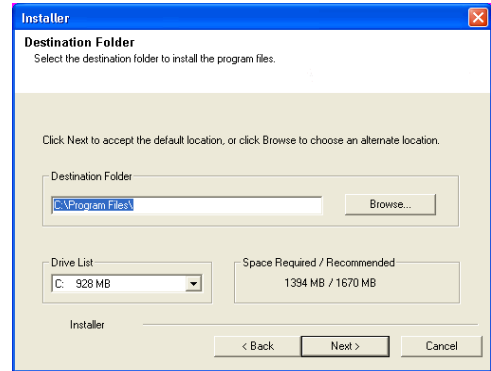
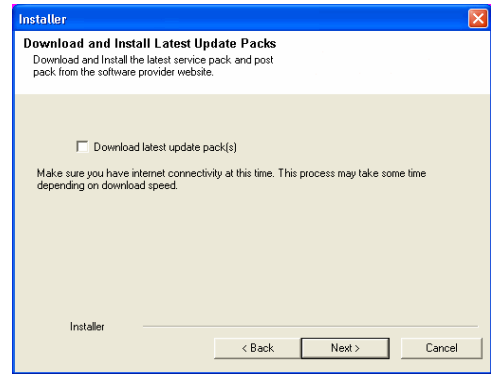
/ : * ? " < > | #

It is recommended that you use alphanumeric characters only.

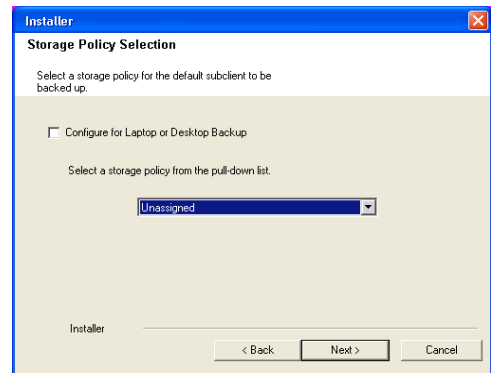
17. Click **Next**.

18. Click **Next**.

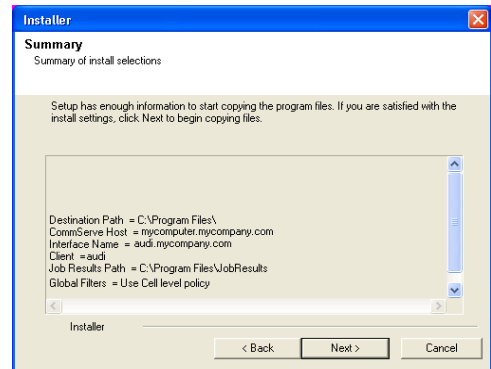
19. Click **Next**.



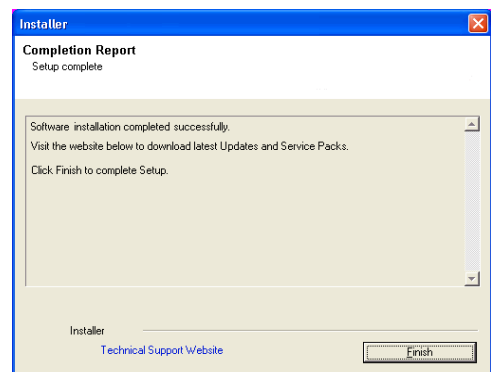
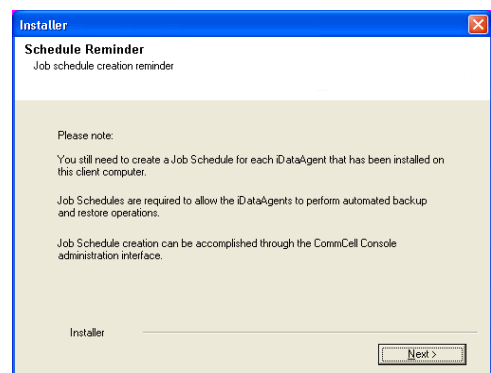
20. Click **Next**.



21. Click **Next**.



22. Click **Finish**.



INSTALL GATEWAYPROXY FOR UNIX CLIENT

1. Place the **Software Installation Disc** on a GatewayProxy computer.
2. Run the following command from the Software Installation Disc:
./cvpkgadd
3. The product banner and other information is displayed.
Press **Enter** to continue.

4. Read the license agreement. Type **y** and press **Enter** to continue.
5. Press **Enter**.

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

Advanced 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) Advanced options
- 3) Exit this menu

Your choice: [1]

7. Press **Enter**.

Certain Calypso packages can be associated with a virtual IP, or in other words, installed on a "virtual machine" belonging to some cluster. At any given time the virtual machine's services and IP address are active on only one of the cluster's servers. The virtual machine can "fail-over" from one server to another, which includes stopping services and deactivating IP address on the first server and activating the IP address/services on the other server.

You now have a choice of performing a regular Calypso install on the physical host or installing Calypso on a virtual machine for operation within a cluster.

Most users should select "Install on a physical machine" here.

- 1) Install on a physical machine
- 2) Install on a virtual machine
- 3) Exit

Your choice: [1]

8. Press **Enter**.

We found one network interface available on your machine. We will associate it with the physical machine being installed, and it will also be used by the CommServe to connect to the physical machine. Note that you will be able to additionally customize Datapipe Interface Pairs used for the backup data traffic later in the Calypso Java GUI.

Please check the interface name below, and make connections if necessary:

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

9. Press **Enter**.

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]

10. Type the appropriate number to install **Unix File System iDataAgent**.
A confirmation screen will mark your choice with an "X".
Type **d** for **Done**, and press **Enter**.

Install Calypso on physical machine 172.19.99.62

Please select the Calypso module(s) that you would like to install.

```
[ ] 1) MediaAgent [1301] [CVGxMA]>
[ ] 2) UNIX File System iDataAgent [1101] [CVGxIDA]

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

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

11. Press **Enter**.

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

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

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

- 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.

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

13. Press **Enter**.

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.

14. Press **Enter** to accept the default path and continue, or
Enter a path to modify the default path and press **Enter**.
Do not use the following characters when specifying the path:
!@#%&*():/?\
15. Press **Enter** to accept the default location for the log files and continue, or
Enter a path to modify the default location and press **Enter**.
16. Press **Enter**.
17. Type the **Group name** and press **Enter**.
Press **Enter** again.
18. Type a network TCP port number for the Communications Service (CVD) and press **Enter**.
Type a network TCP port number for the Client Event Manager Service (EvMgrC) and press **Enter**.
19. If this computer and the CommServe is separated by a firewall, type **Yes** and then press **Enter**.
20. Type **2** to select **CommServe can open connection toward us** option and press **Enter**.
21. Enter the client name of the CommServe computer in place of **CommServe Client**

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]

Please specify where you want us to install Calypso binaries.

It must be a local directory and there should be at least 176MB 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]

Please specify where you want to keep Calypso log files.

It must be a local directory and there should be at least 100MB of free space available. All log files will be created in a "calypso/Log_Files" subdirectory, so if you enter "/var/log", the logs will actually be placed into "/var/log/calypso/Log_Files".

Log Directory: [/var/log]

Most of Software processes run with root privileges, but some are launched by databases and inherit database access rights. To make sure that registry and log files can be written to by both kinds of processes we can either make such files world-writeable or we can grant write access only to processes belonging to a particular group, e.g. a "calypso" or a "dba" group.

We highly recommend now that you create a new user group and enter its name in the next setup screen. If you choose not to assign a dedicated group to Software processes, you will need to specify the access permissions later.

If you're planning to backup Oracle DB you should use "dba" group.

Would you like to assign a specific group to Software? [yes]

Please enter the name of the group which will be assigned to all Software files and on behalf of which all Software processes will run.

In most of the cases it's a good idea to create a dedicated "calypso" group. However, if you're planning to use Oracle iDataAgent or SAP Agent, you should enter Oracle's "dba" group here.

Group name: skyl

REMINDER

If you are planning to install Calypso Informix, DB2, PostgreSQL, Sybase or Lotus Notes iDataAgent, please make sure to include Informix, DB2, etc. users into group "skyl".

Press <ENTER> to continue ...

Every instance of Calypso should use a unique set of network ports to avoid interfering with other instances running on the same machine.

The port numbers selected must be from the reserved port number range and have not been registered by another application on this machine.

Please enter the port numbers.

Port Number for CVD : [8600]

Port Number for EvMgrC: [8602]

Is there a firewall between this client and the CommServe? [no] Yes

Please specify now how your firewall is limiting network traffic. Whether it's possible to open connection from here to a CommServe's tunnel port, whether all connections toward CommServe are blocked, and we should instead expect CommServe to connect back to us, or whether there is a proxy in between.

1) This machine can open connection to CommServe on a tunnel port
2) CommServe can open connections toward us
3) CommServe is reachable only through a proxy

Your choice: [1]

Please specify client name of the CommServe below.

Name.

Press **Enter**.

CommServe Client Name: mycompany

22. Specify a local port number through which the Client/MediaAgent will receive communication from the CommServe.

Press **Enter**.

Since we cannot contact CommServe directly, we will need to configure a reverse tunnel connection from the CommServe to us. Please enter a local port number to listen on below, then go to CommServe and create a persistent tunnel toward this client in the [outgoing] section of FwConfigLocal.txt. When finished, return to this configuration screen, and hit Enter to continue.

Local HTTP/HTTPS tunnel port number: 8550

23. Press **Enter**.

If you have checked "Lockdown CommCell" in firewall properties of the CommServe or Proxy, you need to provide path to the directory with CommCell HTTPS certificate below.

This certificate can be obtained by right-clicking CommServe name in the Java GUI, and selecting All Tasks -> Export Firewall Certificate popup menu item.

Have you enabled "Lockdown CommCell"? [no]

24. Press **Enter**.

Commcell Level Global Filters are set through Calypso GUI's Control Panel in order to filter out certain directories or files from backup Commcell-widely. If you turn on the Global filters, they will be effective to the default subclient. There are three options you can choose to set the filters.

- 1) Use Cell level policy
- 2) Always use Global filters
- 3) Do not use Global filters

Please select how to set the Global Filters for the default subclient? [1]

25. Type the number of a Client Group and press **Enter**.
A confirmation screen will mark your choice with an "X". Type **d** for done with the selection, and press **Enter** to continue.

This screen will be displayed only if Client Groups are configured for the CommCell.

Client Group(s) is currently configured on CommServe cs.company.com. Please choose the group(s) that you want to add this client client.company.com to. The selected group(s) will be marked (X) and can be deselected if you enter the same number again. After you are finished with the selection, select "Done with the Selection".

[] 1) Unix

[] 2) DR

[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

26. Enter the number corresponding to the storage policy through which you want to back up the Unix File System iDataAgent and press **Enter**.

Please select one storage policy for this IDA from the list below:

- 1) SP_StandAloneLibrary2_2
- 2) SP_Library3_3
- 3) SP_MagLibrary4_4

Storage Policy: [1]

27. Type **3** to the **Exit** option and press **Enter**.

The installation is now complete.

Certain Calypso packages can be associated with a virtual IP, or in other words, installed on a "virtual machine" belonging to some cluster. At any given time the virtual machine's services and IP address are active on only one of the cluster's servers. The virtual machine can "fail-over" from one server to another, which includes stopping services and deactivating IP address on the first server and activating the IP address/services on the other server.

Currently you have Calypso installed on physical node stone.company.com.

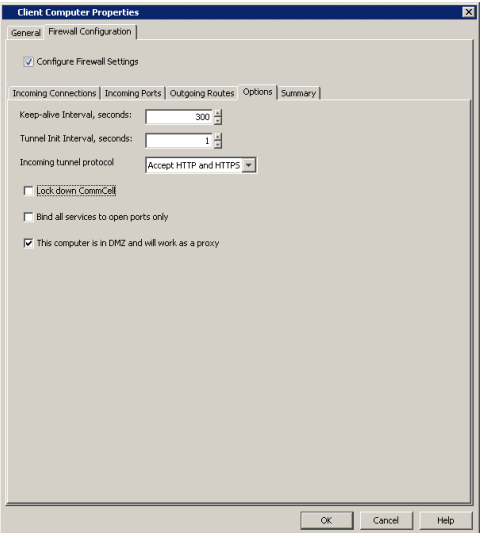
Now you have a choice of either adding another package to the existing installation or configure Calypso on a virtual machine for use in a cluster.

- 1) Add another package to stone.company.com
- 2) Install Calypso on a virtual machine
- 3) Exit

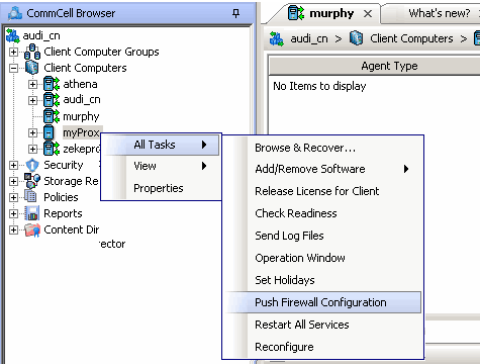
Your choice: [1]

VERIFY THE GATEWAYPROXY

1. From the Proxy Computer, ensure that **This computer is in DMZ and will work as a proxy** is selected in the **Firewall Configuration | Options** tab.



2. Right-click the **GatewayProxy** computer and click **All Tasks | Push Firewall Configuration**.



Setup Firewall Without Proxy - Laptop Backup

Overview

Prepare CommCell

Firewall Using Proxy

Firewall Without Proxy

Create Installation Package

Web Access

◀ Previous

Next ▶

SKIP THIS STEP IF YOU ARE USING PROXY SERVER

Click **Next** ▶ to Continue.

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.

The following sections explain the steps involved in operating the direct connection setup, where the client opens tunnel connection toward the CommServe and the MediaAgent:

1. Configure Firewall On CommServe
2. Configure Firewall On MediaAgent
3. Configure Firewall On Client Group

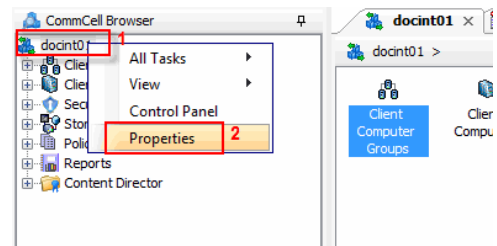
BEFORE YOU BEGIN

Review the following considerations before you begin:

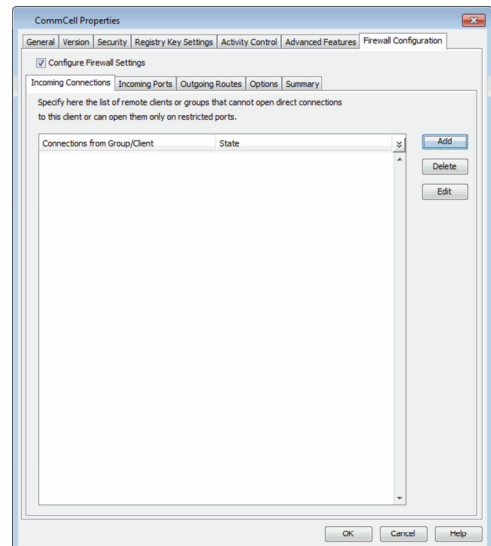
- Make a note of the port configuration on your firewall and substitute them appropriately in the following instructions.
- Microsoft Internet Information Services (IIS) uses port number 443 by default. So if you have IIS running on a computer, then you will not be able to use port 443 for firewall configuration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

CONFIGURE FIREWALL ON COMMSERVE

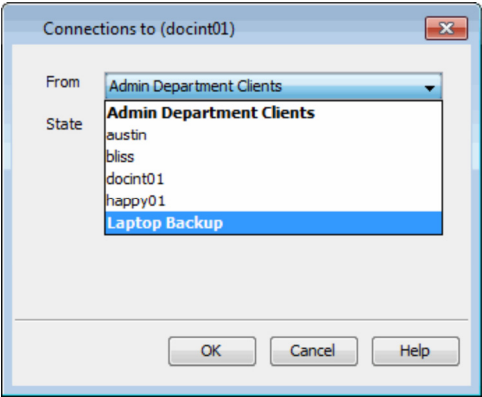
1. From the CommCell Console, right-click the CommServe computer and click **Properties**.



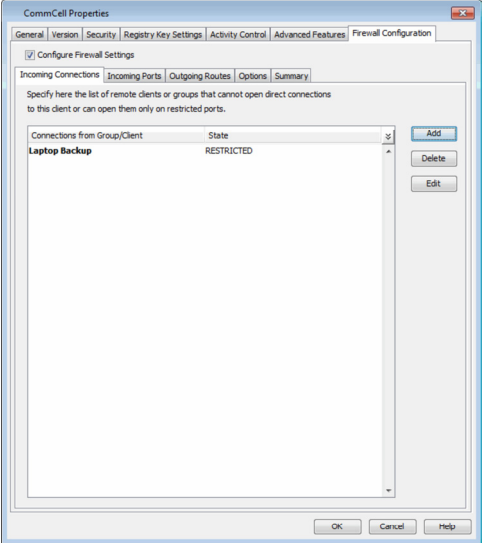
2.
 - Click the **Firewall Configuration** tab.
 - Select **Configure Firewall Settings** box.
 - Click **Add**.



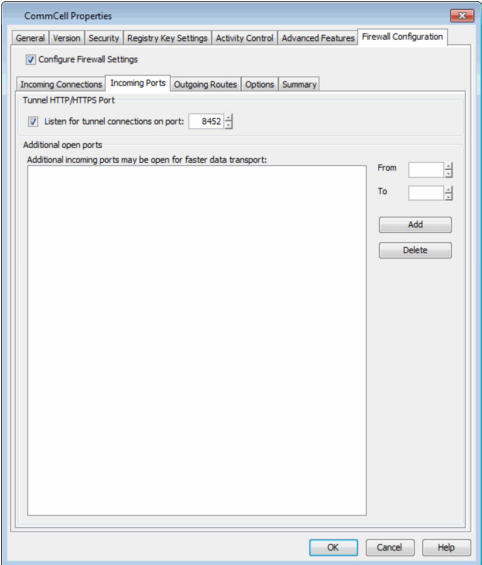
3.
 - From the **From** list, click the **Laptop Backup** client group.
 - From the **State** list, click **Restricted**.
 - Click **OK**.



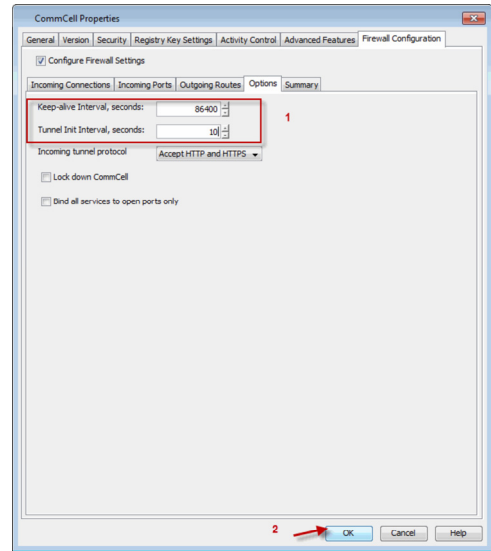
4. Click **Incoming Port** tab.



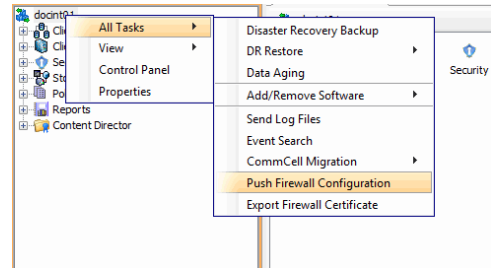
- 5.
- Select **Listen for tunnel connection on port** box and type or select the port number on which the incoming tunnel connection is received.
 - Click **Options** tab.



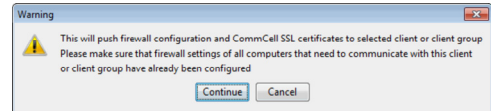
- 6.
- In the **Keep-alive Interval, seconds** box modify the value to 86400 (24 hours).
 - In the **Tunnel Init Interval, seconds** box, modify the value to 10.
 - Click **OK**.



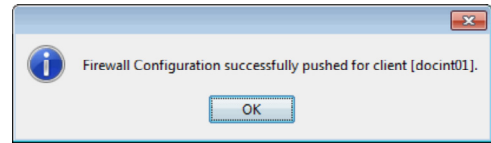
7. From the CommCell Browser, right-click the CommServe computer, point **All Tasks** and then click **Push Firewall Configuration**.



8. Click **Continue**.



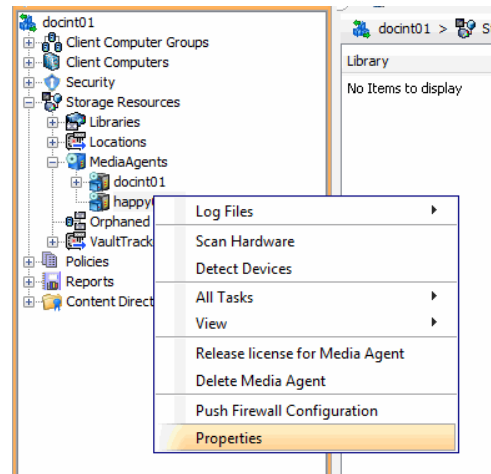
9. The specified configuration is saved.
The firewall configuration was pushed successfully.



CONFIGURE FIREWALL ON MEDIAAGENT

SKIP THIS SECTION IF MEDIAAGENT IS SAME AS COMMSERVE.

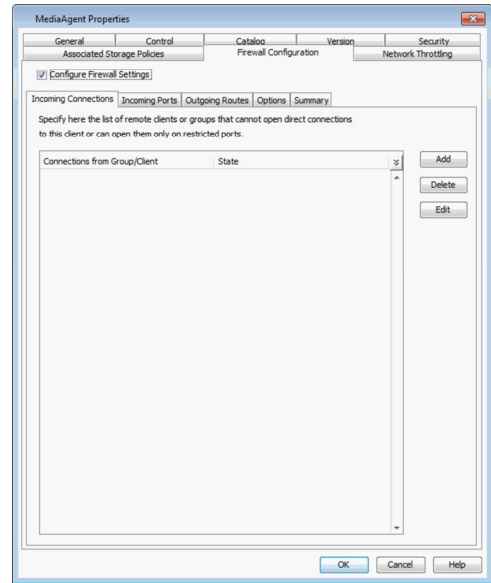
10. From the CommCell Console, navigate to **Storage-Resource | MediaAgents**, select and right-click **<media_agent>** and then click **Properties**.



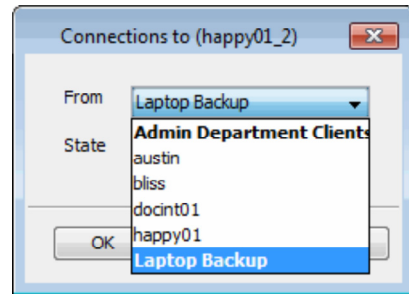
11.

- Click **Firewall Configuration** tab.
- Select **Configure Firewall Settings** box.

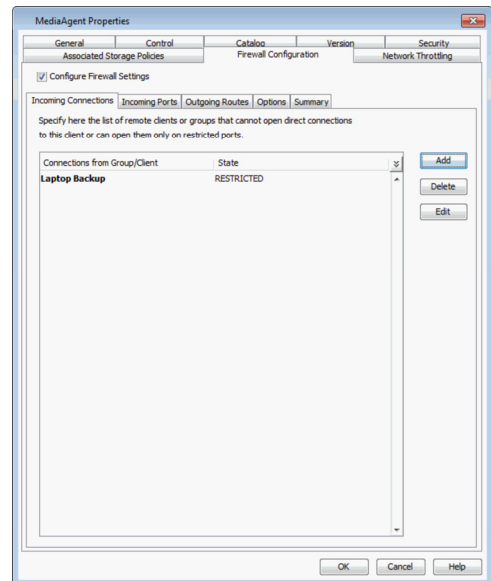
- Click **Add**.



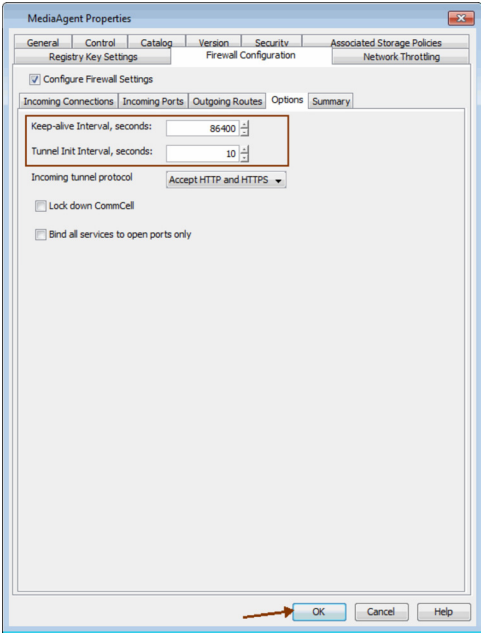
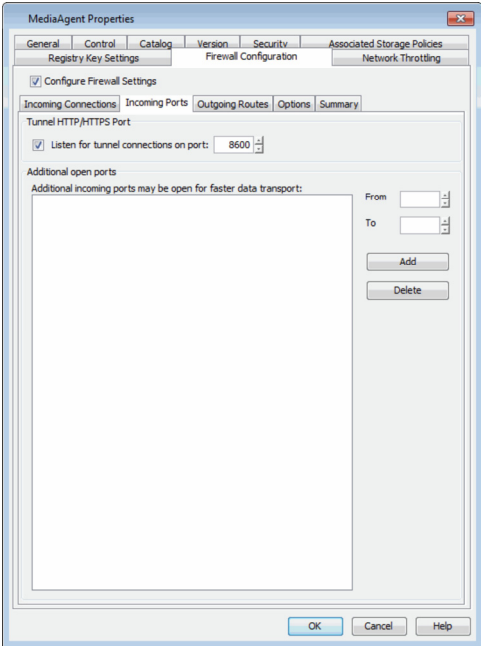
- From the **From** list, click the **Laptop Backup** client group.
 - From the **State** list, click **Restricted**.
 - Click **OK**.



- Click the **Incoming Ports** tab.

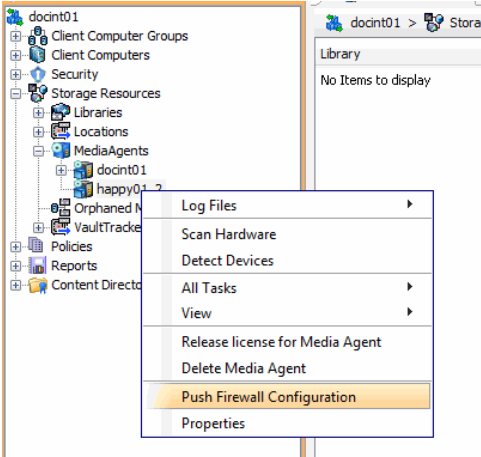


- Select **Listen for tunnel connection on port** box and type or select the port number on which the incoming tunnel connection is received.
 - Click **Options** tab.

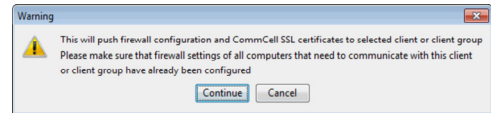


- 15.
- In the **Keep-alive Interval, seconds** box modify the value to 86400 (24 hours).
 - In the **Tunnel Init Interval, seconds** box, modify the value to 10.
 - Click **OK**.

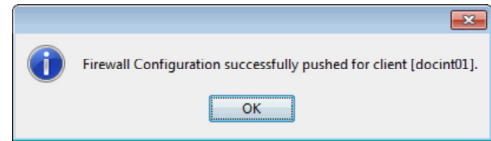
16. From the CommCell Console, navigate to **Storage-Resource | MediaAgents**. Right-click the **<media_agent>** and then click **Push Firewall Configuration**.



17. Click **Continue**.



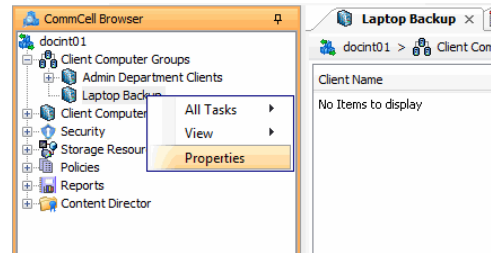
18. The specified configuration is saved.
The firewall configuration was pushed successfully.



CONFIGURE FIREWALL ON CLIENT GROUP

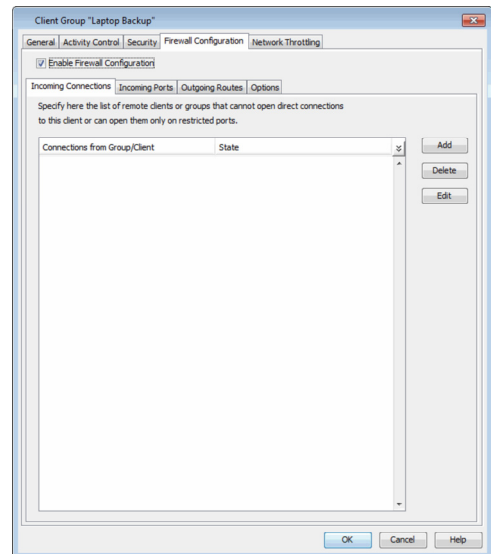
19.

- From CommCell Browser, navigate to **Client Computer Groups**.
- Right-click the **Laptop Backup** group and then click **Properties**.



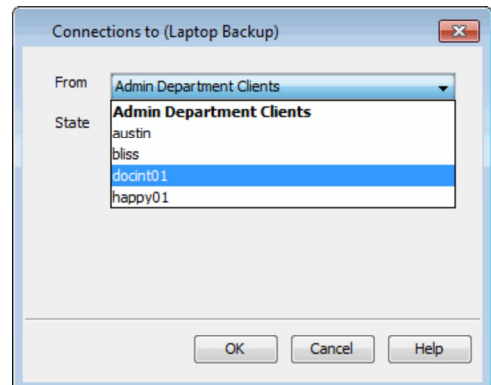
20.

- Click **Firewall Configuration** tab.
- Select **Enable Firewall Configuration** box.
- Click **Add**.



21.

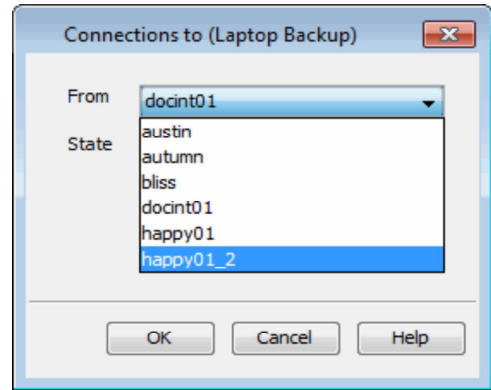
- From the **From** list, click the name of the CommServe computer.
- From the **State** list, click **Blocked**, since the CommServe cannot open connections to the Client.
- Click **OK**.



22.

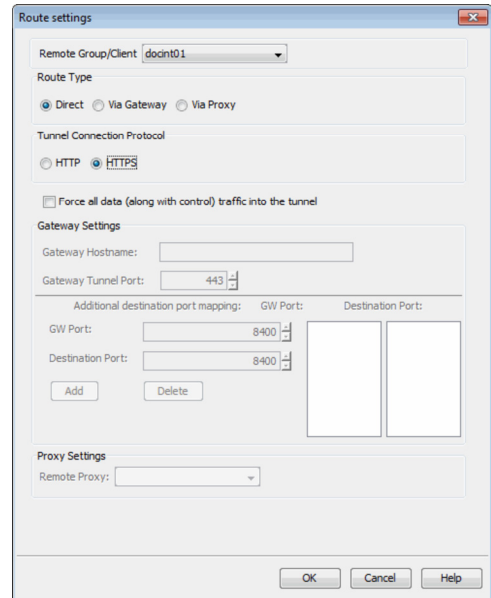
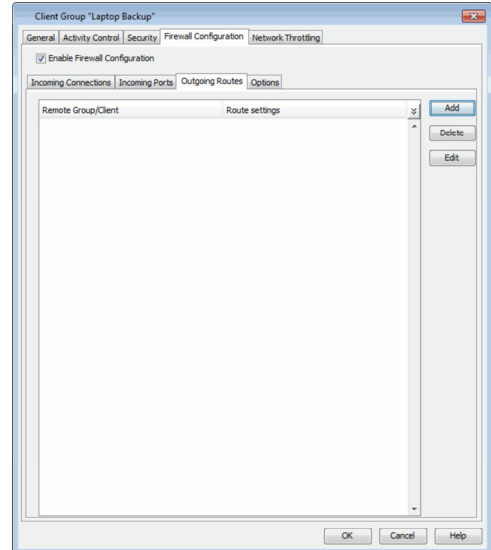
- If you have not configured the firewall on MediaAgent, skip this step.
- If you have configured firewall on MediaAgent, follow this steps:
 - From the **From** list, click the name of the MediaAgent computer.
 - From the **State** list, click **Blocked**, since the MediaAgent cannot open connections to the Client.
 - Click **OK**.

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



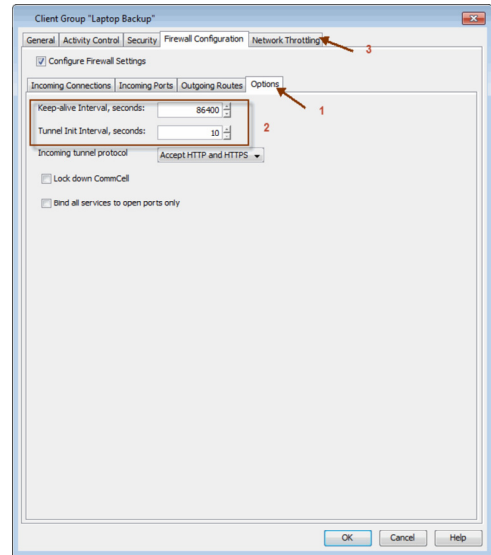
- 24.
- From the **Remote Group/Client** list, select CommServe name.
 - From the **Route Type**, click **Direct**.
 - From the **Tunnel Connection Protocol**, click **HTTPS**.
 - Click **OK**.

If MediaAgent is installed on separate computer, repeat the steps described above and select the **MediaAgent** in the **Remote Group/Client** list.

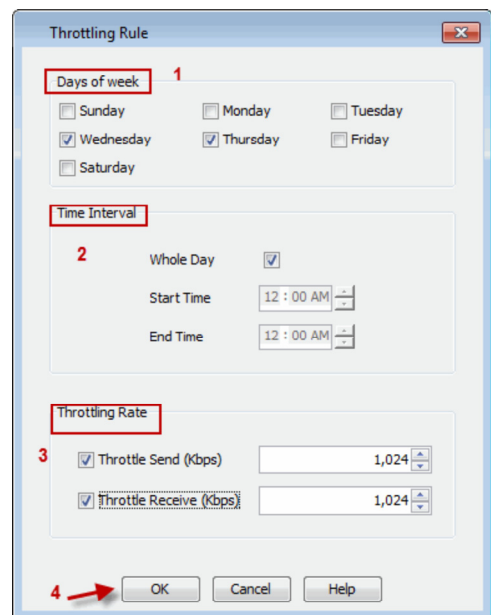
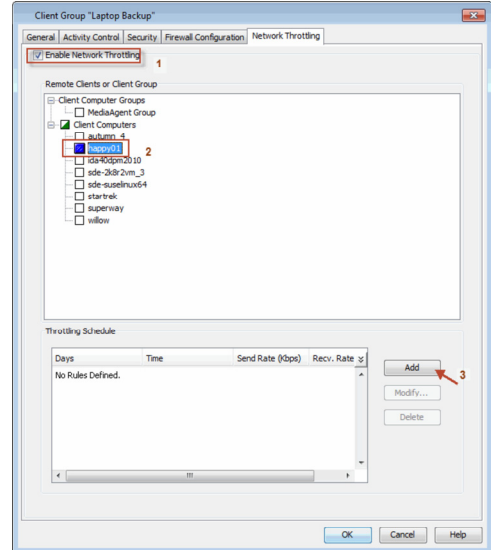


- 25.
- Click **Options** Tab.
 - In the **Keep-alive Interval, seconds** box modify the value to 86400 (24 hours).
 - In the **Tunnel Init Interval, seconds** box, modify the value to 10.
 - Click **Network Throttling** tab.

- 26.
- Select **Enable Network Throttling** checkbox.
 - In **Remote Clients or Client Group**, select the Media Agent designated for this Client Group.
 - Click **Add** to setup throttling rules.



- 27.
- Specify the following and then click **OK**.
- **Days of Week** - select a day or multiple days for the schedule to run.
 - **Time Interval** - select Whole day or a specific time interval for the schedule to run.
 - **Throttling Rate** - select Throttle Send and Throttle Receive rate and enter values.



28. The newly added throttling rules will be displayed in Throttling Schedule.

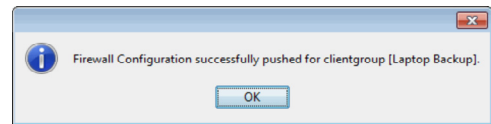
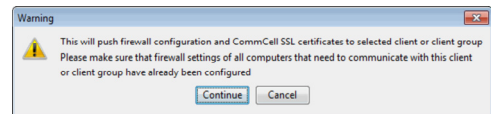
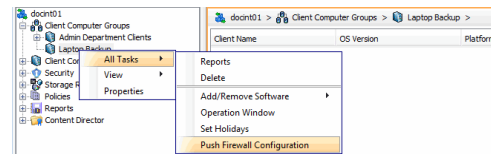
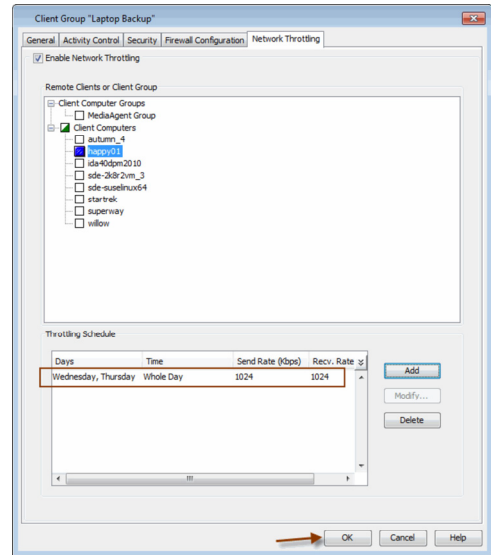
Click **OK**.

29.
 - From the CommCell Browser, navigate to **Client Computer Groups**.
 - Right-click the **Laptop Backup** group and point All Tasks and then click **Push Firewall Configuration**.

30. Click **Continue**.

31. The specified configuration is saved.
The firewall configuration was pushed successfully.

32. The newly added clients will automatically be registered in the client group and will hence inherit the firewall settings established in the client group.



Create Installation Package - Laptop Backup

The Installation Package will be used to install the backup client on a laptop. It will enable the automatic backup of the data residing on the laptop.

The following section describes the steps to create a custom install package.

1. Logon to the client computer as **root**.
2. Run the following command from the Software Installation Package:
./cvpkgadd
3. The product banner and other information is displayed.
Press **Enter**.
4. Read the license agreement. Type **y** and press **Enter**.
5. Type **2** to select **Advanced options**.

6. Press **Enter**.

7. Press **Enter**.

8. Type the number to choose a platform.
 - **1** for 32-bit
 - **2** for 64-bitTo select multiple component, enter the number by adding a space.

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

Advanced 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) Advanced options
3) Exit this menu
Your choice: [1]
```

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

```
[ Custom Package Creator ]
1) Create a custom install package
[ De-coupled Installer ]
2) Pre-install software Components (De-coupled Mode)
[ Integrated File Archiver ]
3) File System iDataAgent with Archiving Enabler
[ Customized Cluster Agents ]
4) Veritas Cluster Agents
[ Third Party Connector ]
5) Symantec NetBackup Agent
6) NetApp Snap Manager for Oracle
7) NetApp Snap Manager for SAP/Oracle
8) IBM Tivoli Storage Manager
[ Done ]
9) Exit this menu
Your choice: [1]
```

Besides general package, you may choose to create one additional native package from the list below.

```
1) General package only
2) Please also create RPM
3) Please also create solaris native package
4) Please also create hpux native package
5) Please also create Mac package using PackageMaker
6) Please also create APT
7) Exit
Package Type Number [1]
```

Please choose one or more platforms to package from the list below.

```
[ ] 1) Linux X86
[ ] 2) Linux X86_64
[ ] 3) Linux IA64
[ ] 4) Linux PPC64
[ ] 5) Linux S390
[ ] 6) Solaris8/9 SPARC
[ ] 7) Solaris10 SPARC
```

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

```
[ ] 8) Solaris10 X86_64
[ ] 9) Aix PPC
[ ] 10) HP-UX PA-RISC
[ ] 11) HP-UX IA64
[ ] 12) Darwin X86
[ ] 13) FreeBSD4 X86
> >>>>>>>>>>>> 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: 1 2

Please choose one or more platforms to package from the
list below.

[X] 1) Linux X86
[X] 2) Linux X86_64
[ ] 3) Linux IA64
[ ] 4) Linux PPC64
[ ] 5) Linux S390
[ ] 6) Solaris8/9 SPARC
[ ] 7) Solaris10 SPARC
[ ] 8) Solaris10 X86_64
[ ] 9) Aix PPC
[ ] 10) HP-UX PA-RISC
[ ] 11) HP-UX IA64
[ ] 12) Darwin X86
[ ] 13) FreeBSD4 X86
> >>>>>>>>>>>> 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: d
```

10. Type **1** to select **Unix File System iDataAgent** and press **Enter**.

```
Please choose one or more subsystems to package from the
list below.

[ ] 1) UNIX File System iDataAgent [1101] [CVGxIDA]
[ ] 2) MediaAgent [1301] [CVGxMA]
[ ] 3) SCSI Driver [1105] [CVGxWA]
[ ] 4) ProxyHost iDataAgent [1102] [CVGxProxyIDA]
[ ] 5) Documentum iDataAgent [1126] [CVGxDctmIDA]
[ ] 6) Oracle iDataAgent [1204] [CVGxOrIDA]
[ ] 7) SAP for Oracle [1205] [CVGxOrSAP]
[ ] 8) SAP for MaxDB [1206] [CVGxSAPMAXDB]
[ ] 9) Informix iDataAgent [1201] [CVGxIfIDA]
[ ] 10) Sybase iDataAgent [1202] [CVGxSybIDA]
[ ] 11) DB2 iDataAgent [1207] [CVGxDB2]
[ ] 12) MySQL iDataAgent [1208] [CVGxMySQL]
[ ] 13) PostGres iDataAgent [1209] [CVGxPostGres]
> >>>>>>>>>>>> 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: 1
```

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

```
Please choose one or more subsystems to package from the
list below.

[X] 1) UNIX File System iDataAgent [1101] [CVGxIDA]
[ ] 2) MediaAgent [1301] [CVGxMA]
[ ] 3) SCSI Driver [1105] [CVGxWA]
[ ] 4) ProxyHost iDataAgent [1102] [CVGxProxyIDA]
[ ] 5) Documentum iDataAgent [1126] [CVGxDctmIDA]
[ ] 6) Oracle iDataAgent [1204] [CVGxOrIDA]
[ ] 7) SAP for Oracle [1205] [CVGxOrSAP]
[ ] 8) SAP for MaxDB [1206] [CVGxSAPMAXDB]
[ ] 9) Informix iDataAgent [1201] [CVGxIfIDA]
[ ] 10) Sybase iDataAgent [1202] [CVGxSybIDA]
[ ] 11) DB2 iDataAgent [1207] [CVGxDB2]
[ ] 12) MySQL iDataAgent [1208] [CVGxMySQL]
[ ] 13) PostGres iDataAgent [1209] [CVGxPostGres]
> >>>>>>>>>>>> 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: 1
```

12. Press **Enter**.
The custom package will be created in the following location:
/opt/UnixCustomPackage/.

```
Save custom package to: [/opt]
```

13. Type **Yes** and press **Enter**.

```
Optionally, you may choose to record install to an xml
parameter file now so
that you can play it later. The recorded xml will be
encapsulated into the
custom package and can be used as an answer file in two
ways:

(1) from the custom package run "silent_install -p
default";
(2) from the native package run native installer
(rpm/pkgadd/swinstall...)

You can still perform the above two tasks without custom
recording if you
choose to use all default parameters.

Do you want to record the install now? [no] yes
```

14. Type **1** to select **Unix File System iDataAgent** and press **Enter**.

Please choose one or more subsystems to package from the list below.

```
[ ] 1) UNIX File System iDataAgent [1101] [CVGxIDA]
[ ] 2) MediaAgent [1301] [CVGxMA]
[ ] 3) SCSI Driver [1105] [CVGxWA]
[ ] 4) ProxyHost iDataAgent [1102] [CVGxProxyIDA]
[ ] 5) Documentum iDataAgent [1126] [CVGxDctmIDA]
[ ] 6) Oracle iDataAgent [1204] [CVGxOrIDA]
[ ] 7) SAP for Oracle [1205] [CVGxOrSAP]
[ ] 8) SAP for MaxDB [1206] [CVGxSAPMAXDB]
[ ] 9) Informix iDataAgent [1201] [CVGxIfIDA]
[ ] 10) Sybase iDataAgent [1202] [CVGxSybIDA]
[ ] 11) DB2 iDataAgent [1207] [CVGxDB2]
[ ] 12) MySQL iDataAgent [1208] [CVGxMySQL]
[ ] 13) PostGres iDataAgent [1209] [CVGxPostGres]
>) >>>>>>>>>> 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: 1
```

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

Please choose one or more subsystems to package from the list below.

```
[X] 1) UNIX File System iDataAgent [1101] [CVGxIDA]
[ ] 2) MediaAgent [1301] [CVGxMA]
[ ] 3) SCSI Driver [1105] [CVGxWA]
[ ] 4) ProxyHost iDataAgent [1102] [CVGxProxyIDA]
[ ] 5) Documentum iDataAgent [1126] [CVGxDctmIDA]
[ ] 6) Oracle iDataAgent [1204] [CVGxOrIDA]
[ ] 7) SAP for Oracle [1205] [CVGxOrSAP]
[ ] 8) SAP for MaxDB [1206] [CVGxSAPMAXDB]
[ ] 9) Informix iDataAgent [1201] [CVGxIfIDA]
[ ] 10) Sybase iDataAgent [1202] [CVGxSybIDA]
[ ] 11) DB2 iDataAgent [1207] [CVGxDB2]
[ ] 12) MySQL iDataAgent [1208] [CVGxMySQL]
[ ] 13) PostGres iDataAgent [1209] [CVGxPostGres]
>) >>>>>>>>>> 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: 1
```

16. Type **Yes** and press **Enter** to enable laptop backup features.

Do you want to configure the iDataAgent for laptop or desktop backups? [no] yes

The following Laptop Backup features are enabled:

- Automatic Ownership
- Automatic Scheduling
- Backup Monitor Tool

For more information, refer to FAQs.

17. Press **Enter**.

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

18. Type the path for installation directory and press **Enter**.

Please specify where you want us to install Calypso binaries.

It must be a local directory and there should be at least 176MB 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:

19. Type the path for log directory and press **Enter**.

Please specify where you want to keep Calypso log files.

It must be a local directory and there should be at least 100MB of free space available. All log files will be created in a "calypso/Log_Files" subdirectory, so if you enter "/var/log", the logs will actually be placed into "/var/log/calypso/Log_Files".

Log Directory:

20. Type **Yes** and then press **Enter**.

Most of Calypso processes run with root privileges, but some are launched by databases and inherit database access rights. To make sure that registry and log files can be written to by both kinds of processes we can either make such files world-writeable or we can grant write access only to processes belonging to a particular group, e.g. a "calypso" or a "dba" group.

We highly recommend now that you create a new user group and enter its name in the next setup screen. If you choose not to assign a dedicated group to Calypso processes, all temporary and configuration files will be created with -rw-rw-rw permissions.

If you're planning to backup Oracle DB you should use "dba" group.

Would you like to assign a specific group to Calypso?

21. Press **Enter** to assign user group.

Most of Calypso processes run with root privileges, but some are launched by databases and inherit database access rights. To make sure that registry and log files can be written to by both kinds of processes we can either make

- It is recommended that you create a new user group before creating

package, to specify access permissions to Calypso processes.

- If you do not have user group created, type no and skip to next step.

22. If you indicated **Yes** in above step, type the **Group name** and then press **Enter**.

such files world-writable or we can grant write access only to processes belonging to a particular group, e.g. a "Calypso" or a "dba" group.

We highly recommend now that you create a new user group and enter its name in the next setup screen. If you choose not to assign a dedicated group to Calypso processes, you will need to specify the access permissions later.

If you're planning to backup Oracle DB you should use "dba" group.

Would you like to assign a specific group to Calypso? [yes]

Please enter the name of the group which will be assigned to all Software files and on behalf of which all Software processes will run.

In most of the cases it's a good idea to create a dedicated "calypso" group. However, if you're planning to use Oracle iDataAgent or SAP Agent, you should enter Oracle's "dba" group here.

Group name: galaxy

REMINDER

If you are planning to install Calypso Informix, DB2, PostgreSQL, Sybase or Lotus Notes iDataAgent, please make sure to include Informix, DB2, etc. users into group "dba".

23. If you enter **no** in step 21, you will be prompted to assign permissions for other users.

- Type the appropriate number and press **Enter**.
- A confirmation screen will mark your choice with an **"X"**.

Type **"d"** for **Done**, and press **Enter**.

Access Permissions for Other Users

Installer will assign full access rights to root user and its belonging group for all installed Software files and its processes.

For any other users, you can specify the access permissions now.

However, since you chose not to assign a dedicated group in previous step, make sure you specify sufficient access rights for other users if you are also planning to install Software agents involving third party software protection.

[X] 1) Allow read permission to other users
[X] 2) Allow write permission to other users
[X] 3) Allow execute permission to other users
[a=all n=none r=reverse q=quit d=done >=next <=previous ? =help]
Enter number(s)/one of "a,n,r,q,d,>,<," here:

24. Type a network TCP port number for the Communications Service (CVD) and press **Enter**.

Type a network TCP port number for the Client Event Manager Service (EVMgrC) and press **Enter**.

Every instance of Calypso should use a unique set of network ports to avoid interfering with other instances running on the same machine.

The port numbers selected must be from the reserved port number range and have not been registered by another application on this machine.

Please enter the port numbers.

Port Number for CVD:

Port Number for EVMgrC:

25. Type **Yes** and then press **Enter**.

Is there a firewall between this client and the CommServe?

- If you have network setup with proxy, click Configure Firewall With Proxy.
- If you have network setup without proxy, click Configure Firewall Without Proxy.

CONFIGURE FIREWALL WITH PROXY

26. Type **3** to select **CommServe is reachable only through a proxy**.

Press **Enter**.

Please specify now how your firewall is limiting network traffic. Whether it's possible to open connection from here to a CommServe's tunnel port, whether all connections toward CommServe are blocked, and we should instead expect CommServe to connect back to us, or whether there is a proxy in between.

1) This machine can open connection to CommServe on a tunnel port

2) CommServe can open connections toward us

3) Commserve is reachable only through a proxy

Your choice: [1]

27. Type **CommServe Client Name** and press **Enter**.

Please specify client name of the CommServe below.

CommServe Client Name:

28. Enter the following information:

Proxy Connection Setup

- Type **GatewayProxy hostname** in **hostname** or **IP Address** and press **Enter**.
- Type GatewayProxy client name in **Proxy short name** and press **Enter**.
- Type the port number of the HTTP Proxy through which the CommServe can be reached and press **Enter**.

Please specify the name of IP address of the proxy that should be used to reach the CommServe along with the port number, on which the proxy is expecting connections.

Proxy hostname or IP address:

Proxy short name:

Proxy HTTP/HTTPS tunnel port number:

- If you have configured your network without proxy, click **Configure Firewall Without Proxy**.
- If you have configured your firewall with proxy, click **Configuration of Other Installation Options**.

CONFIGURE FIREWALL WITHOUT PROXY

29. Type **1** to select **This machine can open connection to CommServe on tunnel port** and press **Enter**.

Please specify now how your firewall is limiting network traffic. Whether it's possible to open connection from here to a CommServe's tunnel port, whether all connections toward CommServe are blocked, and we should instead expect CommServe to connect back to us, or whether there is a proxy in between.

1) This machine can open connection to CommServe on a tunnel port

2) CommServe can open connections toward us

3) CommServe is reachable only through a proxy

Your choice: [1]

30. Enter the name of the CommServe computer in place of **CommServe Client Name**. Press **Enter**.

Please specify client name of the CommServe below.

CommServe Client Name:

31. Enter the fully qualified name or the IP address of the CommServe in the **CommServe Host Name**. This should be TCP/IP network name. e.g., computer.company.com.

Please specify hostname of the CommServe below. Make sure the hostname is fully qualified, resolvable by the name services configured on this machine. If there is a port-forwarding Gateway in front of the CommServe, enter hostname or IP address of the Gateway here.

Press **Enter**.

- Ensure that the CommServe is accessible before typing the name; otherwise the installation will fail.
- If you enter a short name which resolves to the same IP address as the fully qualified CommServe name, you will be asked if you would prefer to use the fully qualified name.

32. Type the incoming port number through which the CommServe computer receives tunnel connection.

Please specify the port number, on which we should open tunnel connections toward the CommServe. This is same as "Tunnel HTTP/HTTPS port" configurable in the "Incoming Ports" tab of the CommServe Firewall Properties adjusted for a possible port-mapping Gateway in front of it.

Press **Enter**.

This is the port number, provided in the step 5 during **Setting up Connection to the CommServe**.

CommServe HTTP/HTTPS tunnel port number: 8500

33. • If this computer is separated from the CommServe by a HTTP Proxy, type **Yes** and enter the following information:

If there is an HTTP proxy between this client and the CommServe (e.g. Squid or Apache), please provide HTTP Proxy configuration below.

HTTP Proxy hostname or IP address: Type the hostname or IP address of the HTTP Proxy through which the CommServe can be reached.

Is there an HTTP proxy between this client and the CommServe? [no]

HTTP Proxy port number: Type the port number of the HTTP Proxy through which the CommServe can be reached.

Press **Enter**.

- If this computer is not separated from the CommServe by a HTTP Proxy, type **No** and press **Enter**.

34. If the CommCell is in the Lockdown mode, enter **Yes** and provide the path to the folder in the which the CommCell HTTPS certificate are available.

If you have checked "Lockdown CommCell" in firewall properties of the CommServe or Proxy, you need to provide path to the directory with CommCell HTTPS certificate below.

See [Enforcing CommCell Specific Certificates for Authentication](#) for more information on the Lockdown feature and steps to export the CommCell Certification.

This certificate can be obtained by right-clicking CommServe name in the Java GUI, and selecting All Tasks -> Export Firewall Certificate popup menu item.

Press **Enter**.

Have you enabled "Lockdown CommCell"? [no]

CONFIGURATION OF OTHER INSTALLATION OPTIONS

35. Type the **Laptop Backup** as a client group and then press **Enter**.

Please enter one Client Computer Group name for this client to join.

If you want to configure any additional settings for the clients before performing the backup, select the **Waiting Room** as the client group.

Client Computer Group Name:

See Configure Additional Settings Before Laptops Execute The First Backup for more information on **Waiting Room** client group configuration.

- 36. Type **Yes** and press **Enter**.
- 37. Type the subclient policy created in step 21 during **Create Subclient Policy**.
- 38. Press **Enter**.
- 39. Enter **Yes** to create the tar file of Custom Package.
- 40. You are advised that the **UnixCustomPackage.tar** file is created.
- 41. The **UnixCustomPackage.tar** is created in the path which you provided in step 18.
YOU CAN NOW PROVIDE THIS PACKAGE TO LAPTOP USERS.

```
Do you want to configure subclient policy? [no] yes
Please enter a subclient policy name for this IDA.
Subclient Policy Name:
Please select which instance you want to install/replay
for this recording:
1) Always install to Instance001
2) Always install to Instance002
3) Always install to Instance003
4) Always install to Instance004
5) Always install to Instance005
6) Always install to Instance006
7) Always install to Instance007
8) Always install to Instance008
9) Always install to Instance009
10) Always install to Instance010
11) Always install to a new instance
12) I want to specify another instance
Your choice: [11]

Archiving the custom package in a tar file (Optional)
Optionally, you may choose to tar the package now.
Do you want to create the tar file now? [no] yes
Creating /opt/UnixCustomPackage.tar ...Done.

Done
[ Custom Package Summary ]
- General package created at /opt/UnixCustomPackage/pkg
- Tar package created at /opt/UnixCustomPackage/tar:
  custom_pkg.tar
Thank you for choosing Bull.
```

[< Previous](#) [Next >](#)

Web Access - Laptop Backup

The following section provides the steps to setup a self-service web console to perform backup, restore and download operations on laptop:

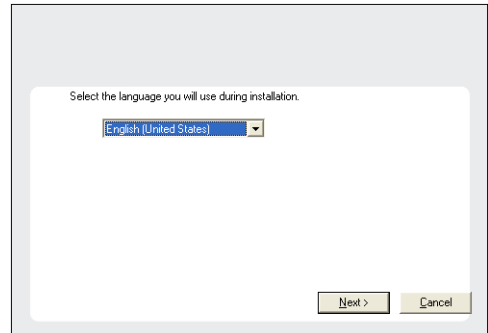
1. Installation
2. Configuration
 - o Add a New Domain Controller
 - o Enable Single Sign On
 - o Enable Secured Access for Web Search Client if you want to access the Web Console using HTTPS.
3. Assigning Owner For Laptop

INSTALLATION

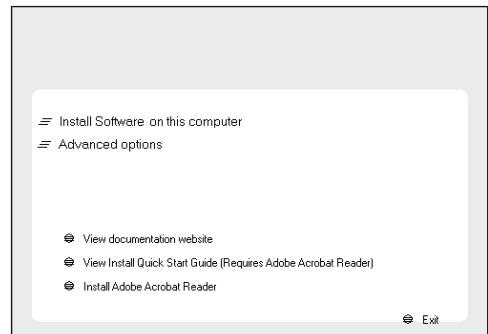
In order to use web console for backup and restore operations, you need to install **Web Server** and **Web Client** on any computer which can connect with the CommServe. The **Web Server** and **Web Client** can be installed on the same computer or on different computers.

For the web console to be available to users without a VPN session, install the Web Client on a dedicated host located in the DMZ, separate from the Web Server.

1. Ensure that the IIS is installed on the computer before installing the Web Server and Web Client.
2. Run **Setup.exe** from Software Installation Package on the computer that satisfies the minimum System Requirements.
3. Select the required language.
Click **Next**.



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



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

6. Expand **Common Technology Engine | Web Console Modules** and select one of the following options:

- **Web Server**
- **Web Client**

For the web console to be available to users without a VPN session, install the Web Client on a dedicated host located in the DMZ, separate from the Web Server.

Click **Next**.

7. Click **Yes**.

8. Specify the SQL Server System Administrator password.

Click **Next**.

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

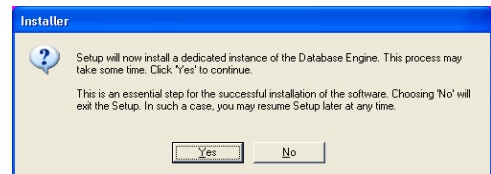
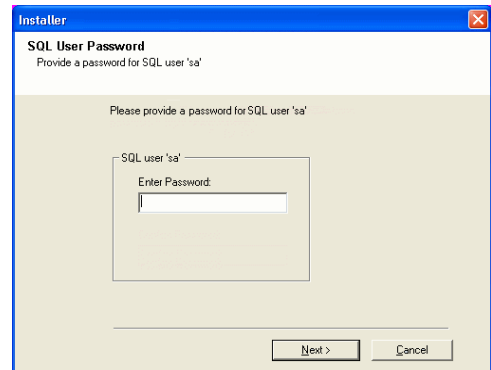
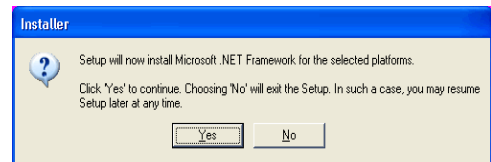
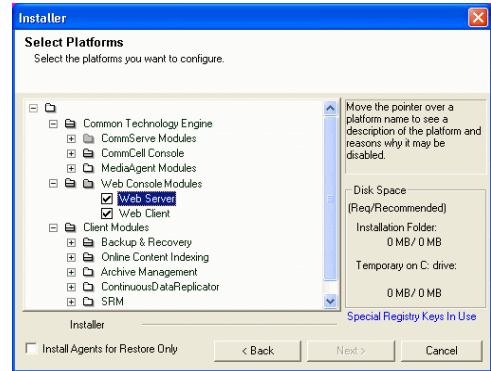
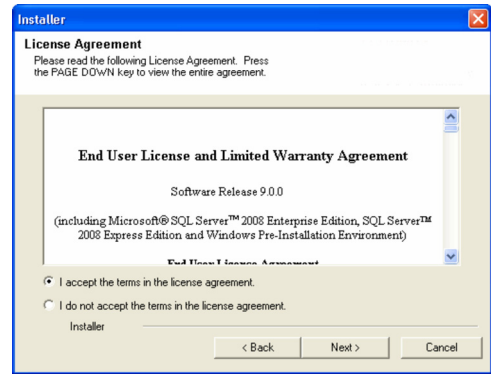
9. Click **Yes**.

10. Verify the Installation Path for the Database Engine.

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

Click **Next**.

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



- The install program installs the database instance.

11. Verify **MSSQL Database Installation Path**.

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

Click **Next**.

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

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

For firewall options and configuration instructions, see Firewall Configuration and continue with the installation.

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

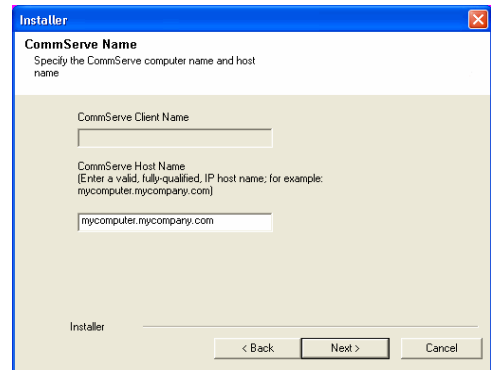
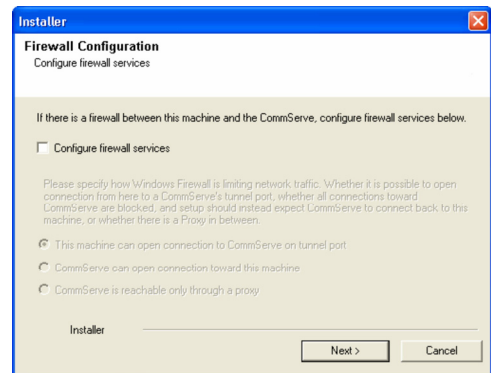
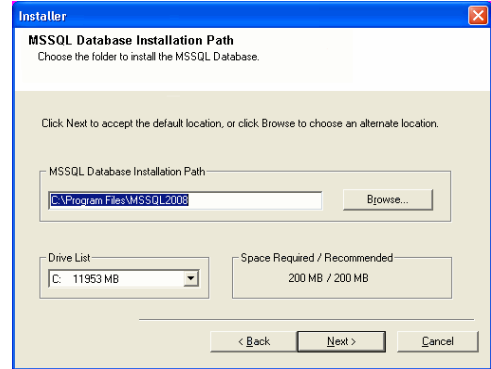
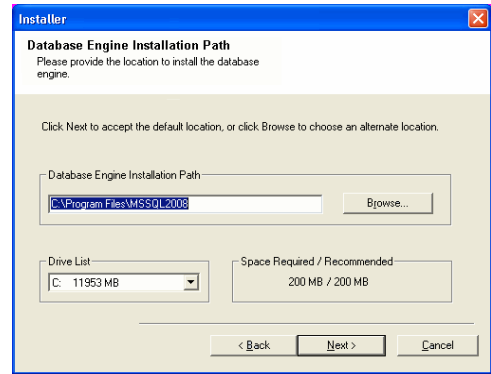
13. Enter the fully qualified domain name of the **CommServe Host Name**.

Click **Next**.

Do not use space and the following characters when specifying a new name for the CommServe Host Name:

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

14. Click **Next**.



15. Modify **Apache Tomcat Server port number** to **82**.

Click **Next**.

Ensure that these port numbers are different and are not already used by any other services or application.

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

Click **Next**.

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

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

17. Click **Next**.

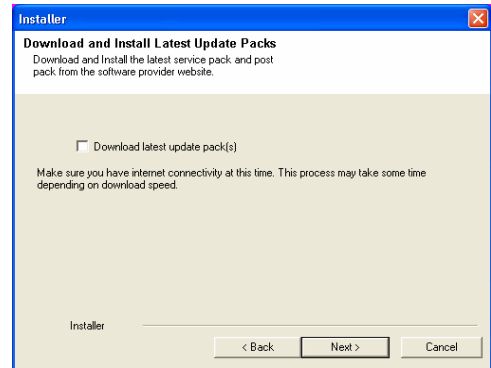
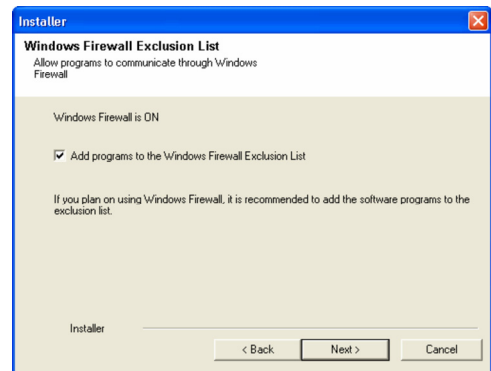
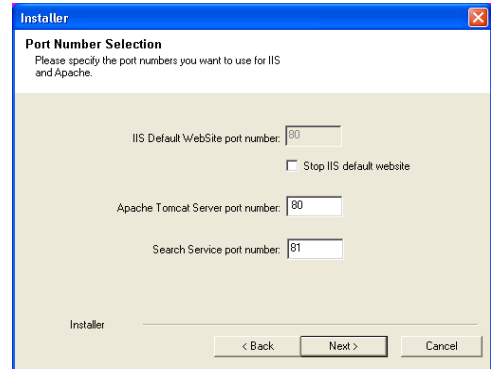
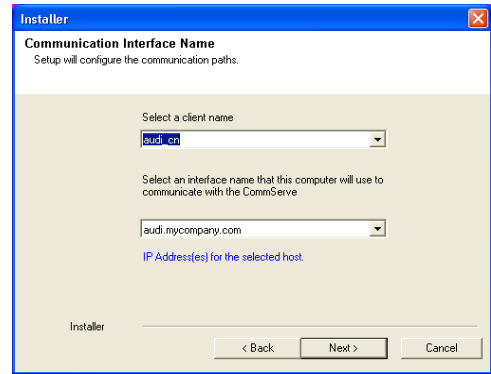
18. Verify the default location for software installation.

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

Click **Next**.

- 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.

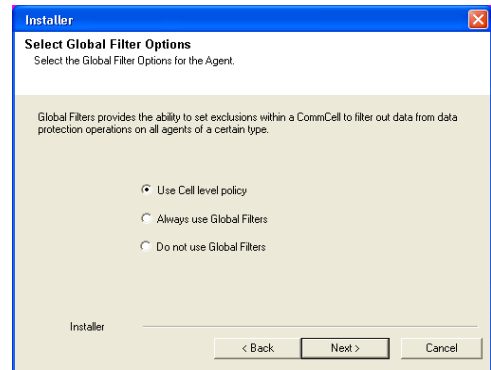
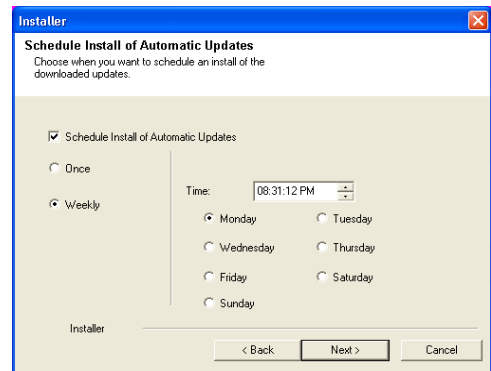
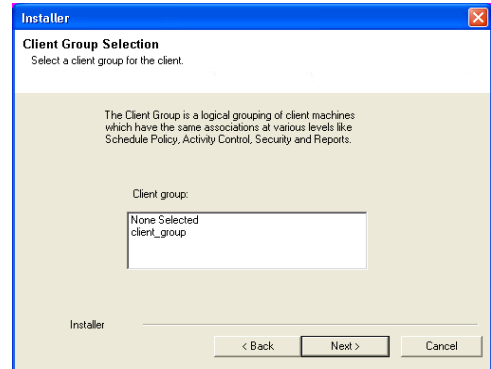
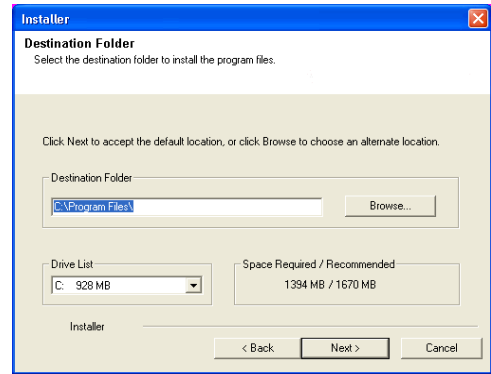
19. Select a Client Group from the list.
Click **Next**.

This screen will be displayed if Client Groups are configured in the CommCell Console.

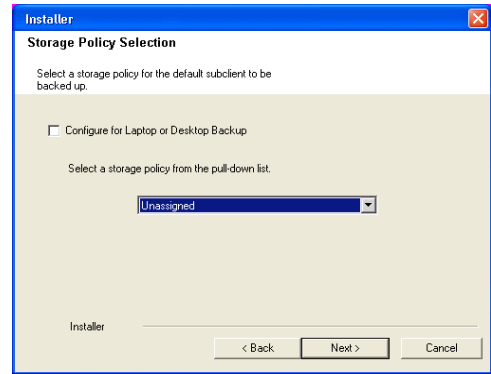
20. Click **Next**.

21. Click **Next**.

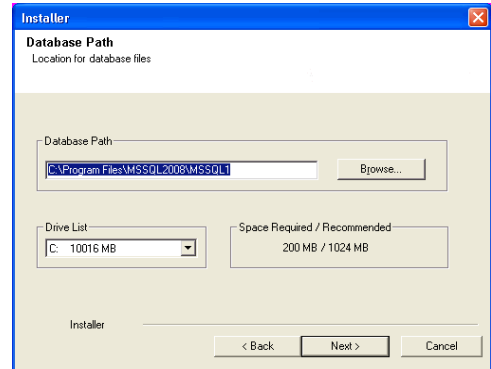
22. Select a **Storage Policy**.
Click **Next**.



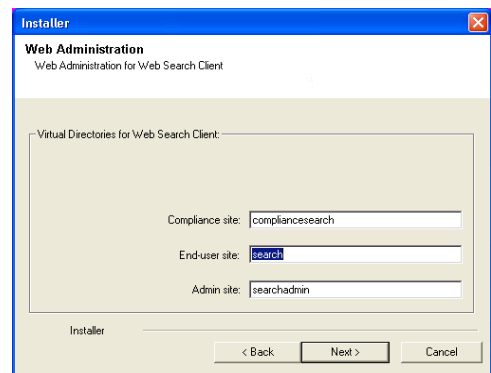
23. Enter the Web Server database installation path.
Click **Browse** to modify the default location.
Click **Next**.



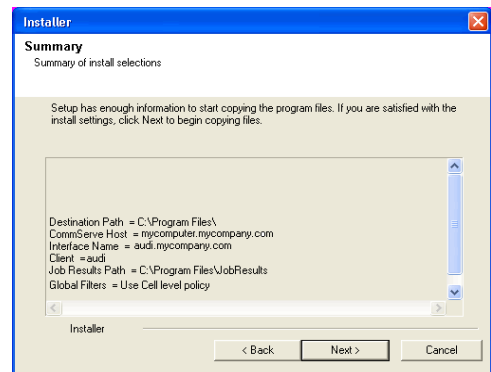
24. Click **Next**.



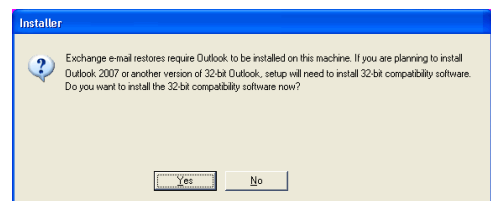
25. Click **Next**.

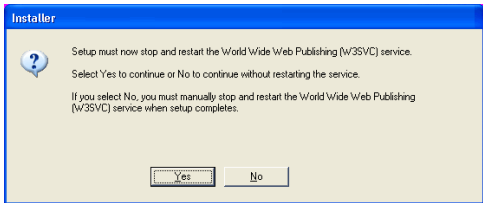


26. Click **Yes**.
This screen will appear if you are installing on Windows Server 2008 computer.

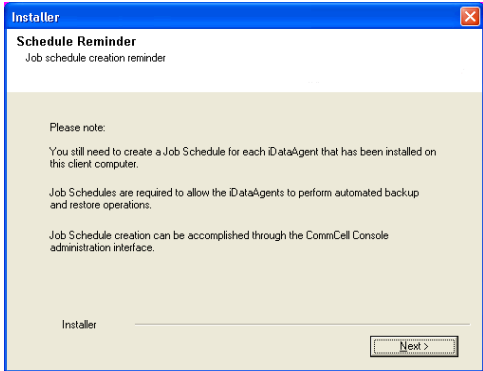


27. Click **Yes**.

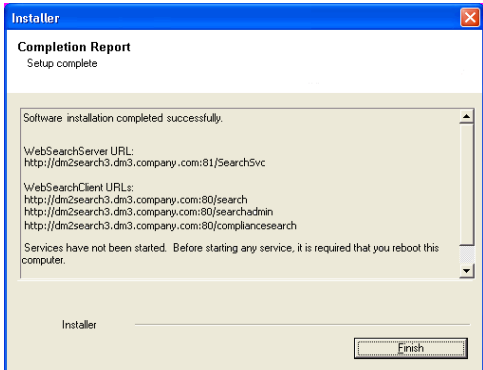




28. Click **Next**.



29. Click **Finish** to finish the installation.



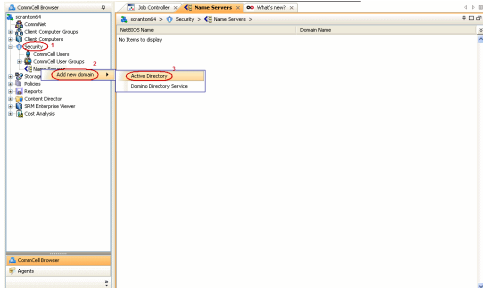
CONFIGURATION

Once the Web Server and Web Client are installed perform the following to configure the Search Console.

ADD A NEW DOMAIN CONTROLLER

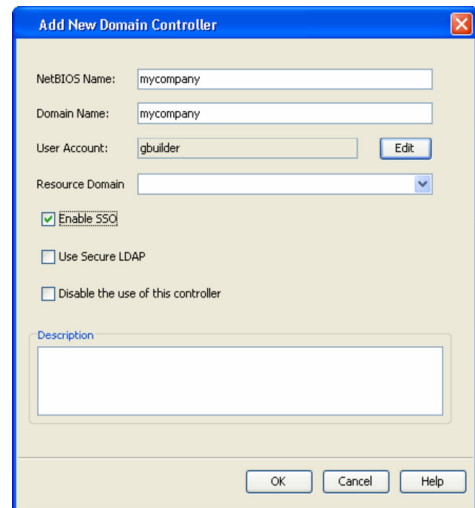
You need to provide the information required to communicate with the Active Directory service provider (such as domain name, hostname of directory server, directory service type, username and password) so that it will be maintained in the Web Server database for authentication purposes. Adding a new domain controller registers the external domain with the Web Server.

30. From the CommCell Browser, expand the **Security** node, right-click **Name Servers | Add New Domain** and click **Active Directory**.

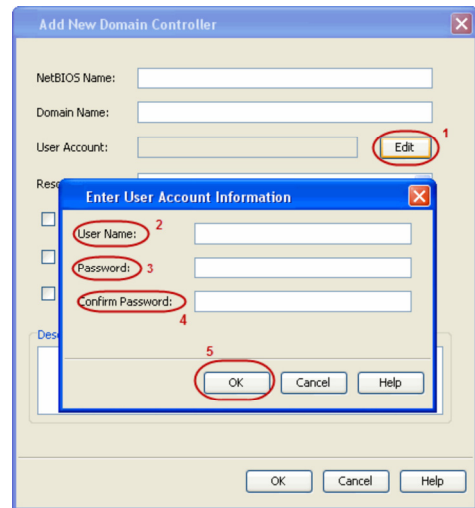


- 31.
- Enter the domain name in **NetBIOS Name** box, e.g., mydomain.
 - Enter the Fully Qualified Domain Name (FQDN), e.g., mydomain.mycompany.com in the **Domain Name** text box.
 - Select **Enable SSO**.

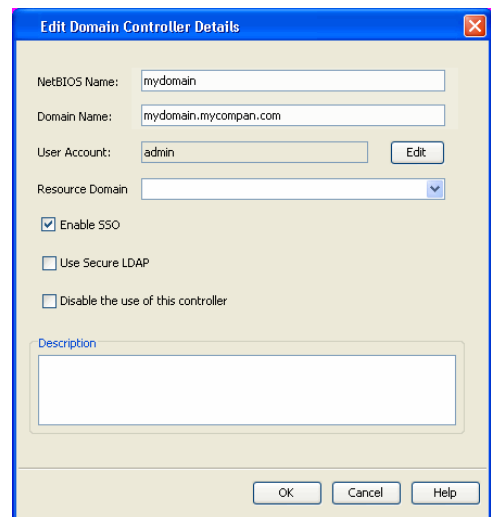
- 32.
- Click **Edit** to enter the user account information of the domain.
 - Type **Username** and **Password** in **Enter User Account Information**.
 - Click **OK**.



33. Click **OK**.



34. Once you have registered the Domain Controller, restart the IIS services on the Web Server.



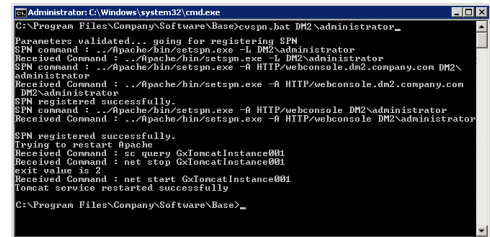
- From your **CommServe** computer, click the **Start** button on the Windows task bar and then click **Administrative Tools**.
- Click **Services**.
- In the **Services** window, select and right-click **IIS Admin Service** and click **Restart**.
- **Restart Other Services** dialog will be displayed, click **Yes**.

ENABLE SINGLE SIGN ON

The Single Sign On (SSO) enables laptop users to automatically login to the Web Console using their user-account credentials from the Active Directory service provider.

Use the following steps to enable Single Sign On, on the computer where the Web Client is installed:

- 35.
- Ensure that you have administrative permissions for the domain.
 - Ensure that Java 6 is installed (1.6.x and above).
 - Open the command prompt and navigate to `<software_installation_folder>/Base` folder.
 - Run the following command:
`cvspn.bat -A <domainName\userName>` (adds a Service Principal Name)
 - If you are enabling Single Sign On from other computer, make sure that the computer belongs to same domain.
 - The userName must match with the Name Server registration done in the Commcell GUI.
 - Configure your browser to include the site in the Intranet zone in case of Internet Explorer.



```
C:\Program Files\Company\Software\Base>cvspn.bat DM2\administrator_
Parameters validated... going for registering SPN
SPN command : ..\Apache\bin\setspn.exe -I DM2\administrator
Received Command : ..\Apache\bin\setspn.exe -I DM2\administrator
SPN command : ..\Apache\bin\setspn.exe -R HTTP/webconsole.dm2.company.com
DM2\administrator
Received Command : ..\Apache\bin\setspn.exe -R HTTP/webconsole.dm2.company.com
DM2\administrator
SPN registered successfully.
SPN command : ..\Apache\bin\setspn.exe -R HTTP/webconsole DM2\administrator
Received Command : ..\Apache\bin\setspn.exe -R HTTP/webconsole DM2\administrator
SPN registered successfully.
Trying to restart Apache.
Received Command : sc query G:\oncatInstance\001
Received Command : net stop G:\oncatInstance\001
exit value is 2
Received Command : net start G:\oncatInstance\001
Tomcat service restarted successfully
C:\Program Files\Company\Software\Base>
```

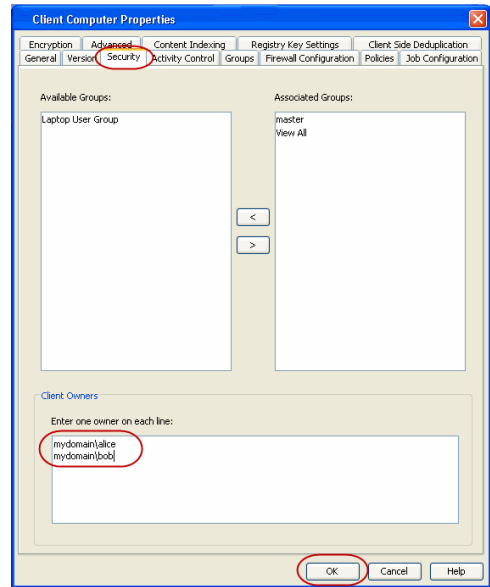
ASSIGNING OWNER FOR LAPTOP

By default, the following users will be designated as owners of the laptop (client) and will have privileges to access the Web Console:

- Active Directory users who are member of **Administrators** group.
The Active Directory domain must be the domain name specified in step 31 during **Add a New Domain Controller**.
- The user account used while registering a new client with the **Register Me** tool.
- The user account used to install the Laptop Backup package.

Use the following steps to include users who are not members of the **Administrators** group:

- 36.
- From the CommCell Browser, expand the **Client Computer Groups | Laptop Backup**.
 - Right-click the **<Client_Computer>** and select **Properties**.
 - Select **Security** tab.
 - Specify owner in the **Client Owner** box.
You can specify the Active Directory user accounts or CommCell user accounts.
 - Click **OK**.



CONGRATULATIONS - YOU HAVE SUCCESSFULLY COMPLETED YOUR LAPTOP BACKUP SETUP.

Click **Advanced Options** for additional information.

Advanced Options - Laptop Backup

TABLE OF CONTENTS

Scheduling Automatic Updates

Modifying the Contents of the Subclient for Specific Laptop Users

Configuring Network Bandwidth Throttling

Disable Throttling on the Schedule Policy

Configuring Automatic Backup Schedules

Power
CPU Utilization

Enabling Automatic Client Registration

Assigning Laptop Owners

Assigning User As Owners
Adding User Profiles As Owners
Assigning User Groups As Owners
Deleting Laptop Owners

Defining The Capabilities For Laptop Users

Defining Download Privilege to Laptop Owners

Modifying the Documentation Link for Backup Monitor

Enabling Secured Access for Web Search Client

Install Java with all the updates
Configure SSL on the Tomcat Server

Configuring Job Restartability

License Requirements

SCHEDULING AUTOMATIC UPDATES

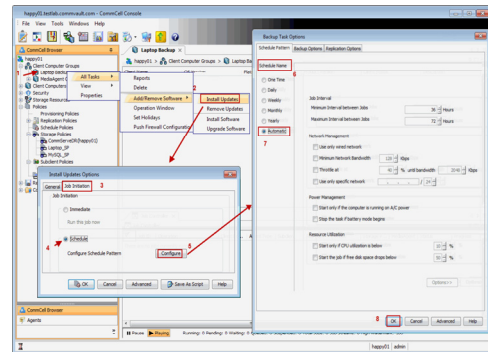
Setup a schedule for Automatic Updates of a software to ensure that the software is up-to-date on the laptops. Follow the steps given below to setup a schedule for automatic updates:

1. From the CommCell Console, navigate to **Client Computer Groups | <laptop group>**.
2. Right-click the <subclient policy> and navigate to **All Tasks | Add/Remove Software** and then click **Install Updates**.
3. Select **Ignore Running Jobs** to install updates on laptops if you have critical backup updates or service pack to be installed prior to running backup jobs.
4. Select **Job Initiation** tab.
 - o Select **Schedule**, click **Configure** button.
 - o Specify name in **Schedule Name** box for automatic updates schedule.
 - o Select **Automatic** option.

It is recommended to specify 3 weeks for **Minimum Interval between Job** and 4 weeks for **Maximum Interval between Job**.

- o Click **OK**.

5. Click **OK**.

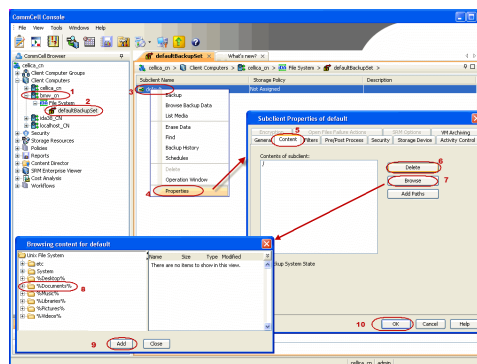
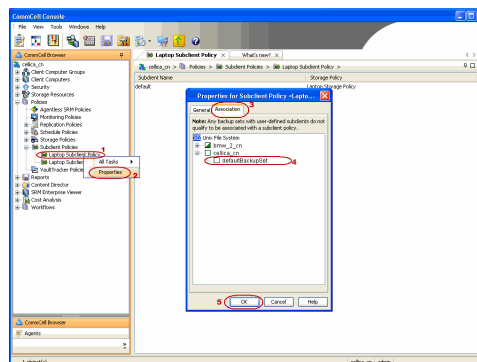


MODIFYING THE CONTENTS OF THE SUBCLIENT FOR SPECIFIC LAPTOP USERS

The default backup set for all clients will be associated to a subclient policy provided during custom package creation. If you wish to modify the content of a subclient backup set associated with the subclient policy, you can disassociate the client from the subclient policy and modify the content of the subclient. Follow the steps given below to disassociate the client from a subclient policy and modify the content of the client:

1. From the CommCell Console, navigate to **Policies | Subclient Policies**.
2. Right-click the <subclient policy> and click **Properties**.
3. Select **Association** tab.
4. Expand the <client> and clear the BackupSet checkbox for which you wish to change the association.

- Click **OK**.
You client is now disassociated from the Subclient Policy.
- From the CommCell Console, navigate to **<client computer> | File System | defaultBackupSet** right-click **default** subclient and click **Properties**.
- Select **Content** tab.
- Select the content (e.g., /opt or /var) in the **Contents of subclient** and click **Delete**.
- Click **Browse** and select the required content (e., Documents) in **Browsing content for default** window.
Click **Add**.
Click **Yes** in the **Warning** window and then click **Close**.
- Click **OK**.



CONFIGURING NETWORK BANDWIDTH THROTTLING

The network traffic for Clients and MediaAgents can be throttled based on the network bandwidth in your environment. This is useful to regulate network traffic and minimize bandwidth congestion.

By default, network throttling is disabled. You can enable the throttling options for an individual client, a client group consisting multiple clients, or a MediaAgent. Once configured, the throttling options are applied to all data transfer and control message operations, such as Data Protection operations including Laptop Backups, Copy operations including DASH copy, Data Recovery Operations, etc.

The throttling values setup in the throttling rule regulates the rate at which the data is sent and received.

You can also setup relative bandwidth throttling to ensure performance when the client machine connects with limited bandwidth. Multiple rules can be created for same client/client group, however the lowest values set up in different rules takes precedence for each time that intersects.

Use the following steps to set up network throttling options for Client Computer Group and thereafter disable throttling from the automatic schedules:

- From the CommCell Browser, expand **Client Computers**.
- Right-click the **<Client_Computer_Group>** and then click **Properties**.
- Click the **Network Throttling** tab.
- Select **Enable Network Throttling** check box.
- Under **Client Computer Groups**, select client computer groups to setup throttling.
- By default, **All clients share allocated bandwidth** check box is selected to share the throttling settings among all selected clients cumulatively.
If this check box is cleared, each client will throttle at the configured rate instead of a combined and shared rate.
- Click **Add** to setup throttling rules.
If you have setup relative throttling at the Schedule Policy level, make sure to note down the values specified there and Disable Throttling on the Schedule Policy.

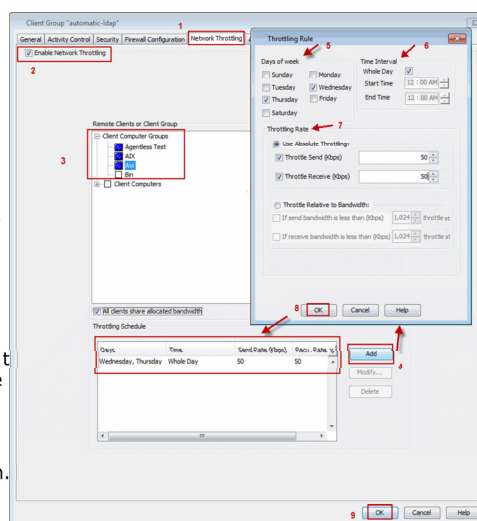
- In **Days of Week** select a day or multiple days for the schedule to run.
- In **Time Interval** select whole day or a specific time interval for the schedule to run.

Select one of the following under **Throttling Rate**:

- Absolute Throttling
- Relative Throttling

Use Absolute Throttling

Select **Throttle Send** and/or **Throttle Receive** rate and enter appropriate



values for each to throttle at the specified speed irrespective of the available bandwidth.

Throttle Relative to bandwidth

- Select **If send bandwidth is less than (Kbps)** to specify a minimum bandwidth required for send throttling to take affect and then specify the percentage rate to throttle the network bandwidth when the minimum bandwidth is available.
- Select **If receive bandwidth is less than (Kbps)** to specify a minimum bandwidth required for receive throttling to take affect and then specify the percentage rate to throttle the network bandwidth when the minimum bandwidth is available.

If the throttle bandwidth is higher than the amount specified in **Kbps**, then the job will run without throttling.

Click **OK**.

The newly added throttling rules will be displayed in Throttling Schedule.

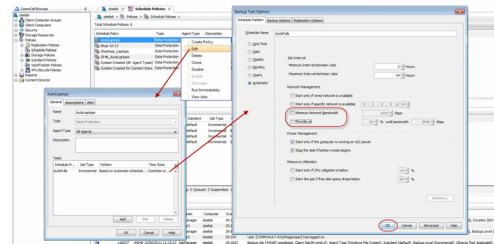
8. Click **OK**.
9. From the CommCell Browser, navigate to **Client Computer Groups | <Client_Computer_Group> | All Tasks** and click **Push Firewall Configuration**.
10. Click **Continue**.

DISABLE THROTTLING ON THE SCHEDULE POLICY

Throttling options must be disabled at the Schedule Policy level so that the throttling values specified in the Client/Client group level takes affect.

Use the following steps to disable network throttling options for an automatic schedule.

1. From the CommCell Console, navigate to **Policies | Schedule Policies**.
2. Right-click the *<laptop schedule policy>* and click **Edit**.
3. Select *<schedule task>* displayed in the **Tasks** and then click **Edit** button.
4. In the **Network Management** area, clear the following options if selected.
 - **Minimum Network Bandwidth**
 - **Throttle at**.
5. Click **OK**.



CONFIGURING AUTOMATIC BACKUP SCHEDULES

An automatic backup schedule can be created to automatically run a backup within a specified time. It can also be scheduled to run when the resources, such as network, power and CPU usage are met. The following sections provide information on configuring different resource management options available to schedule a job.

Automatic backup schedule does not perform synthetic full backups.

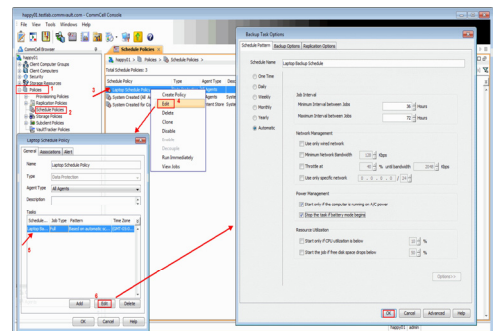
POWER

You can schedule a job to run backups only if the computer is on AC power (not battery power). Additionally, you can set an option to stop the backup job if the computer is switched to battery power. If both this options are set for automatic schedule, then your backups will only run when the computer is on AC power.

Use the following procedure to schedule a job depending up on the power management of laptops.

1. From the CommCell Console, navigate to **Policies | Schedule Policies**.
2. Right-click the *<laptop schedule policy>* and click **Edit**.
3. Select *<schedule task>* displayed in the **Tasks** and then click **Edit** button.
4. In the **Power Management** area, select one the following options:
 - Select **Start only if the Computer is running on A/C power** box, to run the job only when the computer is on A/C power.

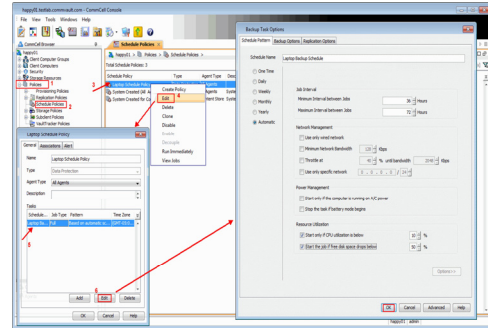
Backups continue to occur when your computer is running on A/C power.
 - Select **Stop the task if battery mode begins** box, backup job will not occur when the laptop is running on battery power.
5. Click **OK**.



CPU UTILIZATION

Use the following procedure to schedule a job depending upon the CPU and the disk usage.

1. From the CommCell Console, navigate to **Policies | Schedule Policies**.
2. Right-click the *<laptop schedule policy>* and click **Edit**.
3. Select *<schedule task>* displayed in the **Tasks** and then click **Edit** button.
4. In the **Resource Utilization** area, select one of the following options:
 - Select **Start only if CPU usage percentage is below** box, specify the amount to run the job when CPU utilization is below the specified percentage.
If the laptop CPU utilization exceeds this percentage during an automatic backup, then a backup won't start unless the CPU utilization falls below the specified percentage.
 - Select **Start only if free disk space percentage drops below** box, specify the amount to run the job when disk space percentage is below the specified percentage.
If the laptop disk space exceeds this percentage during an automatic backup, then a backup won't start unless the disk space percentage falls below the specified percentage.
5. Click **OK**.



ENABLING AUTOMATIC CLIENT REGISTRATION

The Automatic Client Registration feature is useful when have more than one CommServe running in your environment. This feature simplifies the client registration process for laptop clients. You can deploy the same installation package for all laptops and automatically register each laptop with the appropriate CommServe of your choice. The list of clients, where you are going to deploy the installation package, can be administered from a central web interface.

For more information, refer to Auto Client Registration.

ASSIGNING LAPTOP OWNERS

By default, the following users will be designated as owners of the laptop (client) and will have privileges to access the Web Console or Backup Monitor tool.

- Active Directory users who are member of **Local Administrators** group of the laptop (client).
The Active Directory domain must be the domain name specified in step 31 during **Add a New Domain Controller**.
- The user account used while registering a new client with the **Register Me** tool.
- The user account used to install the Laptop Backup package.

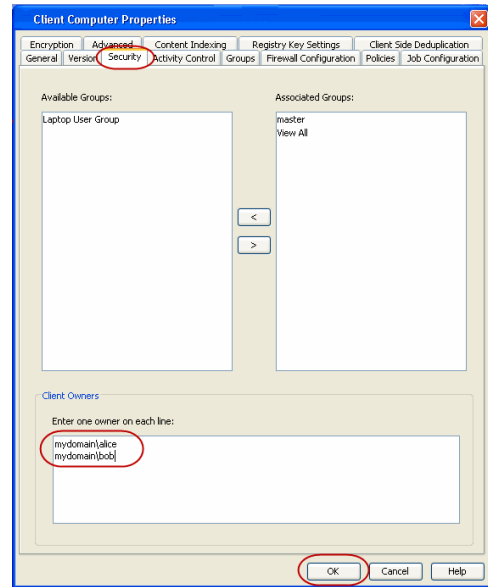
Use the following sections to add or modify additional owners to a laptop.

ASSIGNING USER AS OWNERS

FROM COMMCELL CONSOLE

Use the following steps to include users who are not members of the **Administrators** group from CommCell Console:

1. From the CommCell Browser, expand the **Client Computer Groups | Laptop Backup**.
2. Right-click the *<Client_Computer>* and select **Properties**.
3. Select **Security** tab.
4. Specify owner in the **Client Owner** box.
5. Click **OK**.



FROM COMMAND LINE

The following sections describes how to assign multiple users as owners to a client or multiple clients (client computer groups) through command line.

ASSOCIATING/DISASSOCIATING USER GROUP TO A CLIENT

Use the following steps to associate or disassociate members from an existing user group to a client computer. This will allow you to manage the members in the laptop user group.

If necessary you can use the following steps to overwrite the associate user group available on the client with a given user group.

1. Right-click the **View Sample XML File** link and click **Save Link As...** or **Save Target As...** to save the XML file needed for this task.
2. Open the **.xml** file using an XML editor and modify the following parameters:

- o **clientName** - Specify the names of the client computers that to you want to associate to the user group.

For example: If you wish to associate user group to `client1`, `client2` and `clientx` then you must add the following:

```
<entity>
<clientName>client1</clientName>
<clientName>client2</clientName>
<clientName>clientx</clientName>
</entity>
```

- o **userGroupName** - Specify the user group to which you want to associate to the client.

For example: If you wish to associate `usergroup1` to the above clients, then you must add the following:

```
<userGroupName>usergroup1</userGroupName>
```

- o **associatedUserGroupsOperationType** - Indicate one of the following operation types:

ADD - To associate the User Group to a Client

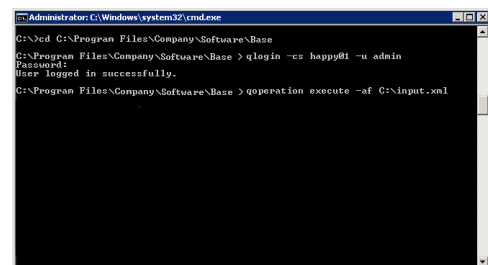
DELETE - To disassociate the User Group to a Client

OVERWRITE - To associate the user group mentioned above and disassociate all the user group available on the client computer. For example:

If `usergroup2` and `usergroup3` are already associated on `client1`, and you wish to overwrite the available user groups with `usergroup4`. This operation associates `usergroup4` to the `client1` and disassociates `usergroup2` and `usergroup3`.

3. Save the file as **input.xml**.
4. From Command prompt, navigate to `<Software_Installation_Directory>/Base` and then run the following command:
 - o Login to the CommServe using the `qlogin` command and commcell credentials.

VIEW SAMPLE XML FILE



For example, to log on to CommServe server1 with username user1:

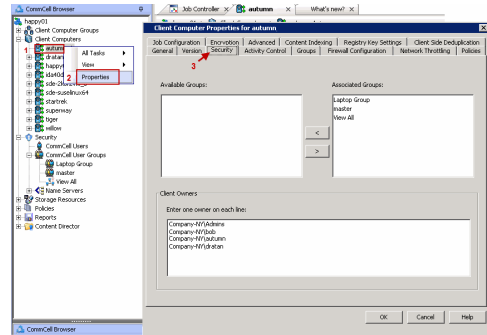
```
C:\>qlogin -cs server1 -u user1
```

- o Run the XML using the qoperation command.

For example, to run **input.xml**

```
C:\>qoperation execute -af input.xml
```

5. You can verify the user group associated to client from **Associated Groups**.
 - o From the CommCell Browser, right-click the **<Client>** and then click **Properties**.
 - o Click **Security** tab.
 - o The **User Group** specified above will be listed in the **Associated Groups**.



ASSOCIATING/DISASSOCIATING USER GROUP TO A CLIENT GROUP

Use the following steps to associate or disassociate members from an existing user group to a client computer group. This will allow you to manage the members in the laptop user group.

If necessary you can use the following steps to overwrite the associate user group available on the client group with a given user group.

1. Right-click the **View Sample XML File** link and click **Save Link As...** or **Save Target As...** to save the XML file needed for this task.
2. Open the **.xml** file using an XML editor and modify the following parameters:
 - o **clientGroupName** - Specify the names of the client computer group that you want to associate to the user group.
For example: If you wish to associate user group to clientgroup1, clientgroup2 and clientgroupx then your element will appear as follows:

```
<entity>
<clientGroupName>clientgroup1</clientGroupName>
<clientGroupName>clientgroup2</clientGroupName>
<clientGroupName>clientgroupx</clientGroupName>
</entity>
```

- o **userGroupName** - Specify the user group to which you want to associate to the client group.
For example: If you wish to associate usergroup1 to above client group, then you must add the following:

```
<userGroupName>usergroup1</userGroupName>
```
- o **associatedUserGroupsOperationType** - Indicate one of the following operation types:

- ADD** - This will associate the User Group to a Client Computer Group
- DELETE** - This will disassociate the User Group to a Client Computer Group
- OVERWRITE** - To associate the user group mentioned above and disassociate all the user group available on the client computer group. For example:

If usergroup2 and usergroup3 are already associated on clientgroup1, and you wish to overwrite the available user groups with usergroup4. This operation associates usergroup4 to the clientgroup1 and disassociates usergroup2 and usergroup3.

3. Save the file as **input.xml**.
4. From Command prompt, navigate to `<Software_Installation_Directory>/Base` and then run the following command:

- o Login to the CommServe using the qlogin command and commcell credentials.
For example, to log on to CommServe server1 with username user1:

```
C:\>qlogin -cs server1 -u user1
```

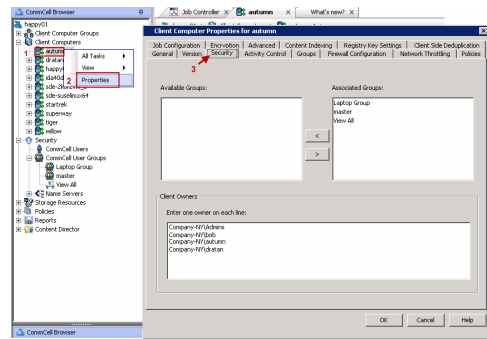
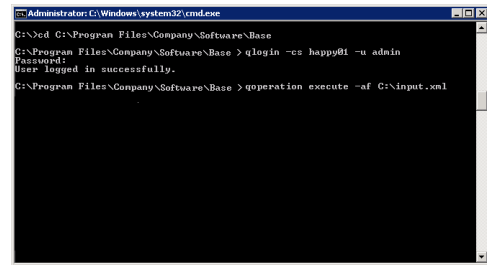
- o Run the XML using the qoperation command.

For example, to run **input.xml**

```
C:\>qoperation execute -af input.xml
```

5. You can verify the user group associated to client from **Associated Groups**.
 - o From the CommCell Browser, right-click the **<Client_Computer_Group>** and then click **Properties**.
 - o Click **Security** tab.

VIEW SAMPLE XML FILE



- o The **User Group** specified above will be listed in the **Associated Groups**.

ASSOCIATING/DISASSOCIATING USER TO A CLIENT

Use the following steps to associate or disassociate user to a client computer. This will allow user to access the client computer and perform backup and restore operations. This will assign user as a owner to the client computer and allow to perform backup and restore operations.

If necessary you can use the following steps to overwrite the user available on the client with a given user.

1. Right-click the **View Sample XML File** link and click **Save Link As...** or **Save Target As...** to save the XML file needed for this task.
2. Open the **.xml** file using an XML editor and modify the following parameters:

- o **clientName** - Specify the names of the client computer group that you want to associate to the user.

For example: If you wish to associate user group to **client1**, **client2** and **clientx** then you must add the following:

```
<entity>
<clientName>client1</clientName>
<clientName>client2</clientName>
<clientName>clientx</clientName>
</entity>
```

- o **clientOwners** - Specify the user to which you want to associate to the client.

For example: If you wish to associate **user1** to above clients, then you must add the following:

```
<clientOwners>user1</clientOwners>
```

- o **clientOwnersOperationType** - Indicate one of the following operation types:

ADD - This will associate the user to a client computer

DELETE - This will disassociate the user to a client computer

OVERWRITE - To associate the user mentioned above and disassociate all the users available on the client computer. For example:

If **user2** and **user3** are already associated on **client1**, and you wish to overwrite the available users with **user4**. This operation associates **user4** to the **client1** and disassociates **user2** and **user3**.

3. Save the file as **input.xml**.
4. From Command prompt, navigate to `<Software_Installation_Directory>/Base` and then run the following command:

- o Login to the CommServe using the **qlogin** command and commcell credentials.

For example, to log on to CommServe **server1** with username **user1**:

```
C:\>qlogin -cs server1 -u user1
```

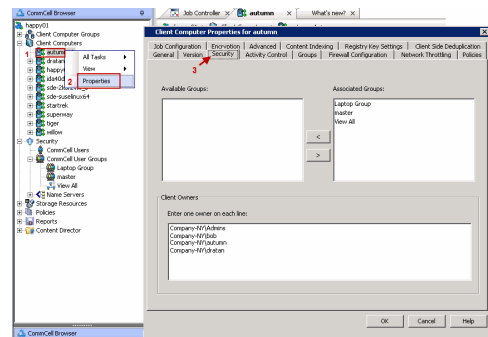
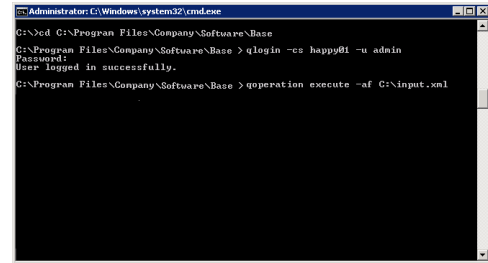
- o Run the XML using the **qoperation** command.

For example, to run **input.xml**

```
C:\>qoperation execute -af input.xml
```

5. You can verify the user associated to client from **Client Owners**.
 - o From the CommCell Browser, right-click the **<Client>** and then click **Properties**.
 - o Click **Security** tab.
 - o The user specified above will be listed in the **Client Owners**.

VIEW SAMPLE XML FILE



ASSOCIATE/DISASSOCIATE USER TO A CLIENT COMPUTER GROUP

Use the following steps to associate/disassociate user to client computer group.

Once this is done the included user will have access to client computer group and can backup and restore their data on this client.

1. Right-click the **View Sample XML File** link and click **Save Link As...** or **Save Target As...** to save the XML file needed for this task.
2. Open the **.xml** file using an XML editor and modify the following parameters:

- o **clientName** - Specify the client computer groups to which you want to associate the user.

For example: If you wish to associate user group to **clientgroup1**, **clientgroup2** and **clientgroupx** then you must add the following:

```
<entity>
```

VIEW SAMPLE XML FILE

```

<clientGroupName>clientgroup1</clientGroupName>
<clientGroupName>clientgroup2</clientGroupName>
<clientGroupName>clientgroupx</clientGroupName>
</entity>

```

- o **clientOwners** - Specify the user to which you want to associate to the client computer group.

For example: If you wish to associate `user1` to above client, then your element will appear as follows:

```
<clientOwners>user1</clientOwners>
```

- o **clientOwnersOperationType** - Indicate one of the following operation types:

ADD - This will associate the User Group to a Client Computer Group

DELETE - This will disassociate the User Group to a Client Computer Group

OVERWRITE - To associate the user mentioned above and disassociate all the users available on the client computer group. For example:

If `user2` and `user3` are already associated on `clientgroup1`, and you wish to overwrite the available user groups with `user4`. This operation associates `user4` to the `client1` and disassociate `user2` and `user3`.

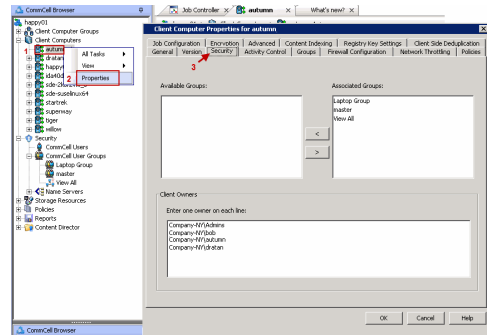
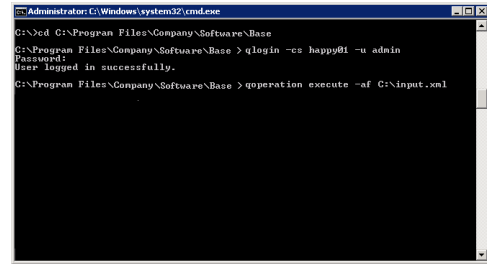
3. Save the file as **input.xml**.
4. From Command prompt, navigate to `<Software_Installation_Directory>/Base` and then run the following command:
 - o Login to the CommServe using the `qlogin` command and commcell credentials.

For example, to log on to CommServe `server1` with username `user1`:

```
C:\>qlogin -cs server1 -u user1
```
 - o Run the XML using the `qoperation` command.

For example, to run **input.xml**

```
C:\>qoperation execute -af input.xml
```
5. You can verify the user associated to client from **Client Owners**.
 - o From the CommCell Browser, right-click the **<Client_Computer_Group>** and then click **Properties**.
 - o Click **Security** tab.
 - o The user specified above will be listed in the **Client Owners**.



ADDING USER PROFILES AS OWNERS

By default, the following users will be designated as owners of the laptop (client) and will have privileges to access the Web Console or Backup Monitor tool.

- Active Directory users who are member of **Local Administrators** group of the laptop (client).

The Active Directory domain must be the domain name specified in step 31 during **Add a New Domain Controller**.
- The user account used while registering a new client with the **Register Me** tool.
- The user account used to install the Laptop Backup package.

Use the following steps to add user profiles as client owners.

1. Logon to the CommServe computer.
2. From the Command prompt, login to the CommServe using the `qlogin` command and commcell credentials.

For example, to log on to CommServe `server11` with username `user1`:

```
C:\>qlogin -cs server11 -u user1
```
3. Run the following `execscript` operation using `qoperation`:

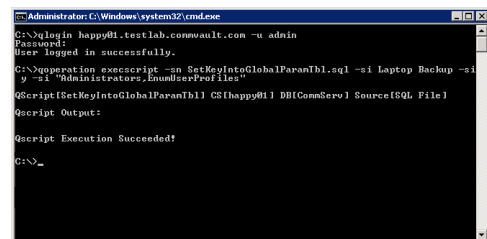
```
qoperation execscript -sn SetKeyIntoGlobalParamTbl.sql -si ClientGroupForLaptop -si y -si "Administrators,EnumUserProfiles"
```

Where:

`Administrators` - is the **Administrators** group under local group.

`EnumUserProfiles` - are the user profiles defined in the laptop.

Make sure to include new groups with the existing groups while executing the script. If not the script will overwrite existing groups with the new group specified as a value in the script.



SPECIFYING ADDITIONAL USER GROUPS

By default, the following users will be designated as owners of the laptop (client) and will have privileges to access the Web Console or Backup Monitor tool.

- Active Directory users who are member of **Local Administrators** group of the laptop (client).
The Active Directory domain must be the domain name specified in step 31 during **Add a New Domain Controller**.
- The user account used while registering a new client with the **Register Me** tool.
- The user account used to install the Laptop Backup package.

If you want to designate all the users in a user group as owners of the laptop (client), follow the steps given below to specify the user group (defined in the laptop):

1. Logon to the CommServe computer.
2. From the Command prompt, login to the CommServe using the `qlogin` command and commcell credentials.

For example, use the following command to log on to CommServe `server11` with username `user1`:

```
C:\>qlogin -cs server11 -u user1
```

3. Run the following `execscript` operation using `qoperation`:

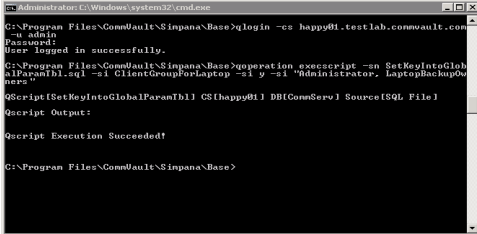
USAGE:

```
qoperation execscript -sn SetKeyIntoGlobalParamTbl.sql -si  
ClientGroupForLaptop -si y -si "Administrators,<group1>,<groupx>"
```

Where:

<Group1>,<Groupx>: Specify the name of the local user group, whose members will be added as owner of the laptop (client). You can add multiple local user groups as input to the script.

Make sure to include new groups with the existing groups while executing the script. If not the script will overwrite existing groups with the new group specified as a value in the script.



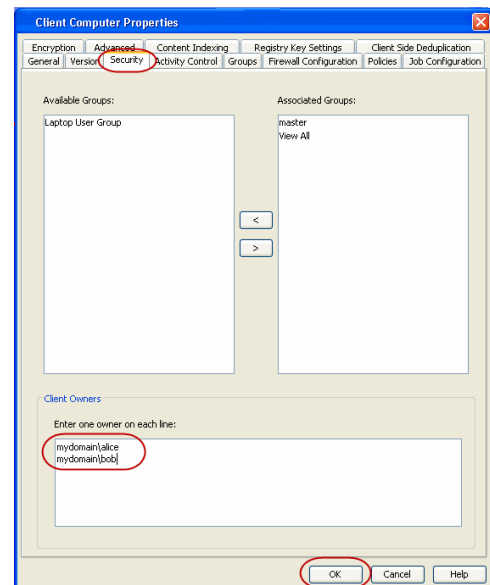
```
Administrator: C:\Windows\system32\cmd.exe  
C:\Program Files\CommVault\CS\Impana\Base>qlogin -cs happy01.testlab.commvault.com  
-u admin  
Password:  
User Logged in successfully.  
C:\Program Files\CommVault\CS\Impana\Base>qoperation execscript -sn SetKeyIntoGlobalParamTbl.sql -si ClientGroupForLaptop -si y -si "Administrators, LaptopBackupOwner"  
QScript [SetKeyIntoGlobalParamTbl] CS[happy01] DB[CommServ] Source [SQL File]  
Qscript Output:  
Qscript Execution Succeeded!  
C:\Program Files\CommVault\CS\Impana\Base>
```

DELETING LAPTOP OWNERS

FROM COMMCELL CONSOLE:

Use the following steps to delete the users as client owners.

1. From the CommCell Browser, expand the **Client Computer Groups | Laptop Backup**.
2. Right-click the **<Client_Computer>** and select **Properties**.
3. Select **Security** tab.
4. Remove the specific owner from the **Client Owner** box.
5. Click **OK**.



FROM COMMAND LINE:

To remove multiple users from the client computer, see [Associating/Disassociating User to a Client Computer](#)

DEFINING THE CAPABILITIES FOR LAPTOP USERS

By default, the owners of the laptop (client) will have permissions to perform all operations from the Web Console and Backup Monitor.

If necessary, you can define specific capabilities to enable user interface options in the Web Console and Backup Monitor to client owners in the CommCell. Such capabilities include the following:

For Web Console:

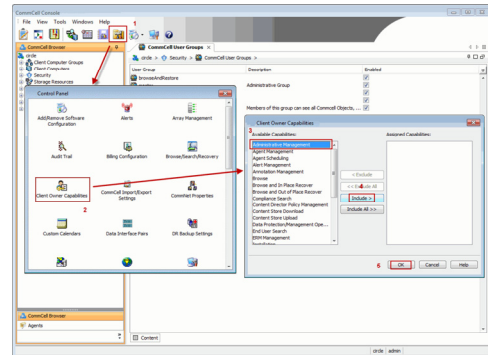
- Running backup jobs
- Changing content rules
- Adding schedules
- Conducting browse/restore

For Backup Monitor:

- Running backup jobs

Use the following steps to assign the security rights to the laptop user.

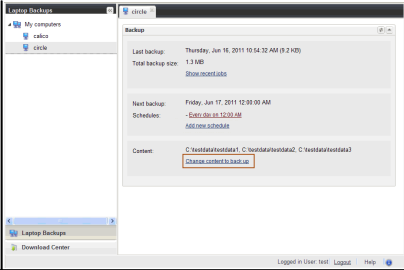
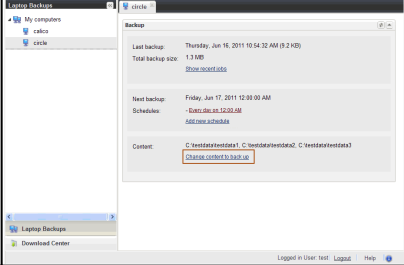
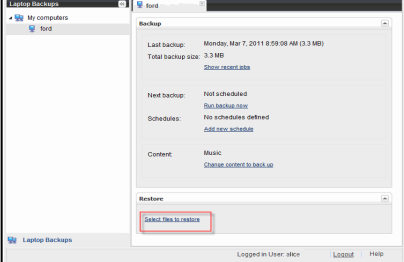
1. From the CommCell Browser, click **Control Panel** icon.
2. From the **Control Panel**, double-click **Client Owner Capabilities**.
3. Select Client Owner capabilities from the **Available Capabilities** list box.
4. Click **Include >** to move the selected capabilities to the **Assigned Capabilities** list box.
5. Click **OK**.



The following table provides the list of specific rights that are applicable to a laptop user.

To view the additional rights available in the CommCell, see Capabilities and Permitted Actions.

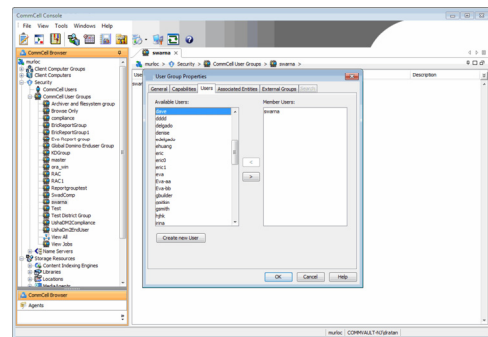
AVAILABLE TASKS/OPERATIONS ON WEB CONSOLE	CAPABILITY ON CONSOLE	DESCRIPTION	WEB CONSOLE
Run backup now	Data Protection/Management Operations This capability is also required to enable Backup Now operation on Backup Monitor tool.	User can run the incremental backup jobs, but cannot Cancel or Suspend the backup job	
Control Jobs (Suspend and Cancel jobs)	Job Management	User can resume, cancel or suspend the backup job	
Add new schedule	Data Protection/Management Operations Agent Scheduling	User can perform the following in the Web Console: <ul style="list-style-type: none"> • Create a new schedule • Modify/Delete the existing schedules created by user 	

			
Change content to back up	Agent Management	<p>User can perform the following in the Web Console:</p> <ul style="list-style-type: none"> • Add a new content path • Modify/Delete the existing content path created by user • Exclude the content path specified by Administrator 	
Select files to restore	<p>Browse or</p> <p>Browse and In Place Recover or</p> <p>Browse and Out of Place Recover or</p>	<p>User can perform the following in the Web Console:</p> <ul style="list-style-type: none"> • Restore the backed up data to the same place/different place as the original data protection operation. • Restore backed up data from a specific time range. 	

DEFINING DOWNLOAD PRIVILEGE TO LAPTOP OWNERS

By default, the laptop users will have permissions to perform all operations from the Web Console. If you have defined specific rules to enable the user interface options in Web Console, you can define the download privilege as follows:

1. From the CommCell Browser, expand the **Security** node.
2. Right-click the **CommCell User Groups** and then click **New User Group**.
3. Specify the user group name in **Name** box.
4. Click **Capabilities** tab.
5. Select **Browse and Out of Place Recover** and **End User Search** capabilities from the **Available Capabilities** list box.
Click > to move the selected capabilities to the **Assigned Capabilities** list box.
6. Click **Users** tab.
7. Select the existing users available in **Available Users** list.
Click > to move the selected capabilities to the **Member Users** list box.
8. Use the following steps, to add a new user:
 - o Click **Create new User** button.
 - o Type name in **User Name** box.
 - o Type password in **Password** and **Confirm Password** box.
 - o Type name of a user in **Full Name** box.
 - o Type email address in **E-Mail** box.
 - o Click **OK**.
 - o The user will be displayed in the **Available Users** list.
 - o Repeat step 7 to assign the above user to User Group.
9. Click **OK**.



MODIFYING THE DOCUMENTATION LINK FOR BACKUP MONITOR

By default, the Backup Monitor tool  button is configured to launch Laptop User Guide documentation directly from the documentation web site.

However, if you wish to modify the default location to the documentation site that is hosted on intranet site or on a shared network location, use the following

steps.

1. Logon to the CommServe computer.
2. From the Command prompt, login to the CommServe using the `qlogin` command and `commcell` credentials.

For example, to log on to CommServe `server11` with username `user1`:

```
C:\>qlogin -cs server11 -u user1
```

3. Run the following **execscript** operation using **qoperation**:

USAGE:

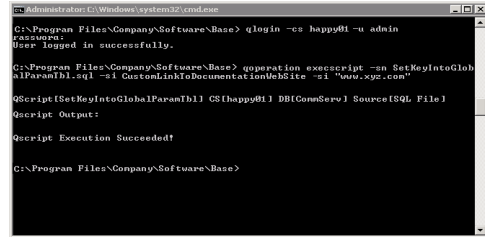
```
qoperation execscript -sn SetKeyIntoGlobalParamTbl.sql -si  
CustomLinkToDocumentationWebSite -si y -si "<URL>"
```

EXAMPLE:

```
qoperation execscript -sn SetKeyIntoGlobalParamTbl.sql -si  
CustomLinkToDocumentationWebSite -si y -si "www.xyz.com"
```

Where:

<URL>: Specify the path of the hosted intranet site or shared network location.



ENABLING SECURED ACCESS FOR WEB SEARCH CLIENT

Use the following steps to enable secured access on the Web search client. This will allow you to access the Web Console using https instead of http.

INSTALL JAVA WITH ALL THE UPDATES

1. Stop the Tomcat services
2. If UAC is enabled, disable it.
3. Download and install the latest version of JAVA with all the updates on the Web client computer.
4. Open the command prompt window on the Web client computer, and execute the following command to verify if JAVA has been properly installed on the Web client computer:

```
C:\>java -version
```

If you find that JAVA with the latest updates has not been installed, uninstall JAVA that you have installed and reinstall it again with all the updates. Navigate to the command prompt on the Web client computer, and run the command specified in step 4 to verify if JAVA has been installed successfully.

Skip this step if the updates are installed successfully.

5. Start Tomcat services. If the Tomcat fails to start, point the JVM manually to Tomcat using the following steps:
 - o Open the command prompt window on the Web client computer, navigate to <PRODUCT_INSTALL_PATH>\Apache\bin folder and execute the following command:

```
C:\<PRODUCT_INSTALL_PATH>\Apache\bin>tomcat6w.exe //ES//GxTomcatInstance001
```

where, Instance001 is the instance installed on the WebClient computer.
 - o On the Tomcat Services Instance properties dialog box, click the **Java** tab, and clear the **Use default** check box.
 - o Restart Tomcat services

CONFIGURE SSL ON THE TOMCAT SERVER

Use the following steps for configuring SSL (Secure Socket layer) on the Tomcat Server:

1. Navigate to command prompt and run the following command:

```
C:\Program Files\Java\jre6\bin>keytool -genkey -alias cvtomcat -keyalg RSA -keystore "C:\Program  
Files\company\product\Apache\cert\keystore"
```

2. Backup the `server.xml` file located in <product_install_path>\Apache\conf before making any changes to it.
3. In order to setup a JAVA JSSE connector to support SSL, search for the following entry in the `server.xml`:

```
<Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />
```

Modify the above entry as following:

```
<Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="off" />
```

4. Add the following entry to the `server.xml` file:

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol" SSLEnabled="true" maxThreads="150" scheme="https"
```

```
secure="true" clientAuth="false" keystoreFile="C:/Program Files/CommVault/Simpna/Apache/cert/keystore" keystorePass="mnoettomcat"
sslProtocol="TLS" />
```

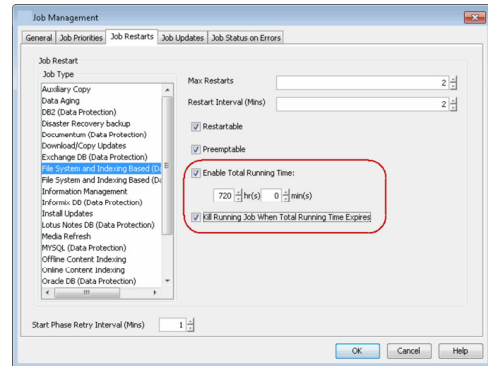
5. Save the `server.xml` file, and restart the Tomcat services.

For more information, refer to <http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html>.

CONFIGURING JOB RESTARTABILITY

Jobs that fail to complete successfully are automatically restarted based on the job restartability configuration set in the Control Panel. For laptop backup jobs and install updates job, it is recommended to configure the job restartability as follows:

1. From the CommCell Browser, click **Control Panel** icon.
2. Select **Job Management**.
3. From the **Job Type** list, select **File System and Indexing Based (Data Protection)**.
4. Select the **Enable Total Running Time** check and specify the **Total Running Time** as 720 or 1440 hrs. The **Total Running Time** is the maximum elapsed time before a job can be restarted or killed.
5. Select the **Kill Running Jobs When Total Running Time Expires** check box to kill the job after reaching the maximum elapsed time.
6. From the **Job Type** list, select **Install Updates**.
7. Select the **Enable Total Running Time** check box and specify the **Total Running Time** as 72 hrs. The **Total Running Time** is the maximum elapsed time before a job can be restarted or killed.
8. Select the **Kill Running Jobs When Total Running Time Expires** check box to kill the job after reaching the maximum elapsed time.
9. Click **OK**.



LICENSE REQUIREMENTS

Laptop Backup requires following licenses based on the License Type:

- For traditional license:
 - **iDataAgent for Linux File System** license is required for each laptop client.
 - **Block Level Deduplication** license is required for the MediaAgent hosting the deduplication store.
- For more information on licensing, see License Administration.
- For License Usage by Capacity, both **Data Protection Core** (for Backup) and **Data Protection Enterprise** (for Backup) license can be used.
- For more information, see License Usage by Capacity.

SEE ALSO

- Alternate Data Path (GridStor) - Provides complete information on Alternate Data Paths.
- Firewall - provides information on configuring the different types of firewalls.

