CA Spectrum®

Administrator Guide

Release 9.4

CA Technologies Product References

This document references the following CA Technologies products:

- CA Spectrum® (CA Spectrum)
- CA Spectrum® Network Configuration Manager (NCM)
- CA Spectrum® Service Performance Manager (SPM)
- CA Spectrum® Service Manager (Service Manager)
- CA Event Manager
- CA Service Desk
- CA Unicenter® Network and Systems Management (NSM)
- CA Embedded Entitlements Manager (CA EEM)
- CA SiteMinder®
- CA NetQoS® Performance Center (CA Performance Center)

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 4: OneClick Administration Pages 41

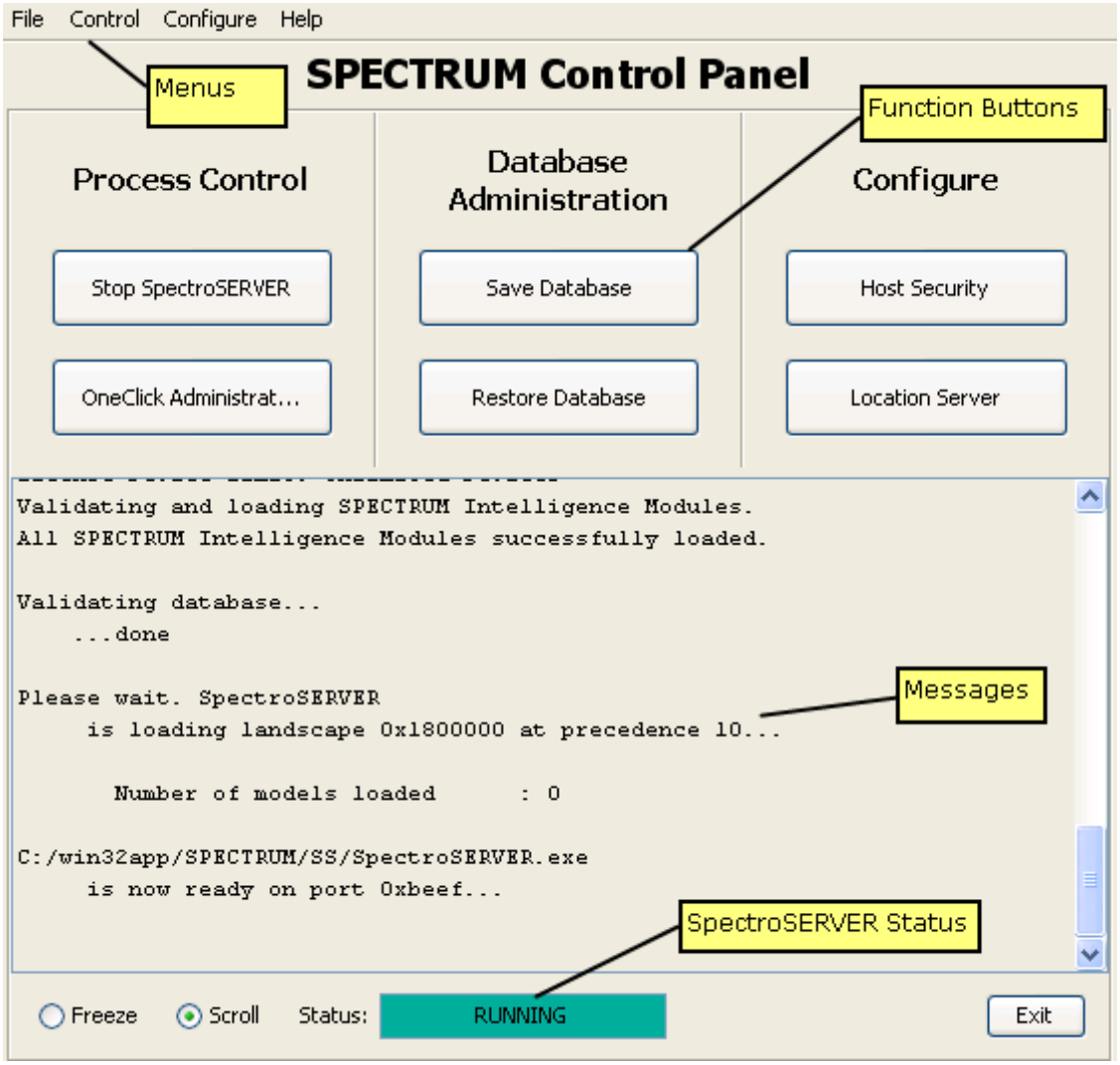
Chapter 5: User Administration in OneClick 55

Chapter 1: CA Spectrum Control Panel

This section contains the following topics:

CA Spectrum Control Panel Overview

The CA Spectrum Control Panel lets you configure resources, start and stop the SpectroSERVER, perform database administration, and maintain the CA Spectrum installation. It provides menus, function buttons, messages, and a status bar.



Access the CA Spectrum Control Panel

To access the CA Spectrum Control Panel on the SpectroSERVER host, you can take the following steps:

- **Windows:** Click Start, Programs, CA, CA Spectrum Control Panel.
- **Solaris:** Select Control Panel from the list of items on the CA Spectrum menu.
- **Linux:** Run the SCP command located in *$SPECROOT*/bin/

You must be logged in as the install user or as someone in the install user's group to launch applications using the CA Spectrum Control Panel.

File Menu

The File menu provides the following functionality:

Select Host Machine

Lets you select the SpectroSERVER that you want to manage.

Save Database

Lets you create an online backup or perform a complete save of the SpectroSERVER database.

Online Backup

If the SpectroSERVER is running, selecting Save Database initiates a CA Spectrum online backup.

Save

If the SpectroSERVER is not running, selecting Save Database initiates a complete save of the SpectroSERVER database using SSdbsave (with the -c and -m switches).

Note: For more information, see the *Database Management Guide.*

Restore Database

Lets you load a previously saved database.

Initialize to Legacy Database

Initializes your database to the state that existed following your last installation. All models that are specific to your network are removed. The remaining database structure consists of the modeling catalog and a few internal models.

Important! Do not use this feature without first making a backup copy of your database.

More information:

Restore a Database (see page 17)
Initialize to Legacy Database (see page 18)

Control Menu

The Control menu provides the following functionality:

Start/Stop SpectroSERVER

Controls the operation of the SpectroSERVER.

Auto Start/Stop Archive Manager

Lets you configure the Archive Manager to start or stop with the SpectroSERVER on the workstation you are managing.

Start/Stop Archive Manager

Starts or stops the Archive Manager.

Note: The Archive Manager control buttons will be disabled when any other running process has locked the database.

Important! Do not attempt to change the state of the Archive Manager when you are running an online backup.

OneClick Administration

Prompts for the host and port of the OneClick web server and opens a browser to the OneClick Administration Pages.

Note: To determine the browser location on Windows, CA Spectrum opens the default web browser for the current user. To determine the browser location on UNIX and Linux, CA Spectrum uses the PATH variable to first locate Firefox, Mozilla, and then Netscape. To specify a browser, set the SPECTRUM_BROWSER environment variable. For more information, see the *Operator Guide*.

SpectroSERVER Performance

Opens the Performance View application. For more information about Performance View, see the *SpectroSERVER Performance Administration Guide*.

Users

Lets you view user details, set a new password for an existing user, and create an administrative super user account.

More information:

About the OneClick Administration Pages (see page 42)

Configure Menu

From the Configure menu you can open the Model Type Editor, and you can open dialogs that let you configure the SpectroSERVER, the location server, and host security. The Configure menu contains the following selections:

- SpectroSERVER
- Location Server
- Host Security
- Model Type Editor

More information:

SpectroSERVER Configuration Dialog (see page 13)
Location Server Configuration Dialog (see page 15)
Host Security Dialog (see page 16)
Model Type Editor (see page 17)

SpectroSERVER Configuration Dialog

The SpectroSERVER Configuration dialog lets you control certain aspects of the SpectroSERVER configuration. When you make changes in this dialog, you are editing the .vnmrc resource file, which controls SpectroSERVER operation and performance.

Note: See the *Distributed SpectroSERVER Administrator Guide* for more information about the .vnmrc file.

Communications

Communications Port

Specifies a TCP port number indicating the port through which the client's user interface communicates with the SpectroSERVER. This parameter can be any valid, unreserved TCP port greater than the port number assigned to the IPPoPORT_USERRESERVED and less than 64,000.

Default: 0xBEEF

SNMP Comm. Port

Specifies a value that can be used to select a port from which SNMP requests can be sent via the SpectroSERVER. It can be set to any unsigned 16-bit integer in the range 0x400 (1,024) to 0xFFFF (65,535). Some implementations of SNMP agents treat the port as a signed number. In these cases, this resource must be set to a value between 0x400 (1,024) to 0x7FFF (32,768).

File Paths

The SpectroSERVER Configuration dialog provides access to the file paths that are defined within the .vnmrc file.

VNM File Path

Specifies the root subdirectory which contains SpectroSERVER external files such as specific device alert mapping.

Performance Tuning

SpectroSERVER is a multi-threaded process. During normal operation, each subsystem allocates numerous work threads. Each thread consumes memory and computing capacity. As a result, they can affect performance. Max Number of Poll Threads and Work Thread Age are two of the parameters that control the allocation of work threads.

Note: To better understand the interaction between resources and the parameters that control work threads, see the *Deployment Capacity and Optimization Best Practices Guide*.

Max. Number of Poll Threads

Specifies the maximum number of work threads dedicated to polling.

Work Thread Age

Specifies how many seconds a work thread can remain in the pool without being used. Work threads that are no longer needed by a subsystem are returned to a work thread pool.

Event Log

Under normal conditions, events are recorded in the CA Spectrum Distributed Data Manager (DDM) database. However, if communication between the SpectroSERVER and the Archive Manager is lost, event information is stored temporarily in the SpectroSERVER database until communication is re-established.

The growth of this temporary event data in the SpectroSERVER database is regulated by entries in the SpectroSERVER .vnmrc resource file. Use the Event Log fields to edit these settings.

Max Event Recs to Save

Maximum number of records that can be stored in the database.

Default: 20,000

Event Record Increment

Specifies the number of records to be deleted from the database when the number of records exceeds the Max Event Recs to Save value.

Default: 100

Note: If you remove the event_record_increment entry from the .vnmrc file, the default is 250 records.

Statistics Log

Under normal conditions, statistics are recorded in the CA Spectrum Distributed Data Manager (DDM) database. If communication between the SpectroSERVER and the Archive Manager is lost, however, statistics information is stored temporarily in the SpectroSERVER database until communication is re-established.

The growth of this temporary statistics data in the SpectroSERVER database is controlled by entries in the SpectroSERVER .vnmrc resource file. Use the Statistics Log fields to edit these settings.

Max Statistics Recs to Save

Specifies the maximum number of records that can be stored in the database.

Default: 5,000

Statistics Record Increment

Specifies the number of records to be deleted from the Statistics Log database when the number of records exceeds the Max Statistics Recs to Save value.

Default: 500

Location Server Configuration Dialog

The CA Spectrum *Location Server* is used to locate other CA Spectrum services on the network. The Location Server Configuration dialog lets you define the location server characteristics and your client applications.

Note: For more information about location servers, see the *Distributed SpectroSERVER Administrator Guide*.

The Location Server Settings section of the Location Server Configuration dialog contains the following settings:

Main LS Host

Specifies the Main Location Server (MLS) hostname. This host workstation determines which connection services are available on the network. Other Location Servers connect to the MLS to determine the location and availability of services.

Main LS Port

Specifies the Main Location Server port address.

Default: 0xdaff

Backup Main LS Host

Specifies the backup MLS name. If the MLS is not available when another host attempts to connect to it, the host is redirected to the backup MLS.

When a CA Spectrum system starts up (or the Process Daemon, processd, is stopped and started), the location server on that system attempts to connect to the MLS to download “map” information. Map information is a listing of each CA Spectrum service that is available and the location of each server. If the MLS is down at that time, the map information is not available to the CA Spectrum system. Therefore, clients cannot connect to any CA Spectrum service.

The role of the backup Main Location Server is to provide redundancy for the MLS in this scenario. If a backup MLS has been configured, the Location Server attempts to contact it after contact to the MLS has failed. Clients can then access CA Spectrum services even though the MLS is down.

Use highly available systems for both the backup MLS system and the Main Location Server.

Each system that is pointing to the same MLS should also point to the same backup main location server.

Backup Main LS Port

Specifies the backup MLS port address.

Max Connections

Specifies the maximum number of port connections that can be made to this location server.

Default: 750

The Client Applications section of the Location Server Configuration dialog contains the following settings:

Hostname

Specifies the client application main location server hostname. It preserves landscape map integrity for different environments.

Port

Specifies the client application Main Location Server port.

Host Security Dialog

The Host Security dialog lets you enter a list of servers and users allowed to connect to the host. You can also do this by editing the .hostrc file in the CA Spectrum directory.

Note: For more information about the .hostrc file, see the *Distributed SpectroSERVER Administrator Guide*.

More information:

Configure Host Security (see page 19)

Model Type Editor

The Model Type Editor option in the Configure menu starts the Model Type Editor application. The Model Type Editor lets you modify the SpectroSERVER modeling catalog and configure relations, object-classes, and their contents. This option is not available unless the SpectroSERVER is in an INACTIVE or STOPPED state.

Note: To learn more about the operation of the Model Type Editor, see the *Model Type Editor User Guide*.

SpectroSERVER Status

The Status field in the CA Spectrum Control Panel indicates the status of the SpectroSERVER with text and color.

Starting: yellow

This field changes to Running (green) after the start-up period expires.

Stopping: yellow

This field changes to Inactive (blue) after the server has shut down.

Running: green

This field indicates a normal running state.

Terminated: red

This condition is abnormal and indicates an error.

Inactive: blue

This field indicates that server shutdown is complete.

Restore a Database

You can load a previously saved database using either the File menu or the Restore Database button.

Follow these steps:

1. Click Restore Database in the CA Spectrum Control Panel.

   A dialog asks whether you want to initialize your database.

2. Click No to perform a models-only load.

   The Restore Database dialog opens.

3. Locate and select the appropriate previously saved database backup.

4. Do one of the following:
   - Windows: Click Open.
   - Solaris: Click Ok.
5. Click OK.

   The database load begins. If SpectroSERVER is running, SpectroSERVER restarts after the database loads.

Initialize to Legacy Database

Initialize to Legacy Database initializes your SpectroSERVER database to its state following your last installation. All models specific to your network are removed. The remaining database structure consists of the modeling catalog and a few internal models.

Important! Do not use this feature without first backing up the database.

Follow these steps:

1. Select File, Initialize to Legacy Database.

   An information dialog displays a warning.
2. Click Yes to continue. Or click Cancel to retain your existing database.

   If the SpectroSERVER is running when you start to initialize your database, a second dialog indicates that the SpectroSERVER is shut down during this process.
3. Click Yes.

   The initialization starts.
4. Restart your OneClick web server and restart any open OneClick Consoles.

   Note: This action refreshes the OneClick explorer hierarchy and topology view.

   The SpectroSERVER database is initialized.

Configure Host Security

The Host Security window lets you enter a list of servers and users allowed to connect to the host.

Note: You can also control access to the host by editing the .hostrc file in the CA Spectrum directory. For more information, see the *Distributed SpectroSERVER Administrator Guide*.

- To add a server/user to the list, enter the name in the appropriate box and click Add.
- To delete an item from either the Server List or the User List, select the server or user and click Remove.
- To let all hosts and users have access to the host server, enter a plus sign in Server List Add box and click Add.
- To let only the server where you are logged in to connect to the server, enter a minus sign in the Server List Add box and click Add. The minus sign becomes the name of your computer when is is added to the Server list.

Note: To save the host security configuration, at least one entry in the Server List is required.

Chapter 2: OneClick Web Server Administration

This chapter discusses tasks that OneClick administrators can perform to configure and optimize the OneClick web server. It also covers server-related and client-related configuration and maintenance issues.

This section contains the following topics:

Start and Stop the OneClick Web Server from the Command Line

You can start or stop the OneClick web server from a command prompt.

On Solaris or Linux, log in as root. Use the following commands:

- To start the web server:

  `<$SPECROOT>/tomcat/bin/startTomcat.sh`

- To stop the web server:

  `<$SPECROOT>/tomcat/bin/stopTomcat.sh`

- To restart (stop, then start) the web server:

  `<$SPECROOT>/tomcat/webapps/spectrum/restart.sh`

To start or stop the OneClick web server on Windows, enter the following commands at a command prompt:

- To start the web server:

  ```
  C:\> net start spectrumtomcat
  ```

- To stop the web server:

  ```
  C:\> net stop spectrumtomcat
  ```

Start and Stop the OneClick Web Server from an Administration Page

Several of the OneClick Administration Pages include Restart OneClick Server buttons. You can easily restart the OneClick web server to apply a configuration change. These restart buttons use the 'at' utility to schedule a restart script to run. You can configure this utility for different platforms.

If an error occurs while restarting the OneClick web server, you see an error message on the administration page. In this event, use the troubleshooting tips in one of the following sections to identify the problem. Or restart the web server from the command line.

Troubleshooting the at utility on Windows

By default, CA Spectrum users have permissions to execute 'at' on Windows. However, verify that the current user and the current user group have Read and Execute permissions on the C:\WINDOWS\system32 folder.

Check the status of the 'at' operation by typing 'at' in a command prompt shell to view the 'at' queue. The queue contains all jobs scheduled through 'at' that are still pending. If earlier attempts on these scheduled jobs have failed, the jobs also have an error status code.

Troubleshooting the at utility on Solaris or Linux

Users listed in the following file are denied permission to use the 'at' utility:

- (Solaris) /usr/lib/cron/at.deny
- (Linux) /etc/at.deny

Verify that the user currently running the OneClick process (the OneClick web server) is not listed in this file. Typically, this user is the CA Spectrum Installation Owner user. You can identify the user by entering the following command in a command shell:

```
ps -eaf | grep OneClick
```

If the 'mail' utility is set up for the operating system and the current OneClick user, 'at' automatically emails notifications about scheduled jobs and their output or error messages. Check these email notifications for pertinent information.

More information:

Start and Stop the OneClick Web Server from the Command Line (see page 21)

Start and Stop the OneClick Web Server from the Windows Control Panel

You can start and stop the OneClick web server from the Windows Control Panel.

Follow these steps:

1. Click Start, Control Panel.

   The Control Panel opens.

2. Double-click Administrative Tools.

   The Administrative Tools window opens.

3. Double-click Services.

   The Services window opens.

4. Select SpectrumTomcat from the services list and determine its status.

5. Do *one* of the following:

   - If the SpectrumTomcat service is running, click Stop to stop the web server.

     Or click Restart to stop and then start the web server.

   - If the SpectrumTomcat service is stopped, click Start to start the web server.

Configure the OneClick Server to Support Over 100 Users

To support a large number of users on a single Solaris OneClick server, increase the hard limit on the number of file descriptors. We recommend this step to ensure support for more than 100 OneClick Console users. The /etc/system file sets the limit of file descriptors.

Follow these steps:

1. Make a backup of your /etc/system file.

2. Add the following line to your /etc/system file:

   ```
   set rlim_fd_max=4096
   ```

Launch OneClick Clients with Context

You can launch OneClick clients within the context of a topology or model. Pass contextual parameters and values with the URL that launches OneClick. The URL can include parameters in the following format:

`http://<hostname>/spectrum/oneclick.jnlp?<parameter>=<value>`

Possible parameters include the following:

topology Parameter

The value of the topology parameter can be a model handle or an IP address. Using this parameter in a URL launches a OneClick client or reuses an existing one, selects the Explorer tab if not already selected, expands the tree to show the model, selects the Topology tab if not already selected, and selects in the Topology panel the model specified by the topology parameter in the URL.

Examples:

`http://<hostname>/spectrum/oneclick.jnlp?topology=0x3780003d`
`http://<hostname>/spectrum/oneclick.jnlp?topology=10.253.9.7`

explorer Parameter

The value of the explorer parameter can be a model handle or an IP address. Using this parameter in a URL launches a OneClick client or reuses an existing one, selects the Explorer tab if not already selected, and expands the tree to show the model. The currently selected tab in the Contents panel will reflect the new model.

Examples:

`http://<hostname>/spectrum/oneclick.jnlp?explorer=0x3780003d`
`http://<hostname>/spectrum/oneclick.jnlp?explorer=10.253.9.7`

alarm Parameter

The value of the alarm parameter can be either the integer alarm ID (to facilitate integration with legacy applications), the complete global alarm ID (in the form 3f983d3d-2045-1000-012b-000bdb5a1c31), or *<model handle>@<alarm ID>*. Using this parameter in a URL launches a OneClick client or reuses an existing one, selects the Explorer tab if not already selected, expands the tree to show the model, selects the Alarms tab if not already selected, and selects the alarm.

Examples:

`http://<hostname>/spectrum/oneclick.jnlp?alarm=0x3780003d@7710`

where 0x3780003d@7710 is *<modelhandle>@<alarm ID>* and

`http://<hostname>/spectrum/oneclick.jnlp?alarm=7710`

where 7710 is the integer *<alarm ID>*.

If you pass the integer alarm ID, pass the model handle also. The integer alarm ID is not guaranteed to be unique across SpectroSERVERs. The full global alarm ID is preferable as it is unique across SpectroSERVERs, but it may not be available to the application launching OneClick.

When launching in context, a new instance of OneClick is not launched if an instance is already running on the host. The context is changed in the current instance of OneClick.

Configure OneClick Client Memory Settings

The default initial memory footprint for OneClick clients is 96 MB, with a maximum of 512 MB. The initial memory setting lets the Java Virtual Machine (JVM) preallocate memory for potentially faster startup. The maximum setting lets the JVM memory grow into a limited space, to accommodate application use that requires additional memory. For example, large views, searches, and other actions can require more memory.

If clients experience out-of-memory errors, you can increase the maximum memory setting.

If you change the client memory settings, keep in mind that the settings apply to all OneClick clients. Therefore, take into account any client computers that lack sufficient resources. Use a modest adjustment, such as a 25% increase in the maximum memory allocation, to 640 MB. The steps in this procedure are an *optional* method for addressing out-of-memory issues.

Important! Setting either one of these memory values too high can cause the OneClick clients to fail to launch.

Follow these steps:

1. Click Administration in the OneClick home page.

   The Administration Pages open.

2. Click OneClick Client Configuration in the left panel.

   The OneClick Client Configuration page opens.

3. Complete the fields (see page 48) in the Java Memory Usage section.

4. Click Save.
5. Restart any running OneClick clients.

   The OneClick memory settings that you configured are applied to the OneClick clients.

Configure OneClick Web Server Memory Settings

By default, the maximum memory that the OneClick web server uses is 1024 MB. If the OneClick web server is using more than 75 percent of its configured maximum memory, consider increasing the maximum memory value.

If the web server runs out of memory, an OutOfMemory error appears in the following log files:

- tomcat/logs/stdout.log (for Windows)
- tomcat/logs/catalina.out (for Linux/Solaris).

You can change memory allocations on the Web Server Memory Administration page (see page 54). Test with a modest adjustment, such as a 25% increase in the maximum memory allocation, to 1280 MB. The steps in this procedure are an optional method for addressing out-of-memory issues.

Note: Restart the OneClick web server for these changes to take effect.

Follow these steps:

1. Verify the OneClick web server memory usage:
   a. Click Administration in the OneClick home page.

      The Administration Pages open.

   b. Click Web Server Memory in the left panel.

      The Web Server Memory page opens.

   c. Check the OneClick Server Memory Usage field to verify if memory usage is greater than 75 percent of the configured maximum.

2. Configure the maximum OneClick web server memory usage:

   a. In the Maximum Memory the Server Can Use (In MB) field, enter the new value.

      Note: Do not set the maximum memory to a value larger than the available memory for the system.

   b. Click Save.

      A dialog prompts you to commit your changes and restart the OneClick web server.

   c. Click OK.

      Your changes are saved, and the OneClick web server is restarted.

Configure the OneClick Web Server URL

The *Operator Guide* describes the OneClick home page as a central place where users can launch the OneClick client. By default, all OneClick users must use the following URL to access the OneClick home page:

`http://<OneClick web server>/spectrum`

Also by default, the URL http://<OneClick web server> launches a Tomcat web server configuration page. You can configure the OneClick web server to automatically redirect from http://*<OneClick web server>* to http://*<OneClickweb server>*/spectrum.

Follow these steps:

1. Navigate to the <$*SPECROOT*>\tomcat\webapps\ROOT directory.
2. Create a file named index.html using your preferred text editor.
3. Edit the index.html file to contain the following text:

```
<html>
    <head>
            <meta http-equiv="refresh" content="0;url=/spectrum">
    </head>
    <body>
    </body>
</html>
```

4. Save the index.html file in the ROOT directory referenced in Step 1.

   All OneClick users navigating to http://*<OneClick web server>* are now redirected automatically to http://*<OneClick web server>*/spectrum.

Configure OneClick MySQL Server Passwords

You can change the passwords for both the default OneClick MySQL user (OC_user) and the administrative OneClick MySQL user (OC_admin). Change passwords on the MySQL Password Administration page.

Important! Do not attempt to manually change the MySQL user passwords using a MySQL client connection. Storage of the passwords in OneClick depends on MySQL connectivity. As a result, the only safe way to change the passwords is through the OneClick MySQL Password Administration page.

Follow these steps:

1. Click Administration in the OneClick home page.

   The Administration Pages open.

2. Click MySQL Password in the left panel.

   The Change MySQL Password page opens.

3. Enter the current password and the new password for the user whose credentials you want to modify.

4. Confirm the new password.

5. Click Change Password.

   The password changes immediately. Restarting MySQL or Tomcat is not required.

More information:

MySQL Password Page (see page 46)

Chapter 3: OneClick Server Communications and Network Configuration

This section contains the following topics:

Name Resolution Requirements

For the OneClick web server system to communicate with a SpectroSERVER, the OneClick web server system must be able to resolve the non-fully-qualified hostname of the SpectroSERVER to an IP that can be used to reach the SpectroSERVER.

We recommend using hosts files for the name resolution of SpectroSERVER hostnames. This practice makes it less likely that name resolution is impacted by a network failure.

Configure OneClick for Secure Sockets Layer

OneClick supports the Secure Sockets Layer (SSL) protocol to encrypt communications between the OneClick web server and OneClick clients. OneClick clients can access information securely across unsecured networks, such as the Internet. In addition to encryption, SSL uses certificates for authentication. Authentication protects users from downloading and running applications from suspicious or "untrusted" sources.

Both Certificate Authority-signed certificates and self-signed certificates provide secure connections using SSL encryption. However, certificates signed by a Certificate Authority provide an additional level of security. These certificates verify the creator of the certificate and certify that the product is truly from that vendor. Certificates that are signed by a Certificate Authority protect servers by making it difficult to impersonate a trusted entity (the certified vendor). However, self-signed certificates are appropriate if you require the encryption that an SSL certificate provides without requiring proof of the certificate source.

Follow these steps:

1. On the OneClick web server host, change to the *$SPECROOT*/Java/bin directory.
2. Generate a private self-signed certificate in the custom cacerts file by issuing the following command:

   ```
   ./keytool -genkey -alias tomcatssl -keyalg RSA
   -keystore c:/win32app/Spectrum/custom/keystore/cacerts
   ```

   The keytool prompts with a series of questions and uses the values that you specify to perform the following actions:

   - Create an issuer name for your organization (This name is an X.500 Distinguished Name that is intended to be unique across the Internet. For more information, see the keytool utility at http://java.sun.com).
   - Generate the self-signed certificate using the issuer name.

3. Enter your answers to the following questions:

   ```
   Enter keystore password:
   ```

   If you change the default password for the Tomcat web server, specify the custom password in the *$SPECROOT*/tomcat/conf/server.xml configuration file.

   ```
   What is your first and last name?
   ```

   Enter the common name (with the fully qualified domain name) of your website. For example, www.ca.com.

   ```
   What is the name of your organizational unit?
   ```

   Enter a small organization name, such as the name of a division, business unit, or department. For example, Purchasing.

   ```
   What is the name of your organization?
   ```

   Enter a large organization name, such as ABCSystems, Inc.

   ```
   What is the name of your City or Locality?
   ```

   Enter your city name, such as Hyderabad.

   ```
   What is the name of your State or Province?
   ```

   Enter the full name, such as Andhra Pradesh.

   ```
   What is the two-letter country code for this unit?
   ```

   Enter the two-letter country code. For example, IN.

   ```
   Is CN=www.ca.com, OU=Purchasing, O="ABCSystems, Inc.", L=Hyderabad,
   ST=Andrapradesh, C=IN correct?
   ```

   Enter Yes.

   ```
   Enter key password for <tomcatssl> (RETURN if same as keystore password):
   ```

   Enter key password for <tomcatssl>. Press Enter to use the same password as the keystore password.

4. (Optional) If you require a certificate that is signed by a Certificate Authority, request the certificate from the Certificate Authority and then import it.

   Note: Before proceeding with this step (Step 4), as a best practice, skip to Step 5 and set up SSL. You can then test to determine whether the information that you provided in the previous step was correct. If HTTPS works, you can continue with this step.

   As part of certificate configuration, generate a Certificate Signing Request (CSR) file from the system that runs the secure OneClick web server. The Java Development Kit (JDK) that is included with OneClick provides a keytool utility that you can use to generate the CSR file. Use the information that you provided in the previous step. Use the same alias name as tomcatssl.

5. Request and import the Certificate Authority-signed certificate as follows:

   a. On the OneClick web server host, change to the *$SPECROOT*/Java/bin directory.

   b. Generate the CSR file by entering the following command:

      ```
      ./keytool -certreq -alias tomcatssl
      -keystore $SPECROOT/custom/keystore/cacerts -file filename.csr
      ```

      Note: You are prompted for a password. Use the same password that you provided earlier.

      The contents of the .csr file that is generated are used to request the secure certificate from the Certificate Authority (the next step).

   c. Request a secure certificate from a Certificate Authority. Verify the following examples:

      VeriSign: http://www.verisign.com

      TrustCenter: http://www.trustcenter.de

      thawte: http://www.thawte.com

      Instructions are available at these websites.

   d. Import the Certificate Authority-signed certificate into the keystore that is used by the OneClick web server. For more information, see Import a Certificate Authority-Signed Certificate (see page 32).

6. Configure the secure socket on the server that hosts the OneClick web server. For more information, see Configure the Secure Socket on the OneClick Web Server Host (see page 32).

7. If you are running Report Manager, configure OneClick to be launched from Report Manager using SSL. For more information, see Configure OneClick and Report Manager for Secure Sockets Layer (see page 35).

Import a Certificate Authority-Signed Certificate

If you have obtained a Certificate Authority-signed SSL certificate, import it into the keystore that the OneClick web server uses.

A chain (root) certificate from the Certificate Authority must also exist in the keystore. By default, OneClick includes chain certificates from many popular vendors. Click List on the SSL Certificates administration page to view the aliases for these certificates. This information helps you determine whether to obtain one and import it.

Follow these steps:

1. If necessary, download a chain (root) certificate from the Certificate Authority from which you obtained the signed certificate.
2. If you downloaded a chain certificate in the previous step, import it into the keystore used by the OneClick web server:
   a. On the OneClick web server host, change to the *$SPECROOT*/Java/bin directory.
   b. Enter the following command:

      ```
      ./keytool -import -alias root -keystore $SPECROOT/custom/keystore/cacerts
      -trustcacerts -file root_chain_certificate_filename
      ```

      Note: You are prompted for a password for the Tomcat web server. The alias name does not have to be 'root'. You can supply a more descriptive name for the type of root certificate that you are importing. The alias name cannot already exist.
3. Import the Certificate Authority-signed SSL certificate into the keystore used by the OneClick web server:
   a. If necessary, on the OneClick web server host, change to the *$SPECROOT*/Java/bin directory.
   b. Enter the following command:

      ```
      ./keytool -import -alias tomcatssl -keystore
      $SPECROOT/custom/keystore/cacerts -trustcacerts -file
      your_certificate_filename
      ```

      Note: You are prompted for a password for the Tomcat web server. Use the same alias that you used when you generated the private self-signed certificate. See Name Resolution Requirements (see page 29) for more information.

Configure the Secure Socket on the OneClick Web Server Host

Configure the secure socket on the server that hosts the OneClick web server. Consider this task as the final step in configuring the OneClick web server for SSL.

Note: CA Spectrum supports the use of SSL v3.

Follow these steps:

1. Shut down the OneClick web server.
2. Open $SPECROOT/tomcat/conf/server.xml in your preferred text editor.
3. Locate the following section in the server.xml file:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 443 -->
    <!--
    <Connector
           port="443" minProcessors="5" maxProcessors="75"
           enableLookups="true" disableUploadTimeout="true"
           acceptCount="100" debug="0" scheme="https" secure="true"
           clientAuth="false" sslProtocol="TLS" ssl_enabled=yes
           keystoreFile="<SPECROOT>/custom/keystore/cacerts"
           keystorePass="changeit">
     </Connector>
    -->
```

   By default the <Connector> element in the section is commented out.

   Note: The preceding XML fragment is Windows-specific, with 443 as the default port where the OneClick web server listens for SSL communications. End users can omit the port from the URL for accessing the OneClick home page:

   `https://<fully_qualified_host_name>/spectrum`

   On a UNIX-based installation, the OneClick web server is not run as root, and the default port is 8443 (because it must be greater than 1024). As a result, end users must specify the port number in the web browser when they enter the URL to access the OneClick home page:

   `https://<fully_qualified_host_name>:8443/spectrum`

4. Remove the comments around the Connector definition. Perform the following actions:
   a. Remove "<!--" from the line preceding to <Connector.
   b. Remove "-->" from the end of the section (after </Connector>).

5. Replace the <*SPECROOT*> variable in the value for the keystoreFile attribute with the fully qualified path to the directory where CA Spectrum is installed. You can use the cacerts file for the keytool commands to generate the certificates. Verify the following examples:

   Windows

   ```
   C:/win32app/SPECTRUM/custom/keystore/cacerts
   ```

   UNIX

   ```
   /usr/SPECTRUM/custom/keystore/cacerts
   ```

6. Save and close the server.xml file.

7. If you have CA Spectrum integrated with CA Performance Center, perform the following steps to enable the communication between SSL enabled OneClick and CA Performance Center:

   a. Open the "axis2.xml" file in an editor from "$SPECROOT/tomcat/webapps/axis2/WEB-INF/conf".

   b. Locate the following section in axis2.xml:

   ```
   <transportReceiver name="http"


   class="org.apache.axis2.transport.http.SimpleHTTPServer">

           <parameter name="port">8080</parameter>
   ```

   c. Change the section as follows:

   ```
   <transportReceiver name="https"


   class="org.apache.axis2.transport.http.SimpleHTTPServer">

           <parameter name="port">8443</parameter>
   ```

8. Start the OneClick web server.

   You can find instructions on configuring SSL and configuration parameters. For more information, see http://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html.

More information:

Start and Stop the OneClick Web Server from an Administration Page (see page 22)
Start and Stop the OneClick Web Server from the Command Line (see page 21)
Start and Stop the OneClick Web Server from the Windows Control Panel (see page 23)

Configure OneClick and Report Manager for Secure Sockets Layer

If you are running Report Manager and you have configured OneClick to use the Secure Sockets Layer (SSL) protocol to encrypt communications between OneClick clients and the OneClick web server, you must also configure OneClick to be launched from Report Manager using SSL.

Report Manager allows you to create reports on the inventory, performance, change history, and fault history of the network assets managed by CA Spectrum. For more information, see the *Report Manager User Guide*.

Follow these steps:

1. Enable write permissions on the following file:

   `<$SPECROOT>\tomcat\webapps\spectrum\repmgr\js\repmgr.js`

2. Open the file that you modified in the previous step, and locate the launchOneClick function.

3. Locate the following line in the launchOneClick function:

   ```
   url = "http://"+servername+contextApp+"/oneclick.jnlp";
   ```

4. Change "http" to "https" as follows:

   ```
   url = "https://"+servername+contextApp+"/oneclick.jnlp";
   ```

5. Save and close the file.

   Important! This file is overwritten during an upgrade. Repeat this procedure after an upgrade.

Note: You can launch OneClick in the context of a specific report (for example, in the context of a device that is listed in an asset report). However, this type of launch cannot be configured to use SSL.

Errors Connecting to the Secure OneClick Web Server from a OneClick Client Using SSL

Symptom:

I am encountering errors when I try to connect to the secure OneClick web server from a OneClick client using SSL.

Solution:

Verify the following:

- The fully qualified domain name of the host on which the OneClick web server is running was specified in the private key you generated for signing the security certificate used for authentication. When you generated the key, you should have entered the fully qualified domain name at the following prompt: “What is your first and last name?”
- Both the Certificate Authority chain (root) certificate *and* the security certificate were imported into the cacerts file in the custom directory on the secure OneClick web server.

Errors Launching OneClick Client from Report Manager Using SSL

Symptom:

I am encountering errors when I launch a OneClick client from Report Manager using SSL.

Solution:

Verify that you have completed the configuration procedure described in Configure OneClick and Report Manager for Secure Sockets Layer (see page 35).

Configure OneClick to Communicate through a Web Proxy Server

If you use a web proxy server that relays HTTP and HTTPS requests (such as the iPlanet and Microsoft proxy servers), OneClick honors the proxy settings used by Java Web Start. OneClick supports both HTTP and HTTPS proxies and also supports proxy authentication. An administrator must configure the OneClick web server to communicate through a proxy server.

All clients connecting through a proxy must configure the proxy settings in the Java Web Start preference console. See the *Installation Guide* for more information about the Java Web Start proxy settings. To connect through an HTTP 1.1 proxy, that console setting might be the only required change.

Note: The following changes are not necessary to connect to a proxy that supports HTTP 1.1.

For HTTP 1.0 proxy support, configure the OneClick web server to communicate through a proxy server.

Follow these steps:

1. Open the <$*SPECROOT*>/tomcat/conf/server.xml file for editing using your preferred text editor.
2. Add the following attribute to any active Connector elements:

   `maxKeepAliveRequests="1".`

   Setting this attribute to 1 disables keepalives.
3. Save the changes to the server.xml file.
4. Stop and restart the OneClick web server.

More information:

Start and Stop the OneClick Web Server from an Administration Page (see page 22)
Start and Stop the OneClick Web Server from the Command Line (see page 21)
Start and Stop the OneClick Web Server from the Windows Control Panel (see page 23)

Troubleshoot Proxy Issues

A failed attempt to launch a OneClick client with a proxy results in the normal conditions described in Step 1 and Step 2 and the failure in Step 3:

1. A web browser can access the OneClick web server and load the OneClick home page at *http://<hostname>:<portnumber>*/spectrum/index.jsp (through the proxy).
2. Java Web Start can access the OneClick web server and download the needed OneClick files.
3. The OneClick client *cannot* access the OneClick web server and fails with a “Can't connect to ...” error.

Note: If the procedures in Configure OneClick to Communicate through a Web Proxy Server (see page 36) do not enable OneClick to communicate through the proxy server in your environment, consider disabling web proxies. For more information, see the *Installation Guide* for information.

Troubleshoot Poor OneClick Client Performance

Platform: Windows

Symptom:

The OneClick clients take a long time to start up. Once the clients have started, users experience long wait times for the user interface to react to mouse clicks and navigation tasks. They are so slow that we can hardly use them.

Solution:

This behavior results from the default setting for the "reuseConnections" Java System property, which is "false". In previous versions of CA Spectrum, the default value was "true". A change was made to facilitate out-of-the-box connectivity for users with web proxies or load balancers in their environment. Without reusing connections, SSL certificate verification is performed for every request from client to server. This work is expensive, in terms of round-trip times.

Change the value of the "reuseConnections" Java Runtime System property to "true".

To change the property setting, edit the oneclick.jnlp file.

Follow these steps:

1. Navigate to the following directory:

   `<$SPECROOT>/tomcat/webapps/spectrum/`

2. Open the oneclick.jnlp file for editing using your preferred text editor.
3. Add the following line, immediately below the "<resources>" line:

   ```
   <property name="reuseConnections" value="true"/>
   ```

   Restart all open OneClick clients.

Firewalled Environments

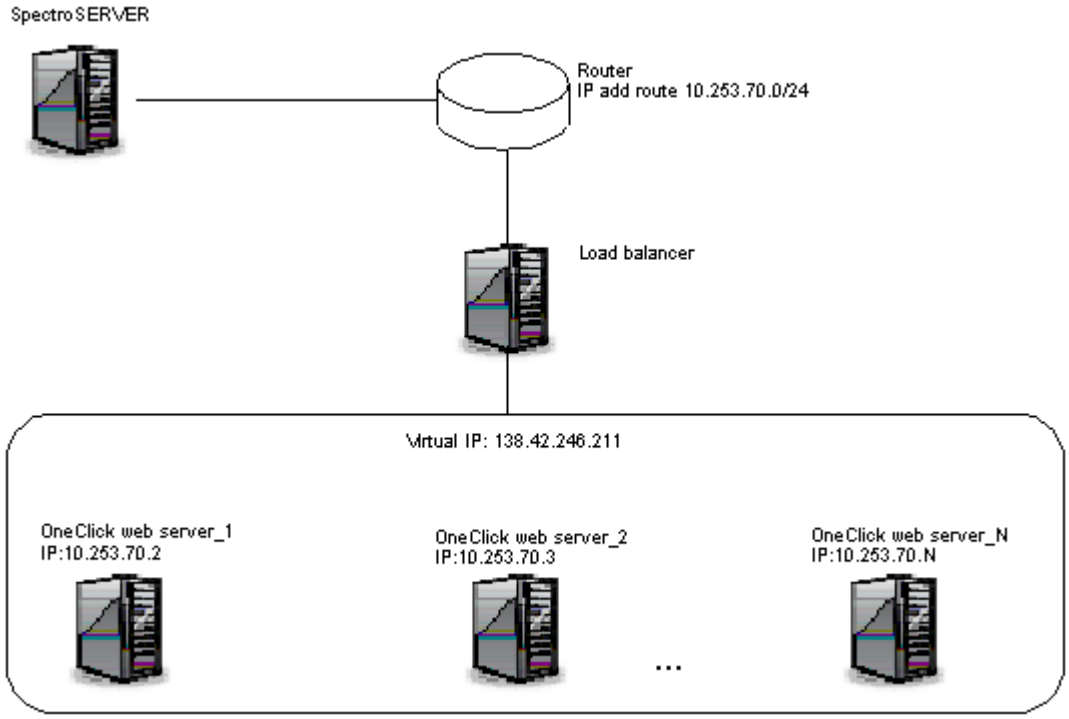
The OneClick web server must communicate with processes on the SpectroSERVER host system to gather data for display to OneClick clients. For the most part, this communication is initiated by the OneClick web server, which establishes connections to specific TCP ports for sending requests and receiving responses. The SpectroSERVER uses bidirectional IIOP (Internet Inter-ORB protocol) to communicate with its CORBA clients. Port 14001 must be open on the firewall to allow the Tomcat web server to receive communications from the SpectroSERVER.

If you use network address translation (NAT) on your network, it is not necessary to perform any additional configuration steps for the OneClick web server to communicate with the SpectroSERVER. However, because SpectroSERVER communication is based on resolving an advertised host name to an IP address, you must configure name resolution on your systems appropriately. Consider a SpectroSERVER host (hostname: “spectrumss”) that is behind a NAT firewall with a private IP address of 192.168.0.2 and a public address of 128.113.0.2. Hosts on the private side of the NAT must resolve “spectrumss” to 192.168.0.2. Hosts on the public side must resolve “spectrumss” to 128.113.0.2.

Load Balancers

To achieve load balancing, identically configured OneClick web servers are accessed through an external load balancing device that employs host/session persistence and any load-balancing mode.

The following figure illustrates a supported load-balancing configuration for multiple OneClick servers.



Check OneClick Web Server Status

You can configure your load balancer to check the status of each OneClick server by using the following HTTP GET statement during periodic server health checks:

`http://<hostname>:<portnumber>/spectrum/stable`

A successful GET returns the contents of the "stable" file. The presence of the stable file indicates that the SpectrumTomcat process is in a stable state. Failure to retrieve the file indicates that the SpectrumTomcat process is not running or is unstable.

How to Log the Actual Client IP Address in a Load Balancing Environment

In a load balancing environment, the load balancer performs SNAT (Source Network Address Translation). As a result, you see the IP Address and the host name of the load balancer instead of the actual client in the logs. You can view the logs when you select Client Log in OneClick.

Configure the load balancer to insert the true source IP address into the HTTP request header field "X-Forwarded-For". You can then see the IP Address and hostname of the actual client that logged in to your OneClick console, instead of the load balancer.

More information about load balancer setup is available on the Internet. For example, see Configuring F5 BIG-IP Load Balancer and Configuring Cisco ACE Load Balancer.

Chapter 4: OneClick Administration Pages

This section contains the following topics:

Access the OneClick Administration Pages

The OneClick Administration Pages are accessible from the OneClick home page. Only OneClick users with OneClick web administration privileges can access these web pages.

To access the OneClick Administration Pages, click Administration in the OneClick home page.

About the OneClick Administration Pages

The Administration Pages provide a navigation panel to select specific features to configure, and a contents panel on the right that displays the configuration information for each feature. The menu bar contains the following options:

Home

Opens the OneClick home page.

CA Spectrum Documentation

Opens the CA Spectrum documentation page.

Debugging

Opens the Debugging page, which contains links to and information about the debugging tools that are included with CA Spectrum.

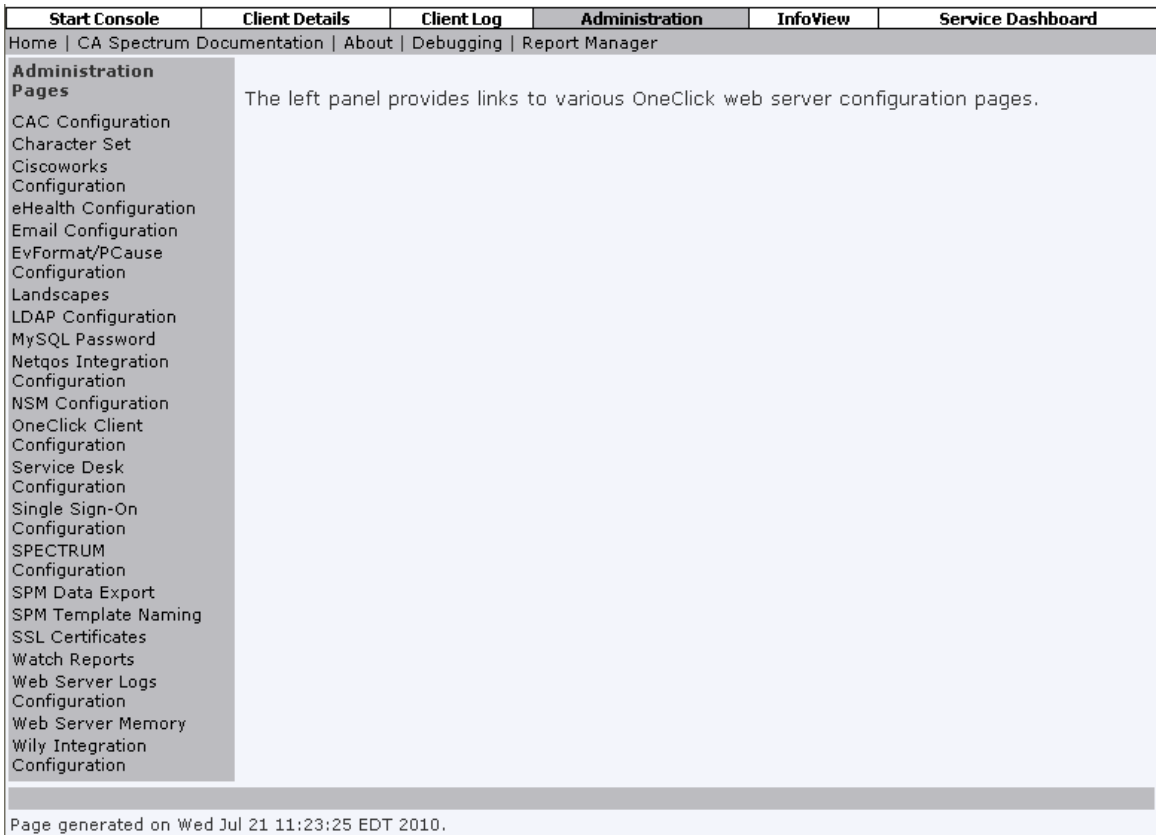
Important! Only use the debugging tools with the help of CA Support.

Report Manager

Opens the Report Manager Admin Tools pages.

Note: For more information about administering Report Manager, see the *Report Manager Installation and Administration Guide*.

The administrative pages that are listed in the navigation panel reflect any OneClick add-on applications that are installed.



The navigation panel and the other OneClick web page links remain available from any OneClick administration page.

CAC Configuration Page

Use the CAC Configuration page to configure OneClick to use Common Access Cards (CAC).

Note: For more information, see the *Common Access Card Authentication Solution Guide*.

Ciscoworks Configuration Page

Use the Ciscoworks Configuration page to configure OneClick for connection to the Ciscoworks web server.

Note: For more information, see the *Cisco Device Management Guid*e.

eHealth Configuration Page

Use the eHealth Configuration page to configure OneClick for connection to an eHealth server. Any changes that you make on this page are reflected in OneClick clients that are launched subsequently. You can use the Test button to test any eHealth configuration changes before you save them.

Note: For more information about integrating CA Spectrum and eHealth, see the *CA eHealth and CA Spectrum Integration and User Guide.*

Email Configuration Page

Use the Email Configuration page to configure OneClick to integrate with your existing email system. Operators can then email alarm-related information from OneClick to assigned troubleshooters and other individuals.

The default SMTP Server Host entry for the mail server is "mailhost", which is a common DNS alias for the mail server. If your environment does not use this alias, you can add an entry for “mailhost” to the /etc/hosts file on the OneClick web server.

Reload EvFormat/PCause Configuration

The EvFormat/PCause Configuration page lets you reload modified Event Format or Probable Cause files into the OneClick server.

You can also reload the EvFormat/PCause files from the command line if desired. Use the command line to reload EvFormat/PCause files from any server.

Follow these steps:

1. Obtain and install GNU wget.

   Note: GNU wget is a simple freeware utility.

2. Run the following command:

   `wget http://`*`ochost`*`:`*`ocport`*`/spectrum/admin/ecds.jsp?reload=Reload --user `*`username`*` --password `*`password`*

   ochost

   Specifies the hostname of the OneClick web server.

   ocport

   Specifies the port number of your OneClick web server.

   username

   Specifies an administrator username for the OneClick web server.

   password

   Specifies an administrator password for the OneClick web server.

Landscapes Page

Use the Landscapes page to view the status for all the landscapes (SpectroSERVERs) that the OneClick server is currently monitoring. You can identify information related to a distributed SpectroSERVER (DSS) setup, including any parent and child landscapes. You can perform a manual synchronization between all distributed models with their corresponding models on the master landscape using the Sync With Master button.

You can manually add or remove landscapes monitored by this OneClick server. You can remove only landscapes that you have manually added.

LDAP Configuration Page

Use the LDAP Configuration page to configure the OneClick web server to use an external LDAP server for user authentication.

This administration page includes the following settings and functionality:

LDAP Server Settings

Server settings to identify a primary and secondary LDAP server by IP address and port number, use SSL, add an SSL certificate, and specify timeout values when attempting to connect to or query the LDAP server.

Save LDAP Passwords to CA Spectrum Database

Lets you give access to OneClick users if the LDAP server is down, based on their last known correct LDAP password.

User Name Lookup

Configure OneClick lookups of usernames, either as a User by Search or a User by Pattern lookup.

Test LDAP Configuration

Once you have configured the OneClick interface with an external LDAP server, lets you test the configuration.

Note: If three consecutive LDAP-based login failures occur, a critical alarm is generated on the VNM that is hosting the Location Server for the OneClick web server.

More information:

Manage User Access with LDAP Configuration (see page 71)
Name Resolution Requirements (see page 29)
SSL Certificates Page (see page 53)
Non-LDAP Users Cannot Log In (see page 121)

MySQL Password Page

OneClick has its own MySQL Server users and passwords: a basic user (OC_user) and an administrative user (OC_admin). Both are used to access the MySQL reporting database on behalf of CA Spectrum applications such as Report Manager and Service Manager, but the administrative user can also grant privileges to other users for this database. For greater security, CA Spectrum provides the MySQL Password page which lets you change the passwords of the OneClick MySQL users.

Important! Do not attempt to manually change the MySQL user passwords using a MySQL client connection. Storage of the passwords in OneClick depends on MySQL connectivity. As a result, the only safe way to change the passwords is through the OneClick MySQL Password Administration page.

The MySQL Password page contains the following settings:

Default User

Specifies the credentials for the default OneClick MySQL Server user (OC_user) that CA Spectrum uses to access the reporting database used in OneClick web applications.

Current Password

Specifies the current password for the OC_user MySQL user.

New Password

Specifies a new password for the OC_user MySQL user.

Confirm New Password

Confirms the new password for the OC_user MySQL user.

Admin User

Specifies the credentials for the administrative OneClick MySQL Server user (OC_admin) that CA Spectrum uses to access the reporting database used in OneClick web applications and grant privileges to other users for this database.

Current Password

Specifies the current password for the OC_admin MySQL user.

New Password

Specifies a new password for the OC_admin MySQL user.

Confirm New Password

Confirms the new password for the OC_admin MySQL user.

OneClick maintains the MySQL server user credentials so that it can connect to MySQL. OneClick stores this password in an encrypted form for security purposes.

More information:

Configure OneClick MySQL Server Passwords (see page 28)

NSM Configuration Page

The NSM Configuration page lets you configure OneClick for connecting to an NSM dashboard and an NSM report server. Only OneClick clients launched after you save any changes reflect the changed settings.

OneClick Client Configuration Page

OneClick uses the Java Web Start framework developed by Sun Microsystems to launch the OneClick Console from the OneClick home page in a browser. To determine how to launch the OneClick Console (for example, the location of necessary JAR files), the Java Web Start framework relies on several Java Network Launching Protocol (JNLP) configuration files for the launch parameter values.

The OneClick Client Configuration page lets you configure settings associated with the OneClick client. These settings are used by the JNLP files which are located in the directory at the following location:

```
C:\win32app\SPECTRUM\tomcat\webapps\spectrum
```

Any modifications that you make to the JNLP files are saved to custom files in the following directory:

```
$SPECROOT\custom\common\config
```

Supported JRE Versions

Specifies which versions of JRE can be installed on the client to start OneClick. If none of the specified versions are installed, the user cannot start the OneClick Console from the OneClick home page and, instead, receives an error message. Multiple JRE versions can be specified as needed. When multiple JRE versions are specified, Java Web Start processes precedence from the top of the list to the bottom of the list.

Allow new versions

Allows OneClick clients to run any JRE version beyond the specified required JRE, including both major and minor JRE releases. Please be advised, as with any custom JRE configuration, using a JRE version other than the version which is provided to you could result in undesirable application behavior.

Note: CA Spectrum supports a documented minimum JRE version level, and supports running the OneClick user interface in that minimum version, or in any later version, unless noted otherwise in the product documentation. We also test with new JRE versions as they become available and update the CA Spectrum product documentation, the online Support knowledge base, or both, if specific JRE versions are incompatible.

Java Memory Usage

The Java Memory Usage section lets you set the minimum and maximum size of the object heap for the Java Virtual Machine used by OneClick clients. For more information, see Configure OneClick Client Memory Settings (see page 25).

Minimum Client Memory Usage (megabytes)

The minimum amount of memory, in megabytes, that must be available on the client to start OneClick.

Default: 64

Maximum Client Memory Usage (megabytes)

The maximum amount of memory, in megabytes, that OneClick can use on the client.

Default: 512

OneClick Client Inactivity

Lets you configure OneClick to check clients for inactivity and time inactive clients out. This feature is disabled by default. If enabled, when timeout occurs, users can enter their username and password to continue using the OneClick client. Inactivity is determined by the absence of keyboard or mouse activity is detected for the specified amount of time.

More information:

Change Individual Privileges for a User or User Group (see page 74)

Enable Inactive OneClick Client Timeout

You can configure CA Spectrum to check OneClick clients for inactivity and time out those clients that have been inactive for a specified amount of time. This setting can enhance network security. For example, if a user leaves the OneClick client running unattended on a desktop, it times out.

Follow these steps:

1. Click Administration in the OneClick home page.

   The Administration Pages open.

2. Click OneClick Client Configuration.

   The OneClick Client Configuration page opens.

3. Complete the settings in the OneClick Client Inactivity section as needed:

   OneClick Inactivity Timeout (minutes)

   Specifies the number of minutes of inactivity to allow before timing out (logging off) a OneClick client.

   Default: 0 (Disabled)

   Applet Inactivity Timeout (minutes)

   Specifies the number of minutes of inactivity to allow before timing out (logging off) an applet.

   Default: 0 (Disabled)

   Note: If you have OneClick clients that are dedicated to network monitoring and inactivity is likely, you can remove the Inactivity Timeout privilege for a user. The user cannot receive a timeout if the timeout setting has been specified.

4. Click Save.

   Timeout of inactive OneClick clients is now enabled.

More information:

OneClick Client Configuration Page (see page 48)

Performance Center Integration Configuration Page

The Performance Center Integration Configuration page lets you configure event sharing between CA Spectrum and CA Performance Center.

The Performance Center Integration Configuration page contains the following settings:

Event Polling Interval

Specifies how frequently CA Spectrum queries the Performance Center Event Manager component for events. If you modify this value, the new polling interval takes effect at the next polling cycle.

Default: 60 seconds

Event Polling

Enables or disables event polling.

Note: For more information, see the *CA Spectrum and CA Performance Center Integration Guide*.

Service Desk Configuration Page

You can view, configure, test, and save CA Spectrum and CA Service Desk Manager integration settings using the Service Desk Configuration administration page.

Note: Before configuring OneClick to connect to CA Service Desk Manager, download and install the integration components on your CA Service Desk Manager server.

You can create and modify CA Service Desk Manager server and admin user parameters, enable and disable the CA Spectrum and CA Service Desk Manager integration, and add and remove CA Spectrum alarms that generate CA Service Desk tickets.

Single Sign-On Configuration Page

The Single Sign-On Configuration page lets you enable and select a Single Sign-On option for CA Spectrum. CA Spectrum supports Single Sign-On using CA Embedded Entitlements Manager (CA EEM) or CA SiteMinder®.

When you save changes to these configuration settings, the OneClick server is automatically restarted in order to apply the changes. If you encounter errors during the restart, see Start and Stop the OneClick Web Server from an Administration Web Page (see page 22) for troubleshooting tips.

CA Spectrum Configuration Page

You can view and set the following CA Spectrum configuration parameters:

- Main Location Server Name
- Backup Location Server Name
- Admin User Name
- SpectroSERVER Polling Interval (sec)
- SpectroSERVER Request Timeout (sec)
- The properties of the object request broker (ORB) used by the OneClick web server for CORBA-based communication with the SpectroSERVER

Note: You can also restart the OneClick server so that any modifications that require a restart can take effect. If you encounter errors during the restart, see Start and Stop the OneClick Web Server from an Administration Web Page (see page 22) for troubleshooting information.

For more information about the implementation of Common Object Request Broker Architecture (CORBA) in CA Spectrum, see the *Development API Reference Guide*.

SPM Data Export Page

The SPM Data Export page lets you change the following settings for SPM (Service Performance Manager) Data Export:

SPM Data Export Enabled

Specifies whether SPM Data Export is enabled or disabled. You must enable it to modify all the other settings.

Log File Cycle Time (min)

Specifies when (in minutes) the SPM log file is saved and closed, and a new file is opened for logging.

Log File Directory

Sets the full path to the directory where SPM log files are stored. The directory structure specified must be created prior to saving.

Landscape Filter

Specifies which landscapes SPM data is obtained from.

Restart OneClick Server

Restarts the OneClick server so that any setting changes that require a server restart can take effect.

More information:

Start and Stop the OneClick Web Server from an Administration Page (see page 22)
Configure Service Performance Manager (SPM) Data Export Parameters in OneClick (see page 85)

SPM Template Naming Page

This page allows you to specify the naming convention for tests created on test hosts that have had a SPM test template applied to them:

IP Address

The test name consists of the template name and the IP address of the test target, which may be the test host or a particular device.

Model Name

The test name consists of the template name and the model name of the test target, which may be the test host or a particular device.

Note: For information about working with SPM test templates, see the *Service Performance Manager User Guide*.

SSL Certificates Page

You can use the SSL Certificates page to view and add SSL certificates used by the OneClick web server.

File with Certificate

Uploads the new key certificate you want the OneClick web server to use.

Alias Name

Specifies a short name for the certificate. This name should be consistent with some of the other commands that may need to be used with it. For example: “ldap” when setting up ldap; “ssl” or “tomcat” when setting up web server SSL.

Note: For LDAP configuration information, see LDAP Configuration (see page 45). For OneClick SSL configuration, see Name Resolution Requirements (see page 29).

Overwrite

Specifies whether to overwrite an existing certificate with this new certificate. To overwrite an existing certificate, you must load the new certificate with the same alias name of the existing certificate.

Yes

Overwrites the existing certificate.

No

Does *not* overwrite the existing certificate.

List

Opens a list of certificates already added to the keystore. Certificates are listed by alias name.

Save

Saves your changes and prompts you to restart the OneClick web server.

Watch Reports

The Watch Reports page lets you generate reports about multiple watches. A *watch* is a mechanism for adding thresholds for model attributes. Watches let you monitor network elements, such as routers, with a high level of detail. They also provide current data that can be used with other CA Spectrum tools in network analysis.

Note: For more information, see the *Watches User Guide*.

Web Server Logs Configuration Page

You can use the Web Server Logs Configuration page to view and set OneClick server log file rotation settings. The OneClick web server log files are located in the <$SPECROOT>/tomcat/logs directory.

You can set an alarm notification when the log file directory becomes larger than a specified size in megabytes. You can view the current size of the log file directory. You can specify the age in days at which a log file is deleted from the directory.

Web Server Memory Page

You can use the Web Server Memory page to view and set the maximum amount of memory the OneClick server uses. Any changes you make require you to restart the OneClick server. You can also view the percentage of the maximum memory allocation the OneClick server is currently using.

Note: You can also restart the OneClick server so that any modifications that require a restart can take effect. If you encounter errors during the restart, see Start and Stop the OneClick Web Server from an Administration Web Page (see page 22) for troubleshooting information.

More information:

Configure OneClick Web Server Memory Settings (see page 26)

Chapter 5: User Administration in OneClick

This section contains the following topics:

About OneClick User Administration

User administration involves creating and managing OneClick user accounts. As the OneClick system administrator, you must create a user account for each new user you want to access the system.

As you create new user accounts in OneClick, you can add them within user groups or as stand-alone users. When you have multiple users with similar needs, consider creating user groups to manage their user accounts. When you have users with unique needs, you may want to create user accounts independent of user groups.

Best Practices for Creating and Managing User Accounts

This section describes some best practices for creating and managing user accounts in OneClick.

Important! OneClick includes a default Administrator user with full privileges. This user is the Installation Owner account that you created during SpectroSERVER installation. You cannot delete this user from the Users tab. However, you can delete this account from the Results list that is displayed after a search using the Locater tab. You can also delete this user by removing the landscape of the main location server from the user account. *Do not remove this default Administrator user. Deleting this user produces undesirable results, such as preventing access to OneClick for all other users*.

The benefits of creating and managing individual user accounts include:

- Simplest method
- Best for environments with a small number of users

- Best for users with unique OneClick access requirements
- Individual user accounts can be moved to a user group later if needed

Creating and Managing User Accounts Within a User Group

The benefits of creating and managing user accounts within user groups include:

- Best for environments with a large number of users. Lets you group multiple users by geographic area, function, department, and so on.
- Ability to grant all users within a group the same access and privileges at one time. You can define a minimum set of privileges that all users within the group should have. Then, you can customize the individual privileges of any user in the group.

Consider the following example of creating a user group:

Task:

Within OneClick, you want to grant network operators one set of minimal privileges that enable them to monitor the network. You also want to grant one of these network operators the additional privilege of modeling the network in OneClick.

Solution:

By creating one user group you can easily satisfy this requirement. To configure this requirement in OneClick, you would do the following:

1. Create one user group and place all the user accounts for the network operators in the user group.
2. Grant everyone in the group minimal monitoring privileges.
3. Grant only the one network operator in the group the modeling privilege.

Who Can Perform User Administration?

The OneClick administrator must configure user administration in OneClick. Initially, this configuration must be performed by the user who installed CA Spectrum (the Installation Owner user). During the installation, CA Spectrum creates a user account for the Installation Owner. Using this account, this initial user has administrative access to all OneClick features, including user management.

If you are not the initial user but are responsible for user administration, the Installation Owner user must create an administrator account for you. Your account must include an Administrator license and the appropriate user management privileges.

Licenses and Privileges

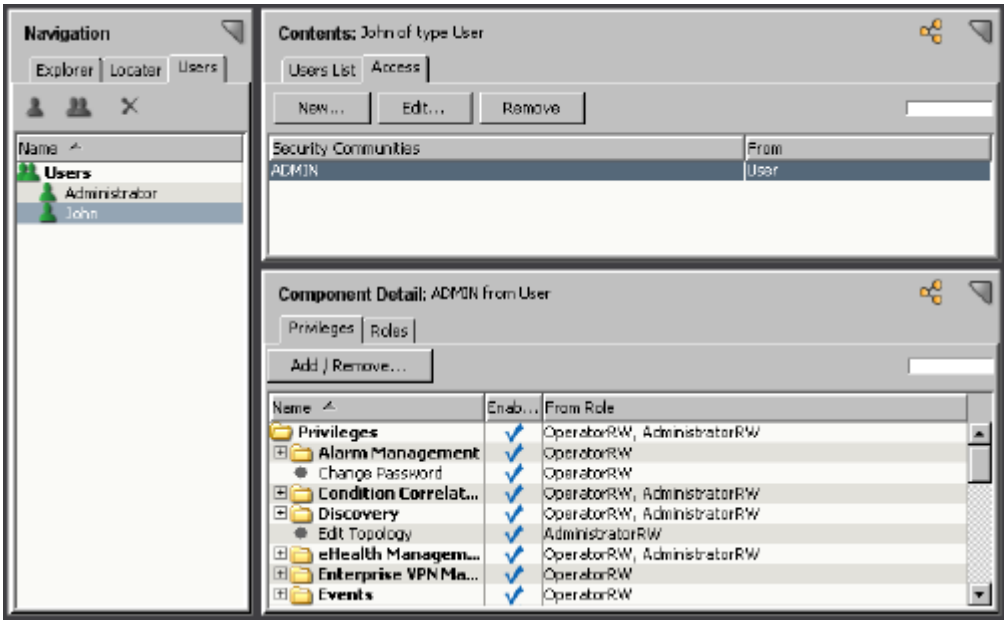
OneClick includes a set of Administrator licenses and Operator licenses. These licenses determine the privileges that a system administrator can assign to a OneClick user. The privileges that are available with a given license are enabled by default. As the system administrator, you can choose to leave these privileges enabled or you can individually disable them, customizing license privileges.

More information:

Create User Accounts and User Groups (see page 65)
Manage OneClick Licenses by Limiting Concurrent User Logins (see page 82)

OneClick User Administration Interface

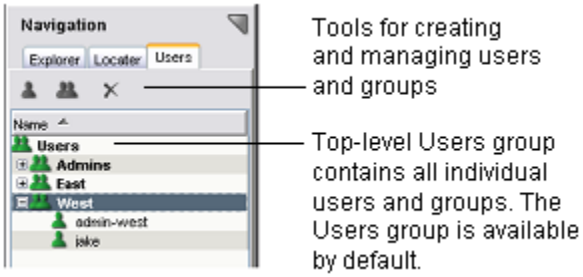
As the OneClick system administrator, you create and manage users within OneClick using options available from the Users tab, as shown in the following image.



Users Tab

The Users tab displays a hierarchical list of users and user groups under the top-level Users group. Initially, after installing CA Spectrum, the Users tab lists only the top-level Users group and the initial CA Spectrum user who installed CA Spectrum (the Installation Owner user) under the Users group.

From the Users tab, you can create and manage user accounts using the tools on the toolbar above the list of users and user groups.



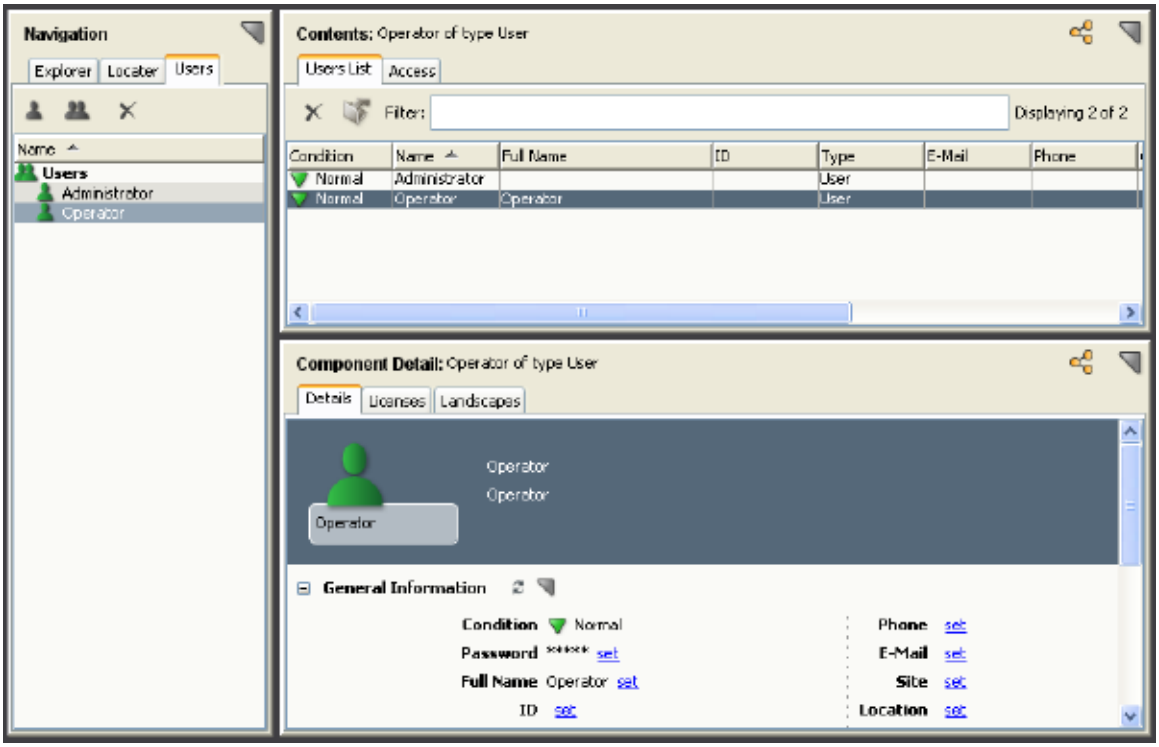
To manage an existing user or user group in OneClick, select it on the Users tab of the Navigation panel. When you select a user or user group on the Users tab, the Users List and Access tabs appear in the Contents panel.

Users List Tab

The Users List tab displays a list of users and user groups for the current landscape along with information about each entry displayed in columns. You can customize this table view by selecting the columns display and by changing the sort order of the table based on the content of a column.

Note: See the *Operator Guide* for more information about customizing table views.

When you select the Users List tab, the Details, Licenses, and Landscapes tabs appear in the Component Detail panel, as shown in the following image.



Details tab

Lets you view information about the selected user or group in the Details tab of the Component Detail panel.

The following subviews are available for both users and user groups:

General Information

Specifies general information for the selected user or group. Values for certain attributes such as contact information can be set by clicking a ‘set’ link and entering a new value.

Advanced

Specifies the following attributes, used for troubleshooting issues with distributed models:

Master Model Handle

Specifies the model on the master (or root) landscape that maintains the master copy and is responsible for distributing changes.

Home Model Handle

Exists on the landscape that is designated as the home. The master model is typically the home except if the master model was not explicitly created, in which case, a 'hidden' model is implicitly created on the master landscape and one of the other landscapes is designated as the home. The home is not used for distribution but is maintained for legacy purposes.

Duplicate Model Handle List

Contains the models from all other landscapes, excluding the home, on which this distributed model exists.

Synchronize Now

Synchronizes all the distributed models with the master. In general this will be done automatically but is provided as a button in case it needs to be done manually.

The following subview is only available when a group is selected:

User Inherited Attributes

Specifies the attributes that users will inherit from the selected group.

The following subview is only available when a user is selected:

LDAP Configuration

Specifies whether OneClick users can log in locally if they are not present in the LDAP directory.

Note: Super users with passwords set in OneClick can log in locally regardless of this setting.

Licenses tab

Lets you view and edit licenses for the selected user or group.

Landscapes tab

Lets you view and edit landscape membership for the selected user or group.

From the Users List tab, you can also do the following:

- Delete the selected user or group.
- Export the Users List tab.

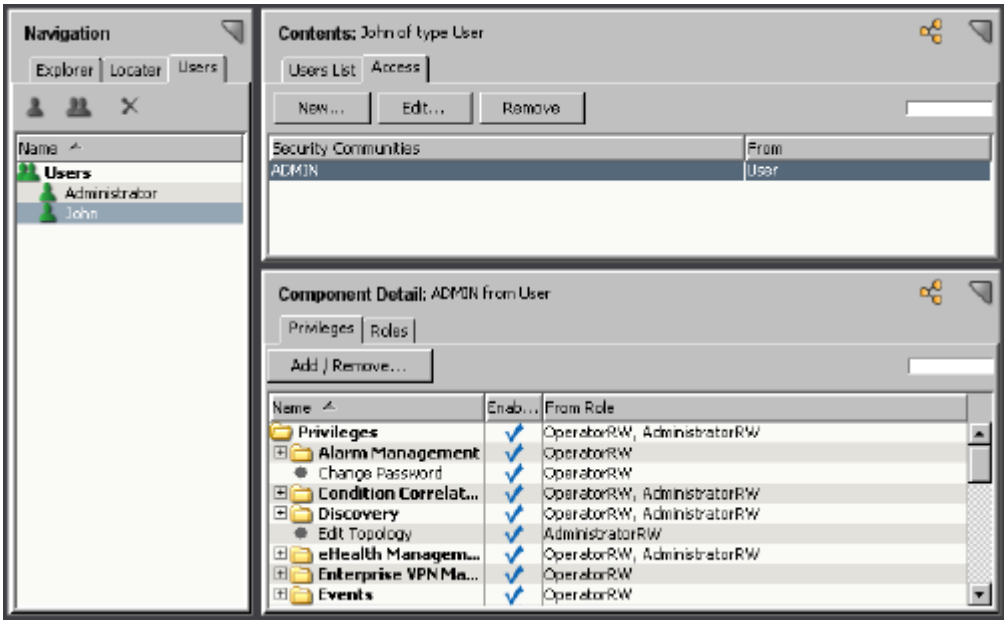
More information:

Manage User Access with LDAP Configuration (see page 71)
Delete Users or User Groups (see page 77)
Specify Inherited Attributes (see page 64)

Access Tab

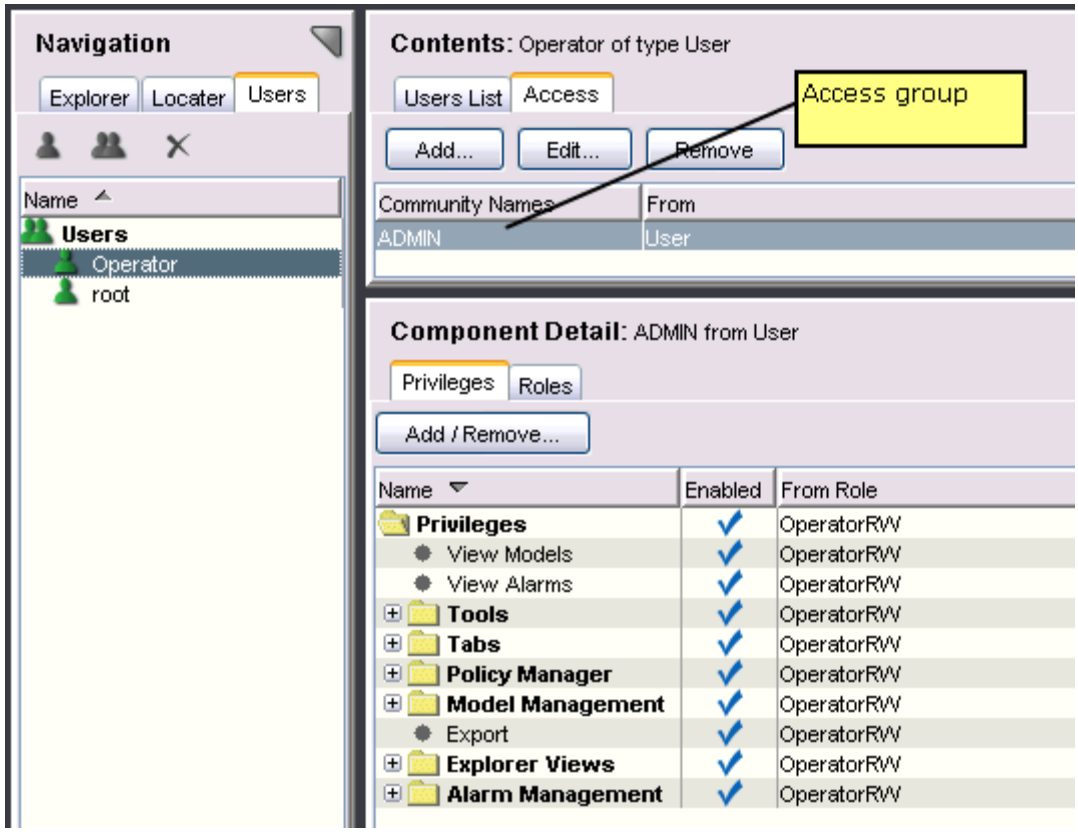
The Access tab in the Contents panel displays the list of security communities assigned to the selected user or user group. Security communities are a tool you can use to limit user access to specific sets of models and views in OneClick. The source of each assigned security community is displayed either from an individual user or a user group.

When you select the Access tab, the Privileges and Roles tabs appear in the Component Detail panel, as shown in the following image.



View and Change Privileges

Access groups appear on the Access tab for a selected user as shown in the following image.



With an access group selected for a user, the available privileges appear in the Privileges tab of the Component Detail panel.

The example Component Detail label shows that these privileges are associated with the selected ADMIN access group at the user level (ADMIN from User). A checkmark is displayed in the Enabled column for each privilege granted to this user. The From Role column shows that all of these enabled privileges are being granted by the OperatorRW role.

Clicking Add/Remove lets you enable and disable privileges for this user at the selected ADMIN access group. You cannot use Add/Remove at the user level to manage privileges for an access group that is inherited from a user group.

Effects of Customizing Privileges

In OneClick you can customize the privileges assigned to an individual user account and/or a user group. When you edit privileges for an individual user account, the changes only affect that user. When you edit the privileges assigned to a user group, the change affects all users within that user group. Users within a group automatically inherit privileges from the group but also retain all assigned individual-level privileges.

You can add privileges to an access group at the user level for users that are members of a group. You can also edit privileges for an access group at the user group level. You cannot remove privileges at the user level that are granted to the user by a user group.

Effects of Removing Privileges Granted by a Role for a User

When you customize the privileges granted by a role for a user, the user is removed from the role. The user retains any privileges granted by the role that are not removed. The role itself does not change. If the privilege is added back for the user, the user does not regain membership in the role.

Customizing the privileges granted by one of the default CA Spectrum roles (such as AdministratorRW or OperatorRW) for a user—which also results in the removal of the role from the user and the direct assignment of the remaining, enabled privileges—has additional consequences:

- If you later create a custom privilege for the default role, which is an assignment specified in the XML file that defines the privilege, the privilege is not automatically granted to the user.
- If you later upgrade CA Spectrum, any new privileges available in the newer version of CA Spectrum that are associated with the default role are not automatically granted to the user.

In either situation, to grant the custom or new privileges to the user, you must either explicitly add them to the user or reassign the default role to the user.

Manage Users Within User Groups

An excellent way to manage multiple users in OneClick is with user groups. After you have created a user group, you can configure it to provide a minimum set of user privileges for all users within that user group. Each user account you place within this group automatically inherits the group-level privileges.

Inheritance Details for Users in User Groups

Users within a user group inherit the following values from the user group:

- Security community
- Legacy SNMP community string
- Access groups
- Privilege roles
- Attributes specified by the administrator

The following special considerations apply to users contained within user groups:

- Any changes made at the group level are automatically inherited by users within the group.
- Membership in CA Spectrum landscapes is not inherited from the user group. This must be set at the individual user level.

More information:

Specify Inherited Attributes (see page 64)

Specify Inherited Attributes

You can specify the attributes that you want users to inherit from the groups to which they belong.

Follow these steps:

1. Click the Users tab in the Navigation panel.

   The Users List opens in the Contents panel.

2. Select the group containing the users whose inherited attributes you want to specify.

   The Details tab displays the User Inherited Attributes subview.

3. Expand the User Inherited Attributes subview.

   The list of attributes currently applied to users in this group is displayed.

4. Click  (Edit the Common Attributes).

   The Common Attributes Editor opens.

5. Double-click the attributes in the Available Attributes list that you want users to inherit.

   The attributes are moved to the Selected Attributes list.

6. Click Save.

   The Common Attributes Editor closes and the selected attributes appear in the User Inherited Attributes list; users in this group will now inherit the values of these attributes.

Create User Accounts and User Groups

When you create a new user or user group, OneClick assigns an Operator license and the OperatorRW privilege role to the new user or user group by default. When you create a new user or group you can choose to assign an Administrator license in addition to the Operator license. When you assign an Administrator license to users or groups, the users automatically inherit all of the privileges associated with both the OperatorRW and the AdministratorRW privilege roles.

To start administering user accounts in OneClick, create users with OneClick default settings. When you create a user or a user group, OneClick assigns an Operator license and the ADMIN security community by default. You can selectively replace the ADMIN security community by modifying users to give them access only to the devices and containers that they manage.

By default, no security is applied to models. To restrict access to a model, add a security string to that model. You can create administrators by adding the ADMIN security string to a universe model and verifying that the appropriate users have access to the ADMIN security community.

Create a new user account or user group using the default privileges that the operator or administrator license provides.

Follow these steps:

1. In the Users tab of the Navigation panel, take *one* of the following steps:

   - **Create a stand-alone user.** Select the top-level Users node and click the Create New User button.

     The Create User dialog opens.

   - **Create a user group.** Select the top-level Users node and click the Create New User Group button.

     The Create Group dialog opens.

   - **Create a user within a group.** Select an existing user group in which you want to create a user and click the Create New User button.

     The Create User dialog opens.

2. Specify the appropriate user information for the user or user group.

   Name

   Specifies the user name for the new user or group. For OneClick users that are present in the configured LDAP directory, this name must match the LDAP user logon name of the user.

   Full Name (Create User only)

   Specifies the full name of the user.

   Web Password (Create User only)

   Specifies a web password for this user. This password is used by OneClick to authenticate this user. For OneClick users that are present in the configured LDAP directory, this password is not used.

   Confirm Web Password (Create User only)

   Confirms the web password you entered when you enter it again in this field.

3. In the Licenses tab, select the licenses that you want to assign to this user or group in the appropriate Member Of check box. By default, new users receive an Operator license and the OperatorRW privilege role.

4. Click the Landscapes tab to configure landscapes for this user or group.

   Note: By default, all available landscapes are selected. In a distributed environment, you can choose additional landscapes in which you want this user to be present. At least one landscape must be selected.

5. Click the Access tab to edit the default model security setting for this user or group.

   At least one security community, such as the default ADMIN community, must be specified here. By default, the user or user group receives the read/write ADMIN access group, which gives them access to all models.

6. (Optional) Create additional access groups for the user.

   Note: Models have blank security strings by default. We recommend adding security strings to individual models or containers and using the corresponding security communities to selectively grant user access to models.

7. Click OK in the Create User or Create Group dialog.

   The new user or group is created and displayed in the Users tab of the Navigation panel.

About Creating, Editing, and Assigning Roles and Privileges

You can individually disable and enable privileges for a user or user group. You can also use roles to grant a set of privileges to a user or user group. You can use the default privilege roles in OneClick, or you can create your own custom privilege roles; however, you cannot edit the default privilege roles themselves. After users are assigned a license category, they can have access privileges provided by the predefined roles.

There are six default roles:

AdministratorRW

(Read/write) Grants privileges required to set up CA Spectrum and its users, as well as perform all network management tasks. This is the least restrictive role. Some examples include the ability to perform device discovery, model management, topology configuration, eHealth integration management, device certification, and user configuration.

AdministratorRO

(Read-only) Grants privileges required to access CA Spectrum modeling and attribute information. Some examples include the ability to view SNMP community strings and SNMPv3 security profiles.

OperatorRW

(Read/write) Grants privileges required to perform most typical tasks for network management using CA Spectrum. Some examples include alarm management tasks, Service Performance Manager tasks, and most Network Configuration Manager tasks.

OperatorRO

(Read-only) Grants privileges that allow the user to monitor network activity and perform limited network management tasks. Some examples include the ability to snooze alarms and to view topology information.

Service ManagerRW

(Read/write) Grants privileges that allow access to the Service dashboard, as well as the ability to edit Service Outages.

Service ManagerRO

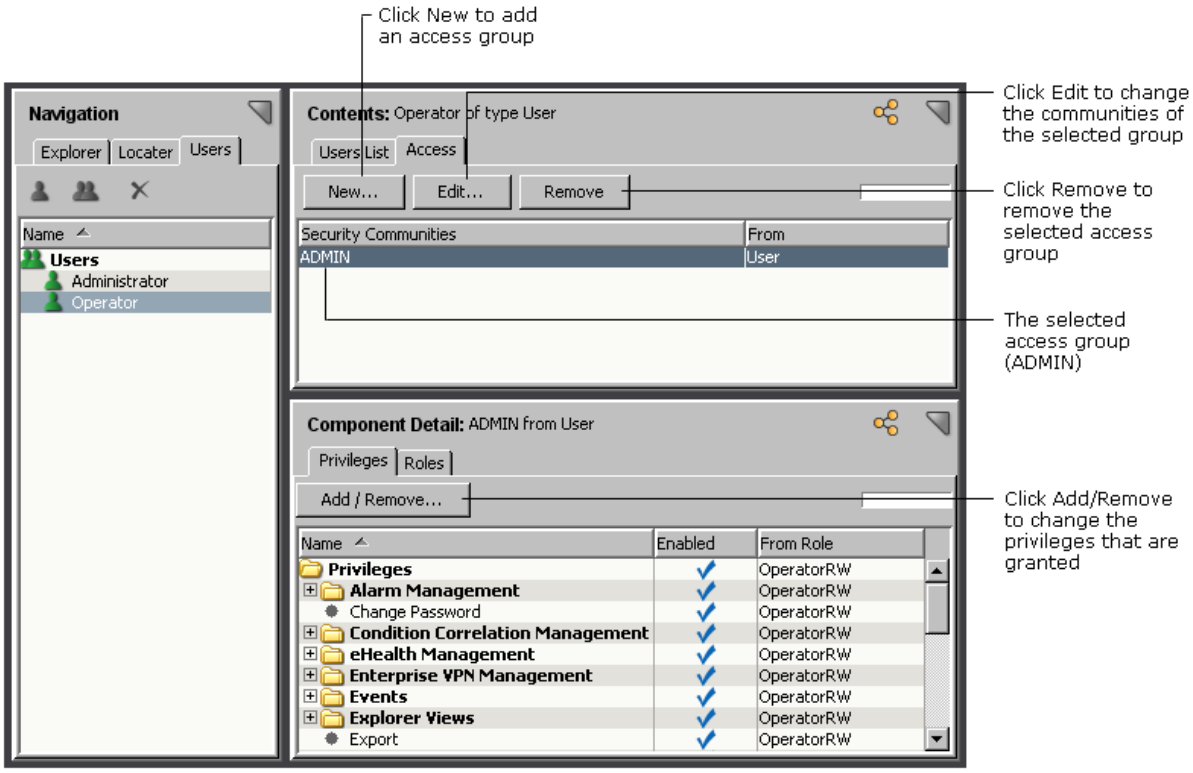
(Read-only) Grants privileges that allow access to the Service dashboard.

If these predefined roles do not meet your requirements, you can create custom roles. Although you cannot modify the predefined roles, you can modify individual privileges.

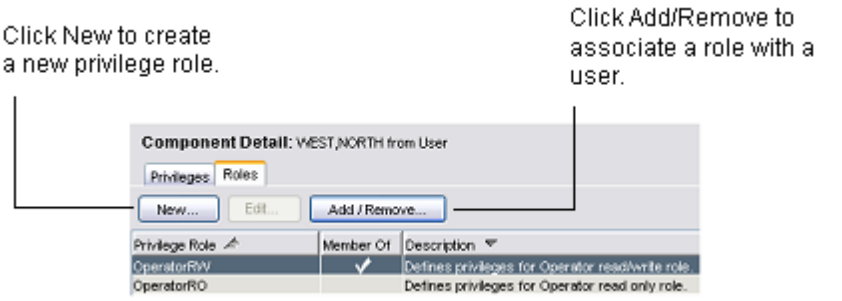
Note: When you upgrade to a newer version of CA Spectrum, any new privileges available in the newer version are automatically added to the appropriate default roles. However, you will need to explicitly add them to any custom roles you may have created, as applicable.

When you edit privileges for an individual user, the changes only affect that user. When you edit the privileges granted by a user group, the changes affect all of the users within that user group. Users within a user group inherit privileges from the group level.

To edit privileges and roles, you modify settings in the Privileges tab and/or the Roles tab for a selected user, as shown in the following image.



In addition to editing individual privileges, you can also grant multiple privileges at one time by assigning a privilege role using the Roles tab, as shown in the following figure.



The default roles included with OneClick and the custom roles that you create are reusable and can be assigned to one or more users. The OperatorRW privilege role automatically grants the privileges provided with the Operator license.

Create and Assign Roles to Users or User Groups

You can create a custom privilege role and then associate it with a user or group. The role has no effect until it is associated with a user account or user group.

You can create a custom privilege role.

Follow these steps:

1. Select a user in the Users tab of the Navigation panel.

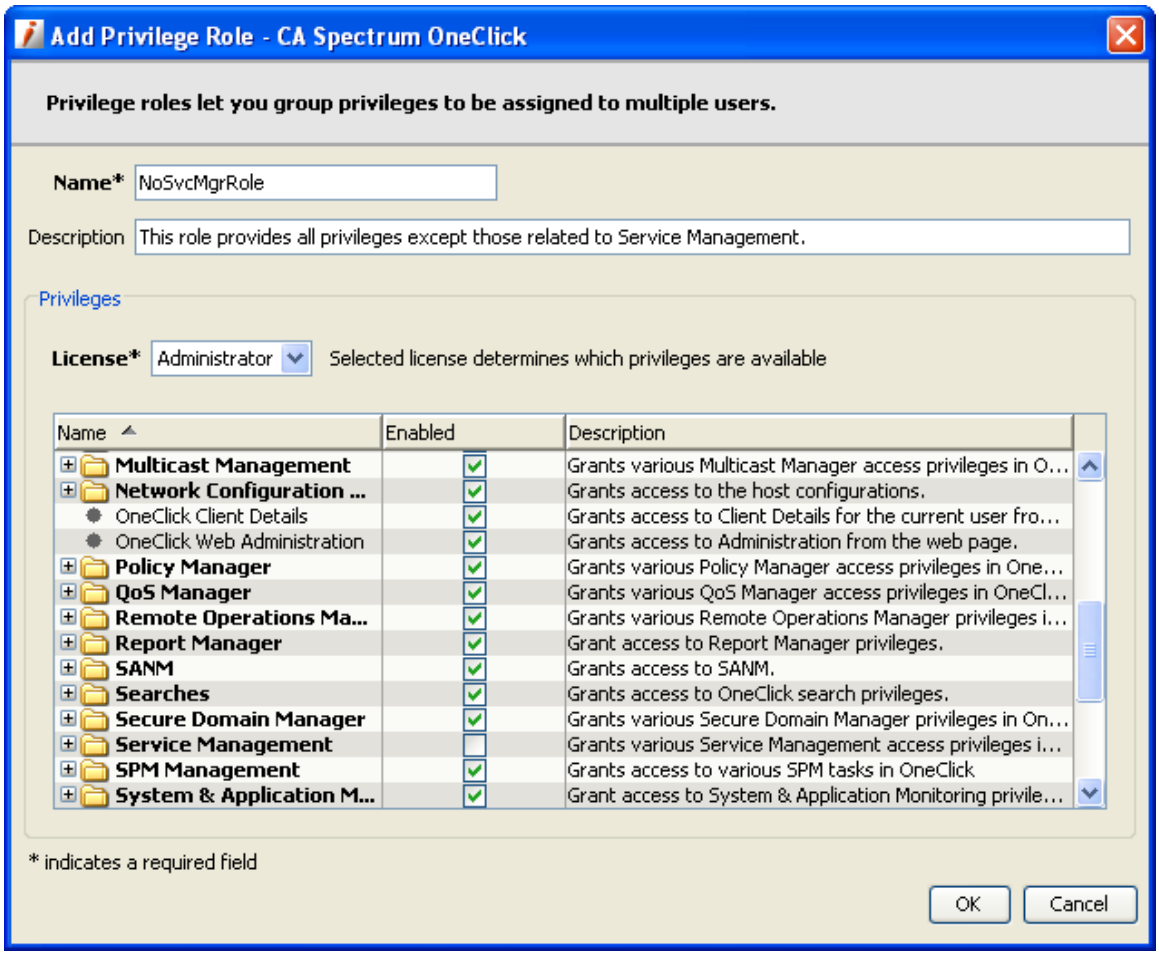
   Note: To create an Administrator-licensed privilege role, select a user with the Administrator license. To create a privilege role based on the Operator license, select a user with the Operator license.

2. Click the Access tab in the Contents panel.

   The Privileges and Roles tabs appear in the Component Detail panel.

3. Click the Roles tab, and click New.

   The Add Privilege Role dialog opens.



4. Type a descriptive name for the new role in the Name field.
5. (Optional) Type a full description of this role in the Description field.
6. Select the appropriate license from the License drop-down list.

   Note: The license chosen here determines the privileges that can be enabled with this role.
7. Select the privileges you want this role to grant by selecting or clearing the Enabled check boxes.
8. Click OK.

   The new role appears as an option in the Roles tab of the Component Detail panel. This role is now ready to be used with any user or user group that has the appropriate license.

You can also assign a privilege role. Assigning a privilege role lets you assign an existing role to a user.

Follow these steps:

1. Select the user you want to apply the role to in the Users tab of the Navigation panel.
2. Click the Access tab and select an access group.

   The Privileges and Roles tabs appear in the Component Detail panel.
3. Click the Roles tab and click the Add/Remove button.

   The Assign Roles dialog opens.

   Note: For users in a group, this step must be done at the group level. Assigning a role at the group level affects all users in the group.
4. Move the role you want to assign to the Exists in/Create in column using the arrow buttons.
5. Click OK.

   The role is automatically assigned to the access group selected in Step 2.

Create a Super User

As the OneClick administrator, you can easily grant all possible privileges and access to a user. A *super user* in CA Spectrum has all available CA Spectrum license roles, privileges, and access in OneClick. Because access groups and privilege roles do not apply to super users, the Access tab is disabled when a user designated as super user is selected in OneClick.

When you install CA Spectrum, the initial CA Spectrum user that is created is a super user. This initial user (also referred to as the Installation Owner user) remains a super user and must always exist in CA Spectrum. The existence of this account is verified each time the SpectroSERVER starts. The value for the initial_user_model_name setting in the *$SPECROOT*/SS/.vnmrc file stores the setting for the initial CA Spectrum super user. The default password for the initial user is ‘spectrum’.

Note: Consider creating an administrator user with user management privileges to manage users. This user is in addition to the user that installed OneClick (the initial user) and can even manage the initial user account. To ensure that a OneClick administrator has all possible privileges, set the value of 'Is Super User' for that administrator (user) to *true*.

Follow these steps:

1. Select a user from the Users List in the Contents panel.

   The Details tab displays information about the user account.
2. Click set in the 'Is Super User' field, and select Yes from the list.
3. Press Enter.

   The user account is now a super user.

Manage User Access with LDAP Configuration

For environments where LDAP is used for authentication, you can allow or restrict local logins from OneClick users who are not present in the LDAP directory. For example, non-LDAP users, such as non-employees who provide support, training, or troubleshooting with no access to LDAP, require log-in access to OneClick.

Note: Super users with passwords set in OneClick can log in locally, regardless of this setting.

Follow these steps:

1. Select the user or user group to edit in the Users tab of the Navigation panel.
2. Navigate to the Details tab of the Component Detail panel for that user or user group.

3. Expand the LDAP Configuration subview.
4. Set the option to 'Allow User to Log In if either the LDAP Password is Invalid or the User does not exist in LDAP' to Yes.

   Note: For security reasons, we recommend saving the LDAP user password to the CA Spectrum database. If the option to 'Allow User to Log In if either the LDAP Password is Invalid or the User does not exist in LDAP' is enabled, you can use the LDAP password for user authentication against the CA Spectrum database.

   Non-LDAP users can log in to OneClick even when they are not present in the designated LDAP directory. Setting this option to No prevents the user from logging in without an LDAP account.

   Important! If LDAP is configured to search for User by Pattern and no match is found during lookup, your attempt to log in fails. In such cases, verify that LDAP is configured to authenticate User by Search.

More information:

LDAP Configuration Page (see page 45)
Non-LDAP Users Cannot Log In (see page 121)

Change Details Displayed for a User or User Group

You can modify user or group attributes from the Component Detail panel.

Follow these steps:

1. Select the user or user group to edit in the Users tab of the Navigation panel.
2. Navigate to the Details tab of the Component Detail panel for that user or group.
3. Use the 'set' link to edit attributes such as the password and security string of an existing user or group.

Change the Licenses of a User or Group

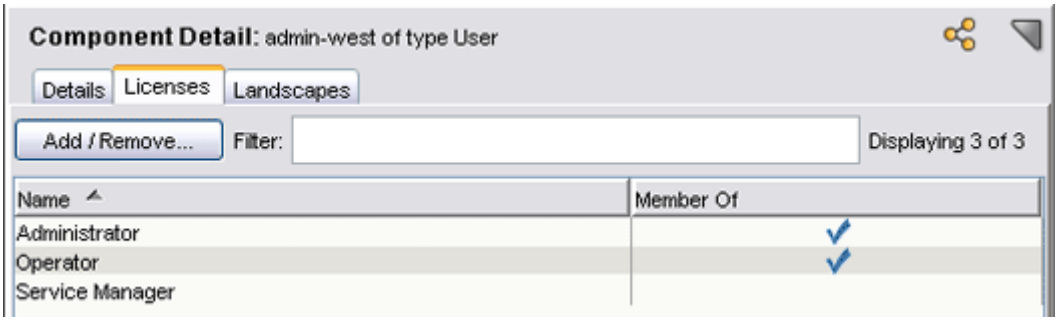
The default settings for a new user account include an Operator license that offers operator privileges. To perform administrative tasks such as user management, discovery, and modeling in OneClick, users must have administrator privileges. The default Operator license does not provide any administrative privileges.

The Administrator license provides the privileges required to perform the following OneClick administrative tasks:

- User Management
- Collection Management

- Discovery
- Topology Editing
- Pipe Management
- Create and Destroy Models
- Search Management

If you are configuring a user account that requires administrator privileges, you must assign the account an Administrator license. You do this by clicking the Add/Remove button in the License tab of the Component Detail panel, shown in the following figure.



When a user logs in, that user consumes assigned licenses from the pool of available licenses. For example, when a user with both Operator and Administrator licenses logs in, one of each license is used.

You can change the licenses that are assigned to a user or to a user group.

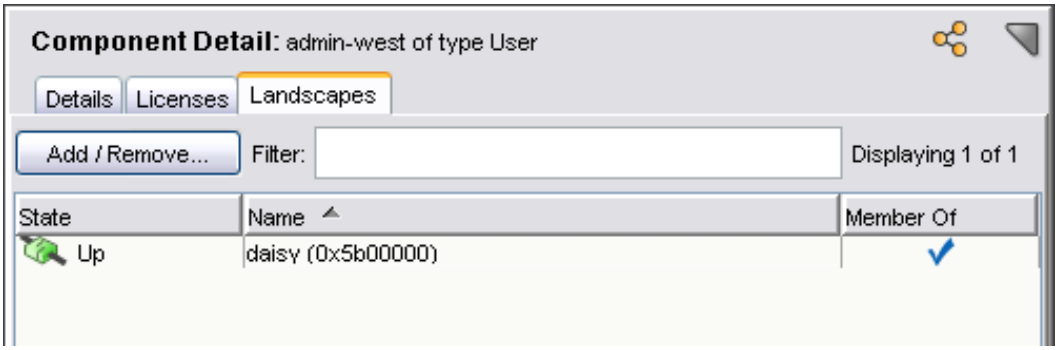
Follow these steps:

1. Select the user or user group in the Users tab of the Navigation panel.
2. Click the Licenses tab of the Component Detail panel.
3. Click the Add/Remove button to select licenses for this user or group.

Change the Landscapes for a User

In a distributed CA Spectrum environment, you can change the landscape membership of users and groups. Use the Landscapes tab of the Component Detail panel. A distributed environment has multiple SpectroSERVERs, each with its own CA Spectrum landscape. For a OneClick user to have access to an additional CA Spectrum landscape, the user must be a member of that landscape.

The following image displays the Landscapes tab for a fictitious admin-west user. This tab displays the state and name of each known CA Spectrum landscape. The check marks in the Member Of column indicate landscapes in which the user is present.



Tips

- You cannot edit membership in landscapes that are in the “down” state.
- We recommend changing user group landscape membership while the group contains no users. Add users to the group once the empty user group is a member of the desired landscapes.

Follow these steps:

1. Click the Landscapes tab of the Component Detail panel.
2. Click the Add/Remove button.
3. Choose the landscapes where you want this user or group to be present.
4. Click OK.

Change Individual Privileges for a User or User Group

User and user group privileges can be added and removed individually.

Follow these steps:

1. Navigate to the Access tab of the Contents panel for the selected user.
2. Select the access group whose privileges you want to modify.

3. Navigate to the Privileges tab of the Component Detail panel for the selected access group.
4. Click the Add/Remove button.
5. Enable or disable the privileges that you want for this access group by selecting or clearing the Enabled check box.

Locate and Review Role Usage

You can search for user roles, review whether they are in use, and determine the users or user groups that are using them. Reviewing this information is helpful if you are trying to delete a user role. You cannot delete user roles that are in use. However, you can verify whether the user is still valid. You can then remove users and groups that are no longer valid from the role and delete the role itself.

Follow these steps:

1. Click the Locater tab in the Navigation panel.
2. Expand the Roles folder and double-click All Roles.

   Note: Enter landscape information if prompted.

   The search results appear in the Contents panel. The Role In Use column indicates whether the role is currently being used. Roles that are in use have a "Yes" hyperlink.
3. (Optional) Click Yes to review the users or user groups that are using this role.

   The Role in Use dialog displays the users and user groups that are currently using this role.
4. Click Close.

   The Role in Use dialog closes.

More information:

Delete Unused User Roles (see page 76)
Unassign Roles (see page 76)

Unassign Roles

You can unassign roles from user groups and users as needed.

Follow these steps:

1. Select the user or user group whose role you want to remove in the Users tab of the Navigation panel.
2. Click the Access tab in the Contents panel, and select an access group.

   The Privileges and Roles tabs appear in the Component Detail panel.
3. Click the Roles tab, and click Add/Remove.

   The Assign Roles dialog opens.

   Note: For users in a group, this step must be performed at the group level. Unassigning a role at the group level affects all users in the group.
4. Move the role you want to unassign to the 'Does not exist in/Delete from' column using the arrow buttons.
5. Click OK.

   The role is automatically unassigned from the selected access group.

Delete Unused User Roles

You can delete user roles when they are no longer used by any users or by any user groups.

Follow these steps:

1. Locate the unused user role that you want to delete (see page 75).

   The search results appear in the Contents panel. Roles that are in use have a "Yes" hyperlink in the "Role in Use" column.
2. Select the unused role to delete.
3. Click Delete.

   The confirm delete dialog opens.
4. Click Yes.

   The user role is deleted.

Move Existing Users to User Groups

You can move existing users to user groups. However, you cannot move the user account under which you are logged in.

Follow these steps:

1. Right-click a user in the Users tab or on the Users List tab.
2. Click Move To Group.

   The Select User Group dialog opens.
3. Select the destination group, and click OK.

Remove Users from User Groups

When you remove a user from a group, the user automatically appears as an individual user. Removing users from groups causes them to lose any privileges that were inherited from the user group level.

Follow these steps:

1. In the Users tab of the Navigation panel, right-click a user.
2. Select Remove From Group.

   The user is removed from the group. This user now appears under the top-level Users group in the Users tab of the Navigation panel.

Note: After removing a user from a group, verify that the user has the desired access groups and privileges.

Delete Users or User Groups

Users and groups can be deleted from OneClick as necessary. When you delete a user group, any users contained in that group are then organized under the top-level Users node.

Important! OneClick includes a default Administrator user with full privileges. This user is the Installation Owner account that you created during SpectroSERVER installation. You cannot delete this user from the Users tab. However, you can delete this account from the Results list that is displayed after a search using the Locater tab. You can also delete this user by removing the landscape of the main location server from the user account. *Do not remove this default Administrator user. Deleting this user produces undesirable results, such as preventing access to OneClick for all other users.*

To delete a user or user group

1. Select the User or User Group for deletion in the Users tab.
2. Click  (Delete).

   The user or group is deleted.

About Using Security Communities to Manage User Access to Models and Devices

Security communities limit user access to specific sets of models and views that use the same security string. Only users with membership in a security community that matches the security string on a model can access the model. You can assign security communities to an individual user or to a user group. All users in a user group inherit the privileges of the security communities assigned to the group.

Important! By default, no security is applied to models. Until you apply security to a model, all CA Spectrum users can see it.

To limit user access to models, create a security community with the desired privileges, and assign it to specific users and user groups. Then selectively apply the security string to the models that those users manage.

Restricted View of Community Names

By default, the Operator Read Only privilege role restricts users from viewing community names. You must enable this privilege for specific Operator Read Only users as needed.

From the Access tab, Privileges tab, you can view, create, edit, and remove security community assignments from a user or user group.

Note: You cannot configure security communities for super users. If you select a user who is a super user, the Access tab is disabled.

Use Security Communities to Manage User Access to Models and Devices

You can use security communities to manage user access to data. The Users tab lets you view the currently assigned privileges for community names.

Follow these steps:

1. In the Users tab, select the user or group for which you want to view privileges to a community name.
2. Select the community name in the Security Community list in the Access tab.
3. In the Privileges tab of Component Detail panel, select Model Management, View Attributes, Community Names.

You can add or remove community names from a user's view.

Follow these steps:

1. In the Users tab, select the user or group for which you want to change community name viewing privileges.
2. In the Security Community list on the Access tab, select the community name that you want to change the user's access to.
3. Click Add/Remove in the Privileges tab in the Component Detail panel.

   The Add/Remove Privileges dialog opens.
4. Click Model Management, View Attributes, Community Names.
5. Change the existing privilege by selecting or clearing the Enabled check box.
6. Click OK.

   The change is implemented.

Or you can create a role that adds the community name privilege. You must then assign the new role to a user or group.

Follow these steps:

1. In the Navigation panel, click the Users tab, and select the user or user group to which you want to assign a security community.
2. In the Contents panel, click the Access tab.
3. Click New in the Access tab.

   The New dialog opens.
4. Enter the name of the new security community that you want to create.

   Note: Do not use spaces when naming security communities.
5. Click Add.

6. Enter any additional security communities that you want to share the same privileges.
7. Click OK.
8. (Optional) Click New again to create security communities for the selected user or user group that will not share the same privileges as the security communities you just created.

   The new security communities appear in the Access tab.

Perform the following procedure in conjunction with assigning new security communities to specific models or model types. Security communities do not provide or limit access to data in OneClick until they are assigned. You must also assign privileges or privilege roles to the security communities that you have created.

Follow these steps:

1. In the Navigation panel, click the Users tab, and select the user or user group to which you want to assign a security community.
2. In the Contents panel, click the Access tab.
3. Select the security community you want to edit.
4. Click Edit in the Access tab.

   The Edit dialog opens.
5. Do *one* of the following:
   - To add an entry to the selected security community, enter the name of the new entry in the first field, and click Add.
   - To remove an entry from the selected security community, select the entry from the list, and click Remove.
   - To modify an existing entry for the selected security community, select the entry from the list. Make modifications to the security community entry in the first field, and click Modify.
6. Click OK.

   The modifications to the selected security community appear in the Access list.

To enable the changes that you made in the preceding procedure, the modified security communities must match the security string attributes that are already applied to models. Or they must match security string attributes that you plan to apply as part of an overall device access and security policy.

You can remove a security community assignment from a user or user group.

Follow these steps:

1. In the Navigation panel, click the Users tab, and select the user or user group whose security community you want to remove.
2. In the Contents panel, click the Access tab, and then select the security community to remove.
3. Click Remove in the Access tab, and then click Yes to confirm your selection.

   The security community is removed from the Access tab for the selected user or user group. This user or user group no longer has access to the relevant models.

Manage Users From the Client Details Page

The OneClick Client Details page lets administrators perform these user management tasks:

- Send messages to logged in clients.
- Manage OneClick licenses by administratively logging off selected users.

Note: This page is not automatically updated with the latest client information. To ensure that you have the latest information, use the Reload function of your web browser to reload the page.

To view the Client Details page:

1. Navigate to http://<*webserver*>/spectrum/index.jsp in a web browser.

   The OneClick home page opens.
2. Click the Client Details link.

   The Client Details page opens, displaying a Client(s) Logged On table.

To send a message to clients using the Client Details page:

1. In the Client(s) Logged On table, select the check boxes next to the user names of the clients to whom you want to send a message, and click Send Message.

   The Enter Message dialog opens.
2. Enter a message and click Send.

   Your message is sent to the clients you selected.

To log clients off using the Client Details page:

1. In the Client(s) Logged On table, select the check boxes next to the user names of the clients that you want to log off, and click Log off Clients.

   A confirmation dialog opens.

2. Click OK.

   The clients are logged off. They receive a message indicating the administrator who logged them off.

Note: Operators can also access the Client Details page, but only to view or log off their own clients.

Manage OneClick Licenses by Limiting Concurrent User Logins

Each time a user launches a OneClick client, that client consumes one instance of each OneClick license assigned to the user. By default, OneClick users can launch unlimited clients with a single set of login credentials. As a result, a single user can consume all of the available OneClick licenses by launching clients repeatedly without exiting from other clients.

The CA Spectrum administrator can restrict the number of concurrent OneClick licenses that a user or user group can consume at one time. You can distribute the available OneClick licenses among multiple users. In addition, you can set the maximum number of logins to zero to effectively lock out a user without destroying the user account.

You can set maximum login restrictions at both the user and the user group level. The maximum login value is not inherited from the user group. The process that CA Spectrum uses to manage the different values for users and groups includes verification of the user's maximum login count. If that count has been exceeded, a message appears.Otherwise, CA Spectrum then verifies the maximum login count specified for the relevant user group. Therefore, all users in a group can log in multiple times until the maximum values are reached. The total count of all users in the group cannot exceed the group total.

By default, users or user groups can launch as many clients as there are licenses. You can modify the setting for maximum logins in the Details tab of the Component Detail panel for a selected user or user group.

To restrict users to one concurrent login:

1. Navigate to the Details tab of the Component Detail panel for a given user selected on the Users tab.
2. Click set in the Maximum Logins field.
3. Type **1** and click Save.

   This user is now restricted to one concurrent login only.

To restrict users from launching a OneClick client:

1. Navigate to the Details tab of the Component Detail panel for a given user selected on the Users tab.
2. Click set in the Maximum Logins field.
3. Type **0** and click Save.

   This user can no longer launch a OneClick client.

To let users launch an unlimited number of OneClick clients:

1. Navigate to the Details tab of the Component Detail panel for a given user in the Users tab.
2. Click set in the Maximum Logins field.
3. Click Unlimited.

Chapter 6: Configuring Additional OneClick Applications

This chapter discusses CA Spectrum add-on application administration and configuration in OneClick from the perspective of a OneClick administrator. This includes managing and configuring other CA Spectrum applications.

This section contains the following topics:

Configure Service Performance Manager (SPM) Data Export Parameters in OneClick

By default, SPM Data Export is disabled in OneClick. To configure SPM data export in OneClick, enable SPM data export logging. Set the time period when data is written to each log file. Then create and specify the directory for the output log file. At the end of the interval that you set, the file is saved, and a new file is created for incoming data. By default, when SPM data export is enabled, 60 minutes of data is captured before the SPM log file is saved and a new file is opened.

Note: By default, when SPM data export is enabled, OneClick attempts to save SPM data files to the /tmp directory. You must first create the /tmp directory or create an alternate location for the SPM log files.

Follow these steps:

1. Click Administration in the OneClick home page.

   The Administration Pages open.

2. Click SPM Data Export in the list on the left.

   The SPM Data Export Configuration page opens.

3. For SPM Data Export Enabled, click Yes.

4. For Log File Cycle Time (min), enter the elapsed time in minutes when the current SPM log file will be saved and closed and a new file opened for logging. The default value for this logging interval is 60 minutes.

5. For Log File Directory, enter the fully qualified file path for the directory where OneClick will store SPM log files.

   Note: Create the directory structure for OneClick to save the data files in. By default OneClick attempts to save the data files in /tmp which you must create first if it does not exist.

6. For Landscape Filter, specify the CA Spectrum landscapes from which OneClick exports data in a distributed environment. Use the left arrow to move the landscapes from which to export data to the Show Landscapes list. Move any landscapes from which data is not exported to the Hide Landscapes list. By default, all available landscapes are included.

7. Click Save.

   You are prompted to commit your changes and restart the OneClick web server. The OneClick web server must be restarted for the changes to take effect.

8. Click OK.

   Your changes are saved and the OneClick web server is restarted.

More information:

SPM Data Export Page (see page 52)

Display Topology Tab Contents in a Web Page

You can use a topology applet to make the contents of your Topology tab available from a web page. Specify the container-based model handle whose topology you want to view.

Note: You can determine the model handle of the container to use from the Attributes tab. For more information, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

To display Topology tab contents in a web page, type the following URL into your web browser:

```
http://<hostname>:<portnumber>/spectrum/topology.applet?mh=<model handle>
```

<model handle>

Specifies the container-based model handle that you want to view the topology of.

The portion of the Topology tab that you specified is now accessible from this web page. From here, you can drill into other containers and return to the starting point.

To display Topology tab contents within an existing web page, take one of the following steps:

- Embed the topology applet into the web page using an iframe:

```
<iframe
src="http://<hostname>:<portnumber>/spectrum/topology.applet?mh=<model
handle>" width="830" height="530"/>

    Your browser does not support embedded objects, <a
href="http://<hostname>:<portnumber>/spectrum/topology.applet?mh=<model
handle>">click here</a> to go to included content.

</iframe>
```

  Note: This method works best for Internet Explorer browsers.

- Embed the topology applet into the web page using the following syntax to avoid using iframes:

```
<div>

<object
data="http://<hostname>:<portnumber>/spectrum/topology.applet?mh=<model
handle>" type="text/html" width="830" height="530">

    Your browser does not support embedded objects, <a
href="http://<hostname>:<portnumber>/spectrum/topology.applet?mh=<model
handle>"> click here</a>to go to included content.

</object>

</div>
```

  Note: This method works best for Firefox browsers.

The portion of the Topology tab that you specified is now accessible in a web portlet. From here, you can drill into other containers and return to the starting point.

Chapter 7: Model Security in OneClick

This chapter describes model security and how to configure it in OneClick.

This section contains the following topics:

How Are Models Secured in OneClick?

Model security in OneClick lets you control user access to models. Secure a model by setting the security string on that model. By default, users can access all models.

Secure modeled network elements in OneClick using the following process:

1. Apply a security string to a modeled element that you want to secure. For example, set the security string of a LAN container model to lan1. For more information, see Using Security Strings to Secure Modeled Elements (see page 89).
2. The security string that is set on the model in Step 1 must appear in an entry on the Access tab of a given user account for that user to access that secured model. For more information, see Use Security Communities to Manage User Access to Models and Devices (see page 78).
3. To prevent a user from accessing secured models, modify the access group in the Access tab for that user. For more information, see Scenarios for Implementing Model Security (see page 93).

More information:

Using Security Strings to Secure Modeled Elements (see page 89)

Using Security Strings to Secure Modeled Elements

Set the security string on a model to prevent users without a matching entry on their Access tab from accessing the model. By default, the security string is empty.

The procedure that follows provides the basic steps to configure model security. It does the following:

- Secures a model with a security string
- Gives a user access to that secured model
- Prevents unauthorized users from accessing secured models

Note: This procedure assumes you have already modeled elements in your OneClick environment. For more information, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

Follow these steps:

1. Select the modeled element, such as a device model, that you want to secure in the Topology tab.
2. Click the Information tab in the Component Detail panel.
3. Expand the CA Spectrum Modeling Information subview, click set in the Security String field, type a security string, and press Enter.

   This model is now inaccessible for users who lack an Access tab entry with this security string.
4. To give a user access to this secured model:
   a. Select the user on the Users tab of the Navigation panel, and click the Access tab of the Contents panel.
   b. (Optional) Remove any access groups that this user no longer requires by selecting access groups and clicking Remove.

      Note: When you remove an access group from a user account, any privileges that are assigned with that access group are also removed.
   c. Click New in the Access tab of the Contents panel.

      The New access group dialog opens.
   d. Enter the security community from Step 3, and click OK.
5. Verify that this user has adequate privileges. To perform this step, assign the appropriate privileges to the access group that you added:
   a. Select the access group.
   b. In the Privileges or Roles tab for the selected access group, assign the privileges you want this user to have for this security community. For example, in the case of an operator user, you might assign the OperatorRW privilege role using the Roles tab.

   When this user logs on, models that have a security string that matches the access group entry that you added and all unsecured models appear on the Topology tab. This user also sees any container models that contain models that are accessible to this user account.

More information:

Create and Assign Roles to Users or User Groups (see page 69)

How to Customize Security String Inheritance

Use the following process to customize security string inheritance:

1. Add relations for security string roll down (see page 91).
2. Define security string roll down overrides for model types (see page 92).

Relations for Security String Roll Down

CA Spectrum will roll security strings down from the left model to the right model, from the following relations:

- Application
- Can_Assign
- CollectsChassis
- Collects
- Contains
- HASPART
- Manages
- Organizes
- Owns
- Provides

Note: For specific details about how to use the Model Type Editor to create new model types, see the *Model Type Editor User Guide*.

To add new relations that security strings will roll down

1. Stop the SpectroSERVER if it is running, and verify that there are no other programs running that can access the SpectroSERVER database.
2. Open the CA Spectrum Control Panel, and click Configure, Model Type Editor.

   The Model Type Editor opens, and the Root model type is set as the current model type. The Root model type is the model type at the highest point in the model type hierarchy.
3. In the Model Type View, find the Security_Model model type.

4. Create a new model type, whose base model type is Security_Model.
5. In the newly created model type, add new attributes of type Relation Handle.
6. Set the default value of each new attribute to the Relation Handle of the relation that you want security strings to roll down.

Define Security String Roll Down Overrides for Model Types

When joining the security strings of two models for a security string roll down, the AND operator is used by default, unless the model type on the right side of the association has a predefined override.

CA Spectrum provides an override for the Container model type. When rolling down a security string to a model on the right side of a security relation whose model type is derived from Container, the OR operator is used. The only exception to this override is the WA_Link model type, which is derived from the Container model type. When rolling down a security string to a model on the right side of a security relation whose model type is WA_LINK, the AND operator is used.

Define security string roll down overrides in the Model Type Editor.

Note: For specific details about how to use the Model Type Editor and create new model types, see the *Model Type Editor User Guide*.

Follow these steps:

1. Stop the SpectroSERVER if it is running, and verify that there are no other programs running that can access the SpectroSERVER database.
2. Open the CA Spectrum Control Panel, and click Configure, Model Type Editor.

   The Model Type Editor opens, and the Root model type is set as the current model type. The Root model type is the model type at the highest point in the model type hierarchy.
3. In the Model Type View, find the Security_Model model type.
4. Create a new model type, whose base model type is Security_Model.

   Important! Create a new model type rather than modify the Security_Model model type directly since changes to the Security_Model type could be overwritten when installing future CA Spectrum upgrades.

5. In the newly created model type, take the following steps:
    a. Modify the default value of the Security_String_Mtypes (0x12967) attribute, adding the model types for which you want to define an override.
    b. Modify the default value of the Security_String_Operators (0x12968) attribute, defining the override operators (0 maps to AND, 1 maps to OR) for the model types that were added to the Security_String_Mtypes attribute. The value of instance x in the Security_String_Operators attribute should be the override operator for the model type identified by the value of instance x of the Security_String_Mtypes attribute.
6. Save your changes and close the Model Type Editor.

Note: Overrides that are defined on model types that are derived from the Security_Model model type take precedence over any overrides that are defined directly on the Security_Model model type.

Model Security Scenarios

The following scenarios provide examples of both simple and more complex model security use cases.

Secure a model in a remote office from local users

To help you understand security strings in OneClick, a simple example follows:

You want to secure a single model in a remote office so that local OneClick users cannot access it. Setting the security string of the model (to “remote,” for example) would secure it. Non-administrator users who lacked an access group with an entry of "remote" would not be able to access that model. Users with only an access group entry of "local", for example, would not have access to this model.

Secure administrative access to a branch office network

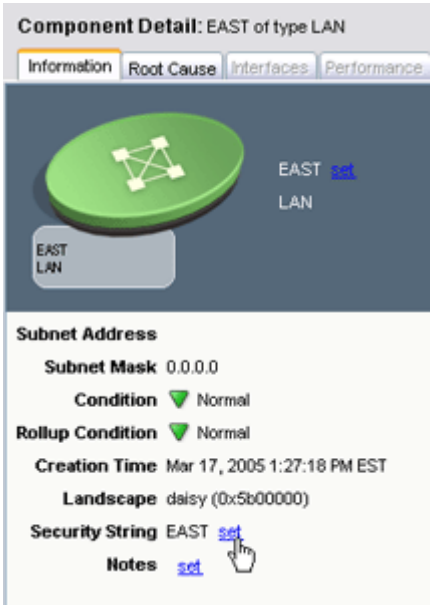
As a complete example of a security implementation in OneClick, consider an East Coast office and a West Coast office. Network administrators in the East coast office must have read/write access to the East Coast office’s network in OneClick. They must also have read-only access to the West Coast network. The inverse is true for the West Coast administrators.

The following procedure can be used to create a solution to this requirement. It can also be modified to suit your needs.

1. Create two LAN containers in OneClick representing the two networks. Name one LAN container WEST, and name the other EAST.
2. Populate each container with different modeled network assets.

3. Set the security string on each LAN container. On the Information tab of the Component Detail panel for a selected LAN container, set the security string:

   a. Set the security string for the EAST LAN container to EAST. This step effectively creates a security community named EAST.



   b. Set the security string for the WEST LAN container to WEST. This step effectively creates a security community named WEST.

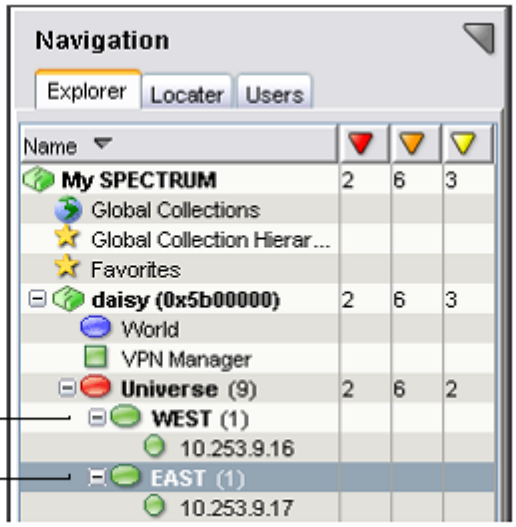
These security strings filter down from the LAN container level to its contained models. A security string set at the container level is automatically set for all its contained models.

When this task is complete, the Explorer tab of the Navigation panel resembles the following image to the OneClick Administrator user:

The **WEST** and **EAST** LAN containers are members of the WEST and EAST security communities, respectively.

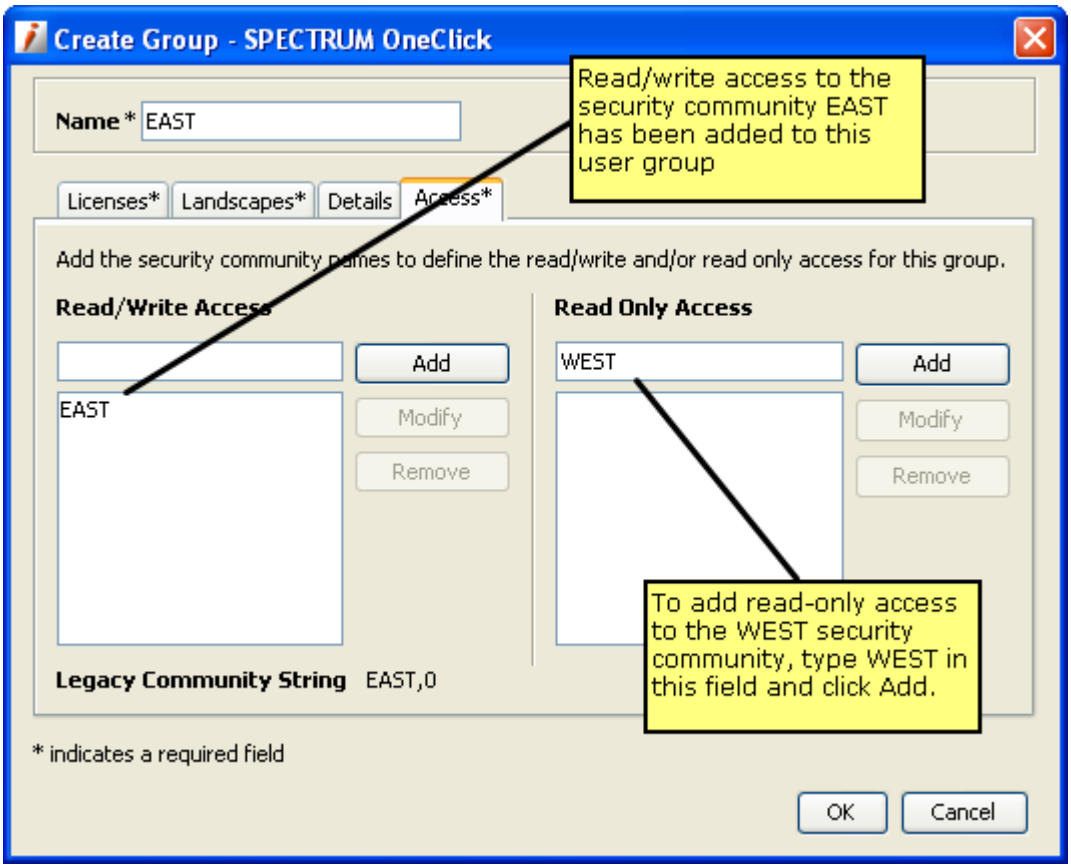
The **WEST** LAN container contains a model of a router at 10.253.9.16

The **EAST** LAN container contains a model of a router at 10.253.9.17



4. Create user groups to correspond with the EAST and WEST network containers:

   a. Create an EAST user group. In the Create Group dialog, create an access group with read/write privileges for the EAST security community:



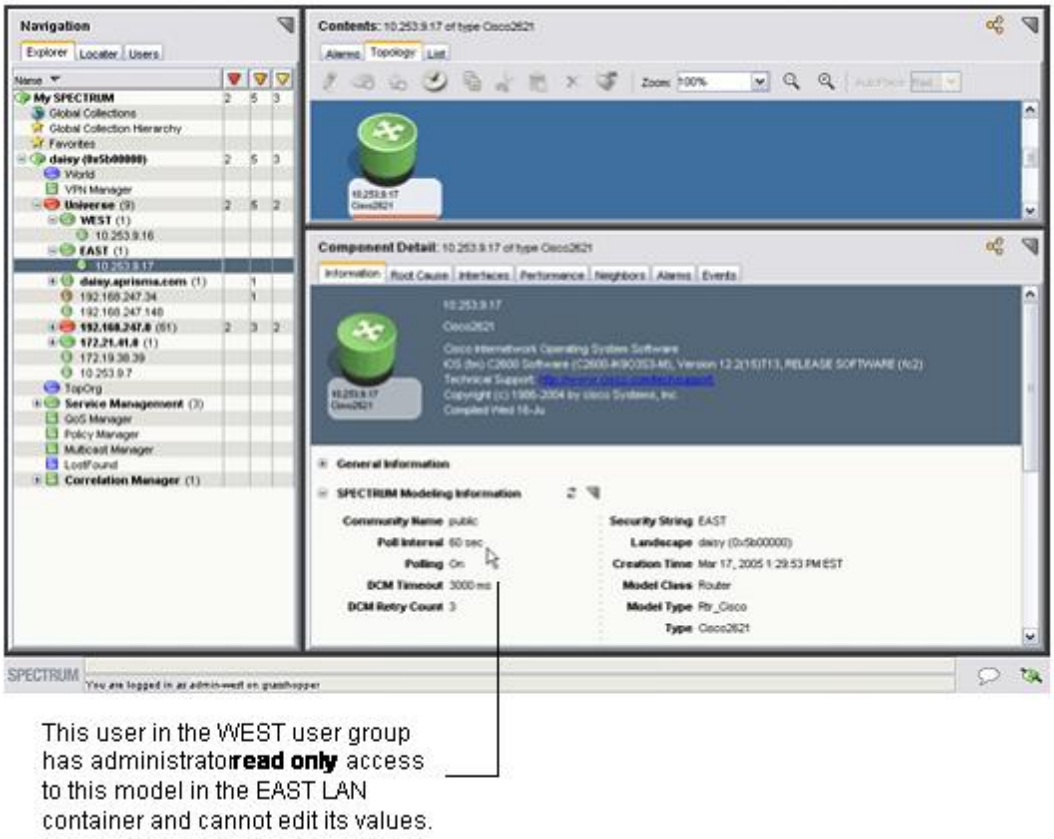
   b. Create a WEST user group. In the Create Group dialog, create an access group with read-only privileges for the EAST security community.

5. Create a user inside the EAST user group and another user inside the WEST user group.

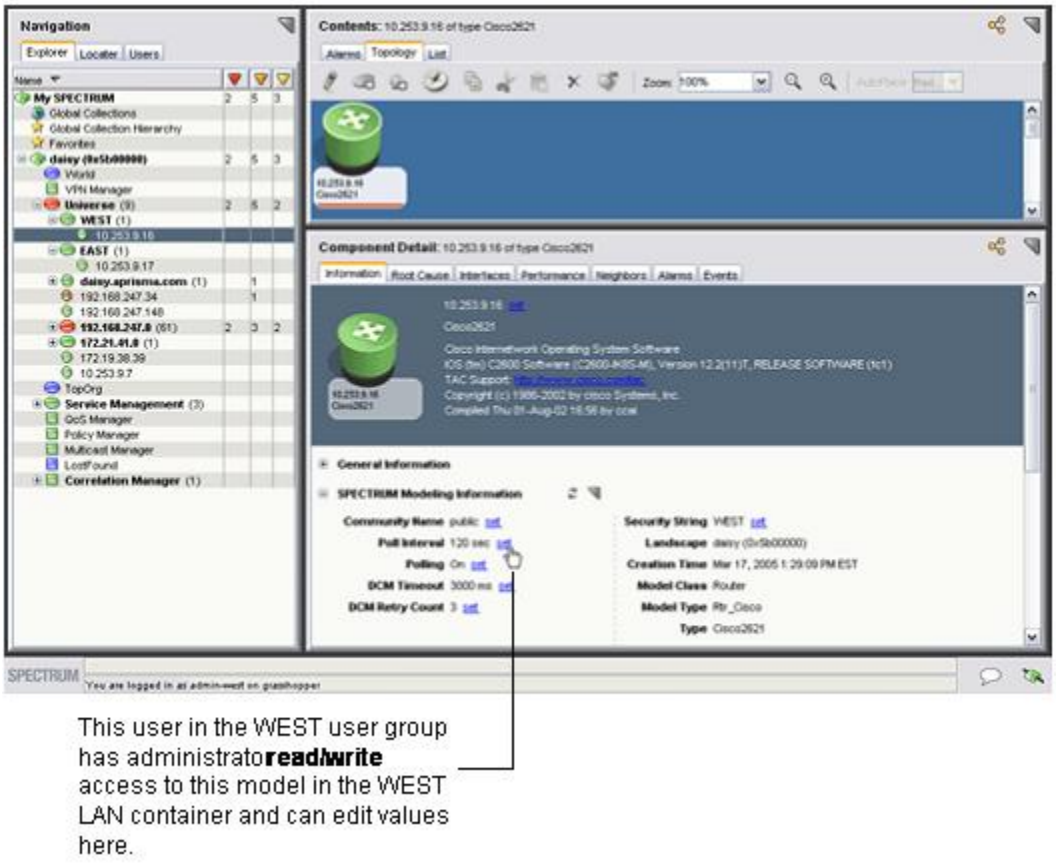
   Note on the Access tab that the access groups (security community) are filled in from the User Group level (not editable here at the User level).

6. To test the changes, log in to OneClick as the user you created inside the WEST user group and navigate to the EAST LAN container.

When viewing models inside the EAST LAN container, users in the WEST user group have Administrator read-only rights as shown in the following image. For example, the image illustrates the fact that this user at this model cannot edit the values in CA Spectrum Modeling Information.



7. Navigate to the WEST LAN container. Note that this user in the WEST user group has Administrator read/write privileges for models inside the WEST LAN, as shown in the following image. The image shows that this user at this model can edit the values in CA Spectrum Modeling Information.



8. If you log in to OneClick as the user that you created inside the EAST user group and navigate to the WEST LAN container, the inverse situation is true: users in the EAST user group have Administrator read-only rights to the models inside the WEST LAN container. And they have read/write rights to the models in the EAST LAN.

Chapter 8: Setting Preferences for Users and Groups

This chapter describes preferences in OneClick and how to use the Set Preferences dialog to set preferences for users and groups.

This section contains the following topics:

Set Preferences Dialog

Preferences in OneClick control the appearance of the OneClick console and the behavior of some user interface options. For example, Preferences control the fonts that are used in tables and the sort order of columns in user interface. You can configure the privileges for users and user groups in OneClick and can also set preferences for users and groups. For more information, see User Administration in OneClick (see page 55). The Set Preferences dialog lets you set, lock, and save preferences for multiple users and groups.

Note: Selecting View, Preferences from the main OneClick menu opens user-level preference editing for the current user. The Alarm Filter dialog that is accessed from this menu can be launched from a button on the Alarms toolbar or from within the Set Preferences dialog.

The Set Preferences dialog organizes OneClick preference settings into the following groups of tasks:

- Alarms Tab
- Events Tab
- Explorer Tab
- General
- Interfaces Tab
- List Tab
- Locater Tab

- Topology Tab
- VPN Manager

If you select the top-level preferences group in the navigation panel, all available preferences and the tools to edit them are displayed in the content panel. Selecting a preference or preference group in the navigation panel displays the preference or preference group in the content panel.

The left panel of the Set Preferences dialog also lets you lock preferences for the selected user or user group. When you launch the Set Preferences dialog in the context of setting preferences for users and groups, the Set Preferences dialog displays the name of the user or group that is edited at the base of the navigation panel.

Access the Set Preferences Dialog

You can access the Set Preferences dialog to set preferences for a user or user group or to set preferences globally for all users.

User or User Group

Follow these steps:

1. On the Users tab, right-click a user or user group to set preferences.
2. Select Set Preferences from the menu.

   The Set Preferences dialog opens.

   You can now set the preferences for a user or user group.

All Users (Globally)

Follow these steps:

1. Right-click the top-level user group (Users) on the Users tab.
2. Select Set Preferences from the menu.

   The Set Preferences dialog opens.

   You can now set the preferences for all users.

About Setting or Locking Preferences

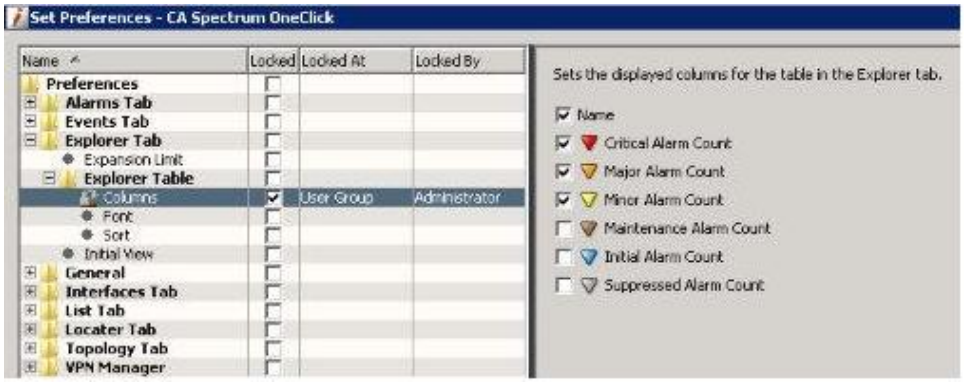
The OneClick administrator can set and lock user preferences at the global level (all users) or at the user group level. Users cannot lock their own preferences. If a preference is set and locked for a user or group, the user or members of the user group cannot change the preference.

Note: A locked preference can only be unlocked and edited at the level where it is locked. If a preference is locked at the global or user group level, the preference cannot be unlocked or edited at the user level. If the Set Preferences dialog is launched in the context of a given user and a preference is locked at the global or group level for that user, the administrator cannot change the preference status. The lock check box is disabled.

The following OneClick administrator privileges control the access to set user and group preferences:

- The Set User Preferences privilege grants access to set preferences for particular users and groups. This privilege is controlled by the user/group model security string. For more information, see the Glossary (see page 128).
- The Set Global Preferences privilege grants access to set preferences at the global level.

The following figure shows preferences for the alarm count columns in the Explorer tab. These preferences are edited to display all alarms for the user group administration. No user in this group can change this preference because it is locked at the user group level. Locked preferences display a small padlock icon.



Set or Lock User Preferences

You set or lock user preferences for users or user groups.

Follow these steps:

1. Right-click the desired user or user group in the Users tab and click Set Preferences.

   The Set Preferences dialog opens.

2. Navigate to the preference you want to set in the hierarchy in the navigation panel.
3. Make changes to the preference in the right panel.
4. Select the check box in the Locked column to lock any corresponding preferences.

   Locking a preference group also locks all preferences that are contained by the preference group. The Locked At column shows the level at which the preference is locked (user, user group, or all users). The Locked By column displays the administrator who locked it.

Alarm Filter Preferences

In addition to being available from a button on the Alarms toolbar, the Alarm Filter dialog can also be launched from the Set Preferences dialog using the Alarms tab, Alarm Filter preference. The right panel displays the Set Alarm Filter button. Access to the alarm filter can be administratively locked. If the alarm filter preference is locked, the filter button in the Alarms toolbar is not available.

You can create multiple alarm filters that are selectable using the Available Filters drop-down in the Alarm Filter dialog. You can configure the available filters for a user or user group and then lock it so the filters cannot be changed but the user can still select from the list of available filters. The Available Filters drop-down is also available on the Alarms tab.

Note: For more information about creating alarm filters, see the *Operator Guide*.

You can also export individual alarm filter preferences to other users and user groups. The exported filters are added to the user's or user group's existing filters; they do not replace existing filters. You cannot import individual alarm filters. Instead, all filters from the importing user or user group are added to the existing filters; they do not replace existing filters.

Note: When exporting preferences in bulk you can only export all alarm filters. You are not given a choice to select individual alarm filters when exporting preferences in bulk. The filters will be added to the existing filters; they do not replace existing filters.

More information:

Set or Lock User Preferences (see page 102)
Import and Export Preferences (see page 103)

Reset Preferences

The Reset Defaults button in the Set Preferences dialog lets you reset preference values back to the default. Resetting the preference automatically applies to the selected user or user group. When you reset the preference, the following occurs:

- For a user, it defaults to:
  - The setting on the User Group if the user is in a group and the preference is set for the group
  - Otherwise, the global setting for all users if set
  - Otherwise, the factory default setting
- For a User Group, it defaults to:
  - The global setting for all users if set
  - Otherwise, the factory setting
- For all users (the top-level Users node), it defaults to:
  - The factory setting

You cannot reset preferences that are locked. If you are modifying the preferences for a user and a given preference is locked at the user's group level, you cannot edit, import, or reset that preference.

Import and Export Preferences

Preferences can be imported from a user or user group and exported to other users and user groups.

Follow these steps:

1. Right-click the desired user or group in the Users tab, and click Set Preferences.

   The Set Preferences dialog opens.

2. Select the preferences to import or export.

   Selecting a preference group selects all of the preferences that it contains. If the top-level Preferences folder is selected, all preferences are selected.

3. Take *one* of the following steps:
   - Click Import to import preferences.
   - Click Export to export preferences.
4. Verify that the preferences you want to import or export are selected in the dialog, and click OK.

   The Select User/Group dialog displays the available users and user groups.
   - When exporting preferences, select a user or user group to which to export. Selecting the top-level Users node specifies all users (global). You only see users/groups for which you have the Set User Preferences privilege. If you lack the Set Global Preferences privilege, you do not see the top-level Users node.
   - When importing preferences, select a single user or group from which to import.
   - For both import and export, you only see the users and user groups that you have permission to view.

   Note: For both import and export, the lock state of each preference is also transferred. For example, importing a locked preference from another user also locks that preference for the target user. If you export a preference that is locked at a higher level for the target user/group, the preference setting is not saved.

Chapter 9: Managing Searches

This section contains the following topics:

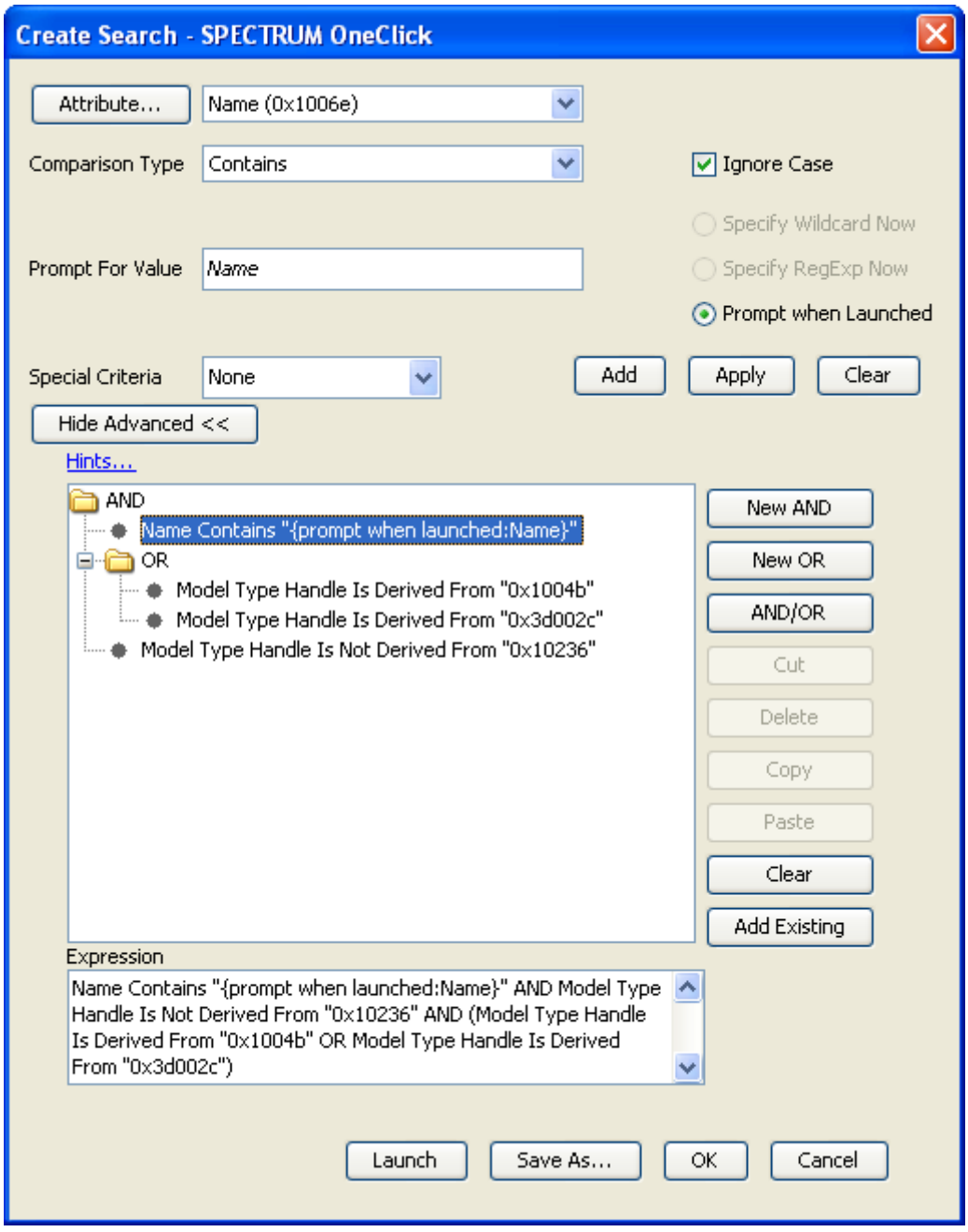
About Searches

You can create custom searches based on attribute values and various comparison criteria. This chapter describes how to create and manage custom searches. In general, these search management tasks are privileges that are granted only to OneClick administrators, not OneClick operators.

Note: While OneClick operators cannot create and manage searches, they can launch them. For information about how operators can use searches, see the *Operator Guide*.

Create Search Dialog

The Create Search dialog contains several options and settings for creating simple and complex searches. The following image is an example of the Create Search dialog.



The options and settings available in the Create Search dialog depend on the type of search you are creating.

Attribute

Specifies an attribute of a device to filter.

Note: If you choose an alphabetic attribute value, you can either clear (ignore) or select (include) the Ignore Case check box.

Comparison Type

Specifies the type of comparison to be made against the value specified in the Attribute field. Options can include Matches Pattern, Equal To, Not Equal To, Contains, Does Not Contain, Starts With, or Does Not Start With. Only the comparison types appropriate to the attribute's data type are available.

Ignore Case

Specifies whether the comparison should be case-sensitive. Selecting the Ignore Case check box makes the comparison not case-sensitive. This selection is only available when it is appropriate for the data type of the attribute you selected.

Attribute Value

Enter or select the desired attribute value you want to use in the comparison.

Note: Depending on the attribute type you select, you may be able to search for empty attribute values by leaving this field blank.

Specify Wildcard Now

Specifies that you want to search for a value using a wildcard (available only for Matches Pattern comparison types). You can use the following wildcards:

*****

Matches *any number* of characters.

For example, 'switc*' returns 'switch' and 'switch-router.'

?

Matches any *single* character.

For example, 'switc?' returns 'switch' but it does not return 'switch-router.'

Both wildcards can be used anywhere and in any combination for a wildcard match.

Specify RegExp Now

Specifies that you want to create a search using Perl Compatible Regular Expression (PCRE) matching on attributes of type text string (available only for Matches Pattern comparison types). PCRE matching helps you to find and group models using specific pattern searches that are more advanced than existing searches or wildcard searches can provide.

Note: For information about how to create PCREs, see http://www.pcre.org.

Note: Remove the "Allow PCRE searches" privilege for operators if you do not want them to run regular expression searches. Operators without this privilege will only be able to run wildcard searches for applicable searches.

Prompt for Value/Prompt When Launched

To create a search that prompts users to enter an attribute value when they run the search, select the Prompt when Launched option and then enter the prompt to display in the Prompt for Value field. This feature lets you create searches that are flexible enough to meet the different search requirements of OneClick users.

Consider the following implementation examples:

- If you want to create a search that locates any particular device type, you could create a search with a string comparison type (contains, does not contain, begins with, and so on) that prompts users to provide a particular device name when they run the search.
- If you want to create a search that locates any device type with a particular Condition attribute value, you could create a search that prompts users to provide a particular condition value when they run the search.

Note: You can clear all fields at any time by clicking Clear.

Special Criteria

Constrains the search criteria in one of the following ways:

None

Specifies that the search criteria will not be restricted to returning only devices or their interfaces.

Interfaces of Devices

Specifies that you want the search to return only the interfaces of the devices it finds in the results list.

Devices Only

Specifies that you want the search to return only devices in the results list.

Show Advanced

Opens the Advanced section of the Create Search dialog. The Advanced section in the Create Search dialog lets you create complex search criteria with any combination of nested AND clauses and OR clauses. This is represented in a tree structure grouped by logical operator (AND and OR) nodes. Each logical operator node can contain any number of attribute criteria nodes and other logical nodes. All nodes directly underneath a logical node are combined using the logical operator.

Add

Adds a new attribute criteria node to the selected AND node or OR node with the information you entered into the Attribute, Comparison Type, and Attribute Value fields.

Apply

Applies the information entered in the Attribute, Comparison Type, and Attribute fields to the selected attribute criteria node.

New AND

Adds a new AND operator node to the selected AND node or OR node.

New OR

Adds a new OR operator node to the selected AND node or OR node.

AND/OR

Toggles the selected AND node or OR node. That is, if the logical operation is currently AND, clicking this button changes it to OR and vice versa.

Cut

Removes the selected node. It can be pasted below another node.

Paste

Pastes the last removed node below the selected AND node or OR node.

Clear

Removes all the nodes below the root node.

Add Existing

(Optional) Adds existing attribute-based, action-based, or relation-based searches to your custom search.

Note: Adding an existing search to your custom search copies the existing search and embeds it, as it is now, into your custom search. If the existing search is later modified, your custom search will not change because it contains only a copy of that existing search, as it was when you copied it and added it to your custom search.

Expression

Displays a textual representation of the search criteria as you create it.

More information:

Create Simple Searches (see page 110)
Create Advanced Searches (see page 111)
Add Existing Searches to Custom Searches (see page 113)

Create Simple Searches

You can create searches that use complex criteria, such as a combination of AND clauses and OR clauses. A simple search contains only a single expression. You can also save searches for later use and organize them in folders.

Follow these steps:

1. Select the Locater tab in the Navigation panel.
2. Do one of the following in the Locater tab:
   - If you want to create a new search from a blank template, click  (Create a new search).
   - If you want to create a new search based on an existing search, select a search and click  (Copy the selected search).

     Note: Some searches cannot be copied and used as the basis for another search. For example, Devices > By IP Address cannot be copied. However, you can create a new advanced search and can copy *any* predefined search criteria into that search. For more information, see Add Existing Searches to Custom Searches (see page 113).

   The Create Search dialog opens.
3. Complete the fields in the dialog as desired (see page 106).
4. Click Save As.

   The Save Search dialog opens.
5. Enter a name and a description for the search.
6. (Optional) Select the appropriate privilege if you want to limit access to the search to users who have a specific custom privilege. The privilege can be either assigned directly to the user or inherited from a role or user group.

   Note: For more information about custom privileges, see the *OneClick Customization Guide*.
7. Select a folder for the search.

   Note: The Locater folder is the top-level folder.

8. Click OK.

   The search is saved in the selected folder.

9. (Optional) Click Launch to run the search.

   The search results appear in the Results tab of the Contents panel.

10. Click OK.

More information:

Create Advanced Searches (see page 111)

Create Advanced Searches

Use the Advanced options in the Create Search dialog to create complex search criteria. You can build a search with many combinations of nested AND clauses and OR clauses.

Follow these steps:

1. Select the Locater tab in the Navigation panel.
2. Take one of the following steps on the Locater tab:

   - To create a search from a blank template, click  (Create a new search).
   - To create a search from an existing search, select a search and click  (Copy the selected search).

     Note: Some searches cannot be copied and used as the basis for another search. For example, Devices > By IP Address cannot be copied. However, you can create a new advanced search and can copy *any* predefined search criteria into that search. For more information, see Add Existing Searches to Custom Searches (see page 113).

   The Create Search dialog opens.

3. Complete the fields in the dialog as desired (see page 106).
4. Click Show Advanced to create complex search criteria that include a combination of AND clauses and/or OR clauses.

   The compound expression tree, logical operator buttons, and Expression field appear.

5. Click Add to move the single expression that you created in Step 3 to the compound expression tree.

   The single expression appears in the compound expression tree.

6. Click one of the following logical operator buttons to build a compound expression:
   - New AND
   - New OR
   - AND/OR

   The selected operator is inserted into the compound expression tree.
7. Repeat Step 3, Step 5, and Step 6 for each compound expression that you want to build.
8. (Optional) Add existing predefined search criteria (see page 113).
9. Click Save As.

   The Save Search dialog opens.
10. Enter a name and a description for the search.
11. (Optional) Select the appropriate privilege from the Privilege drop-down list. Privileges limit access to the search to users with a specific custom privilege. Custom privileges can either be assigned directly or they can be inherited from a role or user group.

    Note: For more information, see the *OneClick Customization Guide*.
12. Select a folder in which to save the search from the Save In Folder section.

    Note: The Locater folder is the top-level folder.
13. Click OK.

    The Save Search dialog closes and you return to the Create Search dialog.
14. (Optional) Click Launch to run the search.

    The search results appear in the Results tab of the Contents panel. The applicable entities have been excluded from the results list based on the compound search expressions you specified.
15. Click OK.

    The Create Search dialog closes and you have now created an advanced search.

More information:

Example Search: Find Devices In Critical Condition (see page 118)
Search Recommendations (see page 114)

Add Existing Searches to Custom Searches

You can add existing attribute-based, action-based, or relation-based searches to any custom search you create. This lets you include predefined search criteria from existing searches including special searches such as All Devices and Devices By IP Address Range.

Note: Adding an existing search to your custom search copies the existing search and embeds it, as it is now, into your custom search. If the existing search is later modified, your custom search will not change because it contains only a copy of that existing search, as it was when you copied it and added it to your custom search.

To add an existing search to your custom search

1. Click the Locater tab in the Navigation panel.
2. Click  (Create a new search).

   The Create Search dialog opens.
3. Complete the fields at the top of the dialog as desired (see page 106).
4. Click Show Advanced.

   The compound expression tree, logical operator buttons, and Expression field are displayed.
5. Click Add Existing.

   The Add Existing Search dialog opens.
6. Select the existing search that contains the criteria you want to copy and add to the current search and click OK.

   The Add Existing Search dialog closes and the criteria you selected is added to the compound expression.
7. (Optional) Click set next to the criteria you added to modify prompt information as desired.

   The Search dialog opens.

8. Do *one* of the following depending on whether you want to prompt users for a value:
   - Select 'Prompt the user' to configure how you want to prompt users:

     Prompt text

     Specifies the text you want to prompt users with when they run the search.

     Default value

     Specifies a default value for this prompt.

     Note: The default value is not shown to users until they run this search.
   - Select 'Specify value now' to enter the prompt value yourself now; users are not prompted to enter anything when they run this search.
9. Click OK.
10. Save the search as described Create Advanced Searches (see page 111).

    You have now created a custom search that includes the addition of an existing search.

Search Recommendations

The following provides search criteria recommendations when defining advanced searches. The order of the criteria can affect the search performance.

The order of attribute criteria is based on two categories: *storage of information* and *data type.*

Storage of information

Attributes should be ordered from least CPU (quickest access) to most CPU (slowest access), as follows:

- Memory flag (least CPU/quickest access)
- Database flag
- Calculated
- External flag (most CPU/slowest access)

Data type

Attributes should be ordered from quickest comparison to slowest comparison, as follows:

- Integer, counter, enumeration, model type handle (quickest comparison)
- IP address, octet string
- Text string (slowest comparison)

Combining the two categories of criteria, the overall attribute placement for complex searches of AND/OR order from top to bottom is as follows:

1. Memory flag
    a. Integer, counter, enumeration, model type handle
    b. IP address, octet string
    c. Text string
2. Database flag
    a. Integer, counter, enumeration, model type handle
    b. IP address, octet string
    c. Text string
3. Calculated
    a. Integer, counter, enumeration, model type handle
    b. IP address, octet string
    c. Text string
4. External Flag
    a. Integer, counter, enumeration, model type handle
    b. IP address, octet string
    c. Text string

Example

You would like to define a search based on the following search criteria (in no particular order):

- ifDesc
- Topology model name string
- Network address
- Model type handle

How should these attributes be ordered for best performance?

Using the recommended ordering logic, the following is the recommended order:

1. Model type handle (memory flag : model type handle)
2. Network address (memory flag/database flag : IP address)
3. Topology model name string (calculated flag : text string)
4. ifDesc (external flag : text string)

Edit Searches

You can edit a custom search that you have saved. The predefined searches cannot be modified.

Follow these steps:

1. In the Locater tab, select the search from the available searches, and click  (Edit the selected search).
2. Edit the search using the controls that are described in Create Search Dialog (see page 106). Select an attribute criteria node to see its information. You can then modify the attribute criterion.
3. Click Apply to change the selected node. Or click the Add button to create a new attribute criteria node.
4. Click OK.

   The modified search is saved.

Delete Custom Searches

You cannot delete preconfigured folders and searches, but you can delete custom searches.

Follow these steps:

1. Click  (Organize, rename, or delete your searches) on the Locater tab.

   The Organize Searches dialog opens.
2. Navigate to the custom search, and select it.
3. Click Delete.
4. Click OK.

   The custom search is deleted.

Organize Custom Searches

You can organize your custom searches in a folder hierarchy. Predefined folders and searches cannot be edited.

Follow these steps:

1. Click  (Organize, rename, or delete your searches) on the Locater tab.

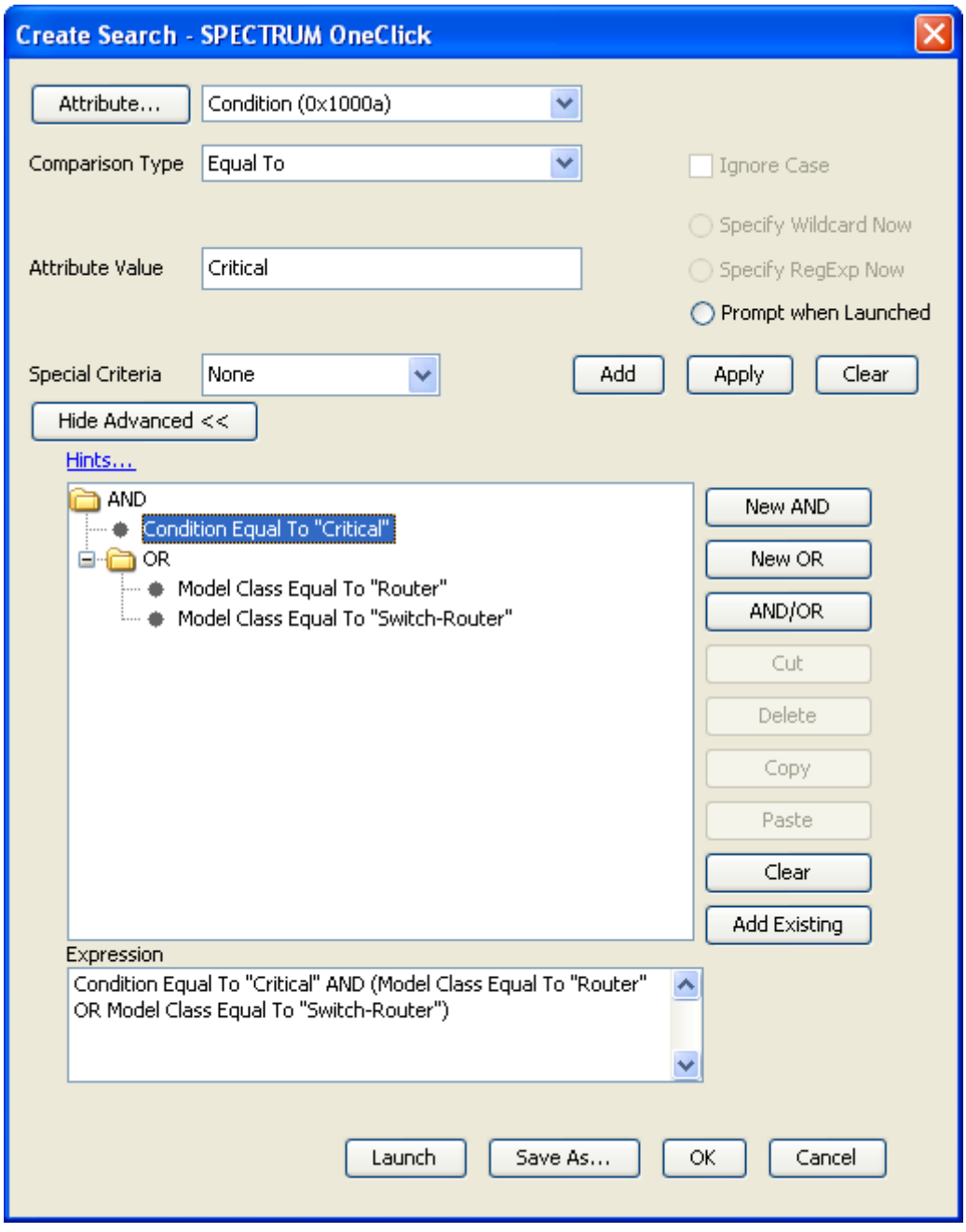
   The Organize Searches dialog opens.

2. Use the dialog to create a hierarchy of folders.
3. Move the searches that you have created into the new folders.
4. Use the Organize Searches dialog to rename or delete your custom folders and searches.
5. Click OK.

   Your custom searches are organized.

Example Search: Find Devices In Critical Condition

Create a compound search that finds all routers or switch routers with a status of "Critical." The following image shows an example of the Create Search dialog after the appropriate compound expressions have been added:



The following procedure provides an example of a useful compound search.

Follow these steps:

1. Select the Locater tab in the Navigation panel.
2. In the Locater tab, click  (Create a new search).

   The Create Search dialog opens.
3. Complete the fields as follows:

   Attribute

   Condition (0x1000a)

   Comparison Type

   Equal To

   Ignore Case

   N/A

   Attribute Value

   Critical
4. Click the 'Show Advanced' button.

   The compound expression box and logical operator buttons appear.
5. Click Add to move the single expression created in Step 3 to the compound expression tree.

   The single expression appears in the compound expression tree and it appears in text string format in the Expression field at the bottom of the Create Search dialog.
6. Click the 'New OR' button.

   The OR operator is inserted into the compound expression tree, beneath the expression: Condition Equal To "Critical."
7. Complete the fields at the top of the Create Search dialog again, using the following parameters:

   Attribute

   Model Class (0x11ee8)

   Comparison Type

   Equal To

   Ignore Case

   N/A

   Attribute Value

   Router

8. Click Add to move this expression to the compound expression tree.

   This expression (Model Class Equal To “Router”) is inserted into the compound expression tree, beneath the OR operator.

9. Complete the fields at the top of the Create Search dialog again, using the following parameters:

   Attribute

   Model Class (0x11ee8)

   Comparison Type

   Equal To

   Ignore Case

   N/A

   Attribute Value

   Switch-Router

10. Click Add to move this expression to the compound expression tree.

    This expression (Model Class Equal To “Switch-Router”) is inserted into the compound expression tree, beneath the OR operator.

11. (Optional) Click Save As to save this search in the Locater tab. You can then run it at any time.

12. Click Launch to run the search immediately.

    The search results appear in the Results tab of the Contents panel.

Appendix A: Troubleshooting

This section contains the following topics:

Non-LDAP Users Cannot Log In

Error binding: javax.naming.AuthenticationException: [LDAP: error code 49 - 80090308: LdapErr: DSID-0C0 903A9, comment: AcceptSecurityContext error, data 52e, v1db1]; remaining name

Reason:

The 'Allow user to login if no LDAP user is found' option is enabled, but your non-LDAP users cannot log in. This error occurs when LDAP is configured using "User by Pattern."

Action:

Reconfigure LDAP to use "User by Search."

More information:

Manage User Access with LDAP Configuration (see page 71)
LDAP Configuration Page (see page 45)

Memory Resources Not Available

The memory resources required to complete the operation were not available.

Reason:

You are attempting to export very large (4000x4000 pixels and greater) Topology view images from OneClick.

Action:

Either reduce the image size by zooming out in the Topology view or increase the OneClick client memory settings as described in Configure OneClick Memory Settings (see page 25).

Blank Panels in OneClick Clients

Symptom:

In a fault-tolerant environment, I am seeing OneClick clients display blank panels after failover to the secondary SpectroSERVER has occurred. OneClick clients display three empty (gray) panels but the connection status shows that the failover switch has occurred.

Solution:

The blank panels occur because user privileges are not in sync between the primary and secondary servers, and the privileges are lost during failover. All user models must be created and completely configured on the primary SpectroSERVER before the primary server's database is copied to the secondary SpectroSERVER. If they are not, any actions done to User models (user associations made to license roles, access groups, and so on) will not be in sync with the secondary server until an online backup occurs. For more information, see the discussion about online backups in the *Database Management Guide.*

OneClick Web Server Shuts Down

Symptom:

I upgraded to VMware 2.0 and it runs an Apache Tomcat server of its own. After I install the OneClick web server, the OneClick web server shuts down when it attempts to bind to port 8005. Then, I receive the following error message:

```
- StandardServer.await: create[8005]:
java.net.BindException: Address already in use: JVM_Bind
```

Solution:

By default, Apache Tomcat uses port 80 on Windows platforms and port 8080 on Linux and Solaris platforms. If SSL is configured, Apache Tomcat uses port 443. Apache Tomcat also uses the default server shutdown port 8005. When installing the OneClick web server, be sure that other applications on the same computer do not use these ports. Or, you can change the ports on the instance of Apache Tomcat that CA Spectrum uses.

Note: We recommend that you do *not* install the OneClick web server on a computer where an instance of Apache Tomcat is already running.

Using the getSpectrumInfo Script

getSpectrumInfo is a script used to gather information about your CA Spectrum environment. The collected data is written to a file that can conveniently be sent to CA Support. The following lists some of the data that is included:

- host information
- configuration files
- installation logs
- SpectroSERVER logs
- Tomcat logs

To use the getSpectrumInfo script

1. Log in to the system for which you want to collect environment data. You will need write permissions to the CA Spectrum installation directory to create the output file.
2. Prepare to enter the script, as follows:
   - On Windows:
     - From the Start, Run menu, type **cmd**, and click OK.

       The DOS prompt appears.
     - Enter **bash –login** to start a bash shell.
     - Navigate to the CA Spectrum installation directory.
   - On UNIX platforms, navigate to the CA Spectrum installation directory.

3. Enter the following command to run the script:

   ```
   ./bin/support/getSpectrumInfo.sh [full|lite|mini]
   ```

   You can use the following parameters on the command:

   full – The complete set of environment data, including all of the Install-Tools/LOGS directory, is collected. The getSpectrumInfo.sh command without any parameters defaults to this option. The output file created can be large.

   lite – A subset of environment data, including selected files from the Install-Tools/LOGS directory, is collected.

   mini – Only the minimum environment data is collected.

   The getSpectrumInfo script begins and displays informational messages as it runs. When it completes, a zipped file is created in the CA Spectrum installation directory in the following format:

   ```
   logs-hostname-YYMMDD-nnnn.tar.gz
   ```

4. Contact CA Support for where to upload the file.

Appendix B: System Customizations

This section lists the parameters that can be edited in the context.xml file and the web.xml file to customize the server and client environment.

context.xml Customization Parameters

The context.xml file, located in the <$SPECROOT>/webapps/spectrum/META-INF directory, contains many OneClick customization parameters. You must restart the OneClick web server after making changes to this file.

maxProcessors

Controls the maximum number of OneClick clients that can be running:

```
<parameter>
    <name>maxProcessors</name>
    <value>75</value>
</parameter>
```

locServerName

Provides the hostname of the CA Spectrum location server:

```
<parameter>
    <name>locServerName</name>
    <value>snowball</value>
</parameter>
```

orbAgentName

```
<parameter>
    <name>orbAgentName</name>
    <value>snowball</value>
</parameter>
```

orbAgentPort

```
<parameter>
    <name>orbAgentPort</name>
    <value>14000</value>
</parameter>
```

adminUserName

```
<parameter>
    <name>adminUserName</name>
    <value>admin</value>
</parameter>
```

smtpHostName and smtpPort

Configure these parameters to set the host name of your mail server and the port that it uses, respectively:

```
<parameter>
    <name>smtpHostName</name>
    <value>mailhost</value>
</parameter>

<parameter>
    <name>smtpPort</name>
    <value>25</value>
</parameter>
```

useSecondarySS

A value of false prevents failover:

```
<parameter>
    <name>useSecondarySS</name>
    <value>true</value>
</parameter>
```

web.xml Customization Parameters

The web.xml file contains additional customization parameters. It is located in the following directory:

```
<$SPECROOT>/tomcat/webapps/spectrum/WEB-INF directory
```

You must restart the OneClick web server after making changes to this file.

To configure the OneClick web server to use a path to SG-Support other than the default, edit the value of the com.aprisma.spectrum.root.install parameter in the following section of the web.xml file:

```
<context-param>
        <param-name>com.aprisma.spectrum.root.install</param-name>
        <param-value>/usr/SPECTRUM/WebApps/SG-Support</param-value>
        <description>
        This parameter defines the absolute path to the directory where
        SG-Support was installed for the Spectrum core product. This
        directory should be <$SPECROOT>/SG-Support.
        </description>
</context-param>
```

Glossary

distributed SpectroSERVER (DSS) environment

A *distributed SpectroSERVER (DSS) environment* consists of more than one SpectroSERVER. This environment enables management of a large-scale infrastructure. The SpectroSERVERs in this environment can be located within a single physical location or in multiple physical locations.

landscape

A *landscape* is all the data that is specific to any one virtual network machine (VNM) in a single network. The term also identifies the network domain that is managed by a single SpectroSERVER. In OneClick, a landscape is the network view of one SpectroSERVER.

legacy SNMP community string

The CA Spectrum *legacy SNMP community string* has been replaced in OneClick by access groups and privileges. The legacy SNMP community string can still be viewed and edited in OneClick under the Details tab for a selected user in the Users tab. The legacy SNMP community string is still used by non-OneClick CA Spectrum applications.

license

A *license* determines which privileges can be granted to holders of that license. Launching a OneClick client consumes any licenses granted to that user.

model

A *model* in CA Spectrum represents a modeled network element.

OneClick Console client

The *OneClick Console client* is a Java JNLP application which provides network operators with a view into the details and health of the network.

OneClick web server

The *OneClick web server* is the server responsible for moving data between SpectroSERVERs and OneClick clients.

role

A *role* is a reusable set of user privileges that you can assign to an access group. For example, the default role (OperatorRW) grants the set of read/write privileges typically needed by a OneClick operator.

security community

A *security community* determines user access to secure models. CA Spectrum users are selectively granted access to models that are secured with a *security string*.

security string

Security strings are expressions that define security communities. Security communities define access to models, securing them from unauthorized users. Security strings are set at the model level for modeled elements in OneClick.

SpectroSERVER

The *SpectroSERVER* is the server responsible for providing network management services such as polling, trap management, notification, data collection, fault management, and so on. This server is also referred to as the Virtual Network Machine (VNM).

super user

A *super user* is a CA Spectrum user that has all possible CA Spectrum privileges and access in OneClick. A user that has been designated a super user is automatically granted all OneClick license roles and privileges.

user

A *user* in OneClick can refer to either a OneClick user account or the actual individual associated with the account. This account is created by a OneClick administrator. It provides a single OneClick user with access to OneClick and stores information about the user, such as password, access, and privileges in the CA Spectrum database.

user group

A *user group* in OneClick is a logical grouping of users that are organized together for a common purpose. Users within the same group can share the privileges granted by the group. When you specify privileges at the group level, OneClick grants each group member those privileges in addition to any privileges they have at the user level.

Index

T

U

W