CA Spectrum®

Network Configuration Manager User Guide

Release 9.4

CA Technologies Product References

This guide references the following products:

- CA Spectrum® (CA Spectrum)
- CA Spectrum® Network Configuration Manager (NCM)
- CA Spectrum® Report Manager (Report Manager)
- CA Service Desk

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 1: Introduction

This chapter provides a general overview of Network Configuration Manager (NCM).

This section contains the following topics:

Network Configuration Manager Capabilities

Configuration management is the process of identifying and monitoring configurations of single devices and device families that comprise a network. Devices include routers, hubs, and switches.

Using the CA Spectrum Network Configuration Manager ensures the following benefits:

- Increases the network uptime by reducing the time to resolve network issues.
- Reduces the network support costs by reducing the occurrence of network issues that require reactive troubleshooting and fixes.
- Reduces the network operational costs by reducing the time to administer system-wide changes.

Each device on the network is configured to provide specific services. Details about how a device operates and how it has been customized are contained in its configuration.

Network Configuration Manager lets you perform the following tasks:

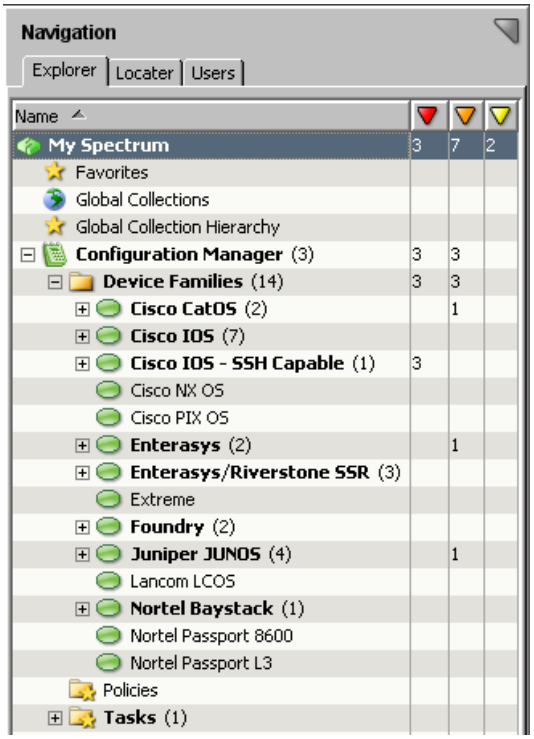
- Manage configurations for supported devices that are modeled in CA Spectrum or OneClick.
- Capture network device configurations and store them in the CA Spectrum database.

- Compare running and startup configurations.
- Upload Perl configuration scripts.
- Load firmware.
- Export configurations.
- Load and merge the configurations to one or more devices of the same family type.

  Note: Merging content appends information to an existing file (it does not overwrite or restore).
- Verify that the correct configuration is running on a device.
- Set up a schedule of automatic captures and policies to ensure reliable device configurations.
- Detect performance problems by verifying device configurations.
- Maintain a history of network device configurations for comparison and troubleshooting.
- Create policies to monitor content in configurations and verify that device content is compliant.

Access Network Configuration Manager

To access Network Configuration Manager from the OneClick Console, select Configuration Manager from the Explorer tab:



When you expand the Configuration Manager node, the Device Families, Policies, and Tasks views appear.

Note: For more information about OneClick, see the *Operator Guide*.

Key Terms

The following terms are important for understanding Network Configuration Manager.

Approval Workflow

Lets you require configuration changes that are initiated through Network Configuration Manager to receive approval before being implemented. An approval workflow can be set up to use CA Service Desk tickets or CA Spectrum authorization privileges for the approval process.

Bulk Task

Bulk tasks are tasks that you can run on multiple devices. The following bulk tasks are available: Upload, Sync, Save to Startup, Load Firmware task, Reload, and Cancel Reload.

Device Family

A group of devices that share common methods to access device configurations. Devices that Network Configuration Manager supports out-of-the-box are automatically placed in a device family. You can use the Extension Utility to create more device families.

Global Synchronization Task

Gathers running configurations for all devices on your network for which Network Configuration Manager is enabled using a schedule. Select a time period and a recurrence frequency to capture configurations from all network-wide supported devices. By capturing the configurations for all devices on your network, you maintain a running configuration history.

Load Firmware Task

Uploads the firmware to Cisco IOS and the Cisco IOS - SSH Capable devices.

Network Configuration Manager Policy

Monitors content in configurations and verifies that device content is compliant. Policies specify a certain aspect of a device host configuration. A policy is checked and compared every time a host configuration file is captured for a device. Devices that violate the policy can generate an alarm and can be semi-automatically repaired. A policy is checked for the compliance when a configuration change occurs on a device.

Reference Configuration

A device configuration that serves as a baseline for reference purposes. You can compare other configurations against the reference configuration. You can have an alarm asserted on the device if the current configuration differs from the reference.

Reload Task

Reloads a device after firmware has been uploaded. This task is available for Cisco IOS and Cisco IOS - SSH Capable devices.

Reusable Task

A task that persists after it has been executed and can be run again multiple times without being redefined. You can also create a recurring schedule to run a reusable task at predetermined times.

Save to Startup Task

Writes a current running configuration to the startup configuration of one or more selected devices. A device saves its configuration in the NVRAM (Nonvolatile Random Access Memory). You can run this task on multiple devices.

Single Device

Representation of a device in your network that CA Spectrum is monitoring. Configuring a single device overrides all global device family configurations.

Sync Task

Captures and verifies policy-compliant device configurations for selected devices on your network and shows the results in real time. When a Sync task captures device configuration, it verifies the configuration against all policies pertaining to the device. You can run this task on multiple devices.

Upload Task

Merges new content into the running configurations of one or more selected devices. You can run this task on multiple devices.

Types of Configurations

The following sections describe the different configurations for a device.

Running Configuration

A running configuration is a version of a configuration that is loaded on a device and defines how the device currently operates. A running configuration only valid for the current run-time session.

Startup Configuration

A startup configuration is the backup version of a configuration that is stored on a device. The startup configuration is used when the device is rebooted. Some devices have primary and secondary startup configurations. A device replaces the previous running configuration with a copy of the startup configuration when it is rebooted.

Configuration File

A configuration file contains a subset of attributes from a running configuration by device manufacturers. Many devices let Network Configuration Manager capture complete configuration files. You can edit captured configuration files.

Supported Devices

Network Configuration Manager supports the device families of the following vendors out-of-the-box:

- Cisco
- Enterasys
- Enterasys
- Riverstone SSR
- Extreme
- Foundry
- Juniper
- Lancom
- Nortel (Baystack and Passport)

Devices that do not fall into one of the out-of-box supported device families can be configured using the Network Configuration Manager Extension Utility.

You can get the list of all the supported devices by querying the device certification database. To access the device certification database, navigate to the CA Support website. The "Recommended Reading" section of the CA Spectrum product page contains a link to "Device and Technology Certification". For more information, see the *Certification User Guide*.

Access the Device Certification Database

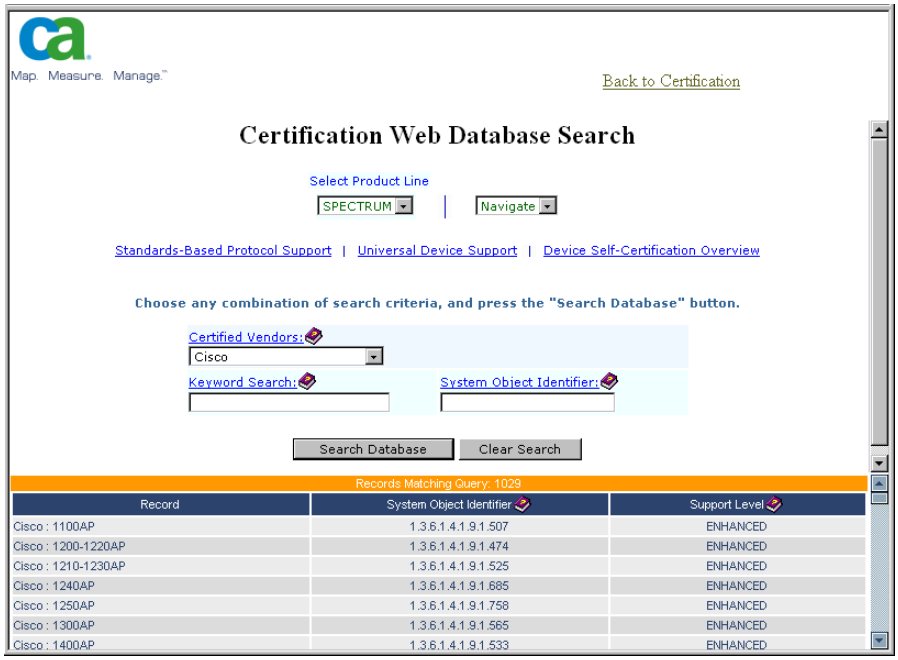
An application on the CA Technical Support website lets you search on all CA Spectrum certified devices. You can determine whether CA Spectrum supports a specific device model and filter by firmware version and release. You can also determine whether a device is supported with a Simple certification or an Enhanced certification.

Follow these steps:

1. Navigate to the CA Support Online website.
2. Access the CA Spectrum product page.

3. Click the 'Recommended Reading' link.
4. Click the 'Device and Technology Certification' link.
5. On that page, click the 'Search engine' link.

   The Certification Web Database Search application appears.
6. Select the Spectrum product from the Product Line drop-down list.



7. Complete the following search criteria fields as needed to locate your device:

   Certified Vendors

   Corporations or organizations that manufacture one or more devices that CA Spectrum has certified. A vendor filter limits your search to all devices owned or acquired by the selected vendor.

   Keyword Search

   Searches in the Device Type Name field of each device. A keyword search limits your search to all devices that contain the specific keyword in the Device Type Name field.

   System Object Identifier

   Searches for a System Object Identifier, or a portion of the System Object Identifier. All devices containing the sequence you enter are returned.

   For example, 1.3.6.1.4.1.9.1.685 identifies the Cisco 1240AP device.

   Note: Not all devices have a unique System Object Identifier. In addition, some devices lack a System Object Identifier.

Support Level

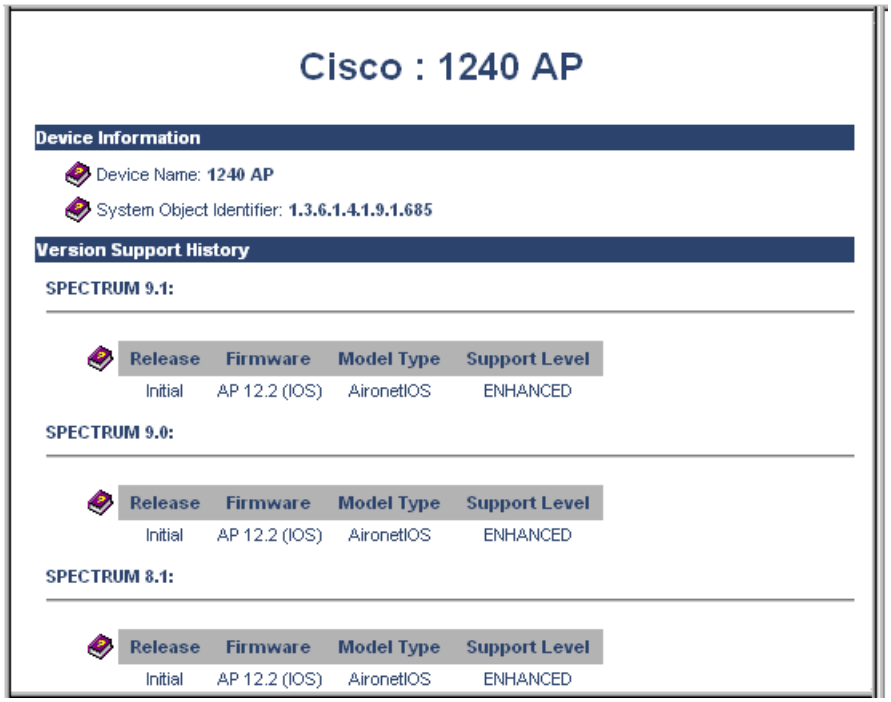
Indicates the current level of CA Spectrum certification support. Two levels of certification support are available. For more information, see the Overview topic.

8. Click the Search Database button to initiate a search based on your search criteria.

   Results are displayed, one line per device. Details at this level include the device name and model, System Object Identifier and Support Level.

9. Click a specific entry in the results table.

   Detailed information about the selected device appears, as shown:



Device Families

To receive Network Configuration Manager support, a device must be associated with a device family. Devices that are supported out-of-the-box are automatically assigned to the proper device family. A device can only belong to a single device family.

A Network Configuration Manager device family provides a central place to configure access methods. The access methods are used to access device configurations from other family members. You can override Device family settings at the local device. For more information, see Configure a Device Family (see page 41).

The Network Configuration Manager Extension Utility lets you create more device families on demand, extending Network Configuration Manager to support more devices and vendors. For more information about manually creating more device families and manually moving devices to user-created device families, see Extension Utility (see page 21).

How Network Configuration Manager Determines Device Families

Network Configuration Manager automatically determines the device family for devices that are supported out-of-the-box. Typically, this determination is made based on the vendor. For more information, see Supported Devices (see page 157).

Cisco IOS Devices

The following device families exist for the Cisco IOS devices:

- Cisco IOS - SSH Capable (supports SSH/SCP communication mode)
- Cisco IOS (does not support SSH/SCP communication mode)

To place a device into the Cisco IOS - SSH Capable family, the following conditions must be met:

- The device descriptor must indicate a firmware version of 12.2 (18) or greater.
- The feature set must contain letters “K9” indicating the device has the necessary encryption functionality that is needed for SCP.
- SSH access for the device must be unblocked at the time of discovery.

  Note: If SSH access to the device is blocked (for example, with a firewall) at the time of discovery, put the device in the Cisco IOS device family.

For example, a device with the following description is placed in the Cisco IOS - SSH Capable family:

```
Cisco IOS Software, 7200 Software (C7200-JK9S-M), Version 12.3(14)T6, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Thu 05-Jan-06 05:36 by dchih
```

A device with the following description is placed in the Cisco IOS family and is not capable of obtaining configurations using SSH/SCP:

Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-J1S3-M), Version 12.3(17a), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Mon 12-Dec-05 1

Cisco NX OS Devices

The Cisco NX OS devices are supported through scripts that use the Net::SSH::Expect modules. The Perl area must be set up with these modules for an out-of box support for Cisco NX OS devices.

For information about setting up your Perl environment, see Perl Modules (see page 61).

Juniper JUNOS Devices

Network Configuration Manager utilizes the JUNOScript API to communicate with the JUNOS devices. Specifically, the JUNOScript API merge command is used to accomplish uploads, as follows:

```
<load-configuration format="text" action="merge">
```

JUNOScript support was developed using JUNOScript version 6.3R1. The new releases of JUNOScript API are typically backward compatible.

The JUNOScript API commands differ from the JUNOS CLI commands. As a result, Network Configuration Manager uploads must use the correct format for the upload to succeed.

For more information, see the documentation website of the Juniper on the JUNOScript API.

Example: Using JUNOScript API Format

The following example illustrates how a command entered from the JUNOS CLI command line differs from the JUNOScript API. The command deletes the snmp location field from a device.

A test device has the following block of configuration text, which sets the snmp location field value to 'Boston':

```
snmp {
     name jun2300-96.4;
     description "Juniper J2300 w/ JUNOS 9.0R4 built 2008-11-18 18:55:38 UTC";
     location Boston;
```

The following command can be used from the JUNOS CLI command line to delete the snmp location field on this device:

```
admin@jun2300-96.4# delete snmp location
```

The following Network Configuration Manager upload deletes the snmp location field from a device:

```
snmp {
     delete: location;
}
```

Both operations are equivalent; however, the JUNOScript API syntax must be used with Network Configuration Manager uploads.

Extension Utility

The Network Configuration Manager Extension Utility lets you extend the functionality of Network Configuration Manager beyond its out-of-box support. With the Extension Utility, you can do the following tasks:

- Create more device families on demand. These additional device families can then be configured to extend the Network Configuration Manager functionality on more devices by using Perl scripts. For more information about creating device families, see Create a Custom Device Family (see page 54). For more information about configuring scripts, see Extension Utility Script Configuration (see page 56).
- Manage more devices and vendors by using Perl scripts for any of the operations Network Configuration Manager executes on a device. The operations such as capturing or writing a startup configuration. The operations also include capturing or uploading a running configuration; and uploading device firmware, reloading a device, and canceling the reload operation on a device. Scripts can be configured within Network Configuration Manager for each of these operations. For more information about using customized scripts to perform these operations, see Network Configuration Manager Extension Utility (see page 53).
- Create customized trap settings for your installation which can be used to correlate the configuration change event information. For more information, see Configure Notification Trap Settings (see page 45).

Network Configuration Manager Prerequisites

To run Network Configuration Manager and actively maintain a running history of device configurations on the managed network, take the following steps:

- Model devices with read/write community strings if you are using SNMP. For more information, see the *Managing and Modeling Your IT Infrastructure Administrator Guide*.
- Verify that devices are SCP-enabled if you are using SSH. For more information, see Communication Modes (see page 22).

Communication Modes

The following table lists communication mode support for devices that are supported in Network Configuration Manager. An 'X' in a column indicates that the communication mode is supported for that device family. When a Perl script is the only way to communicate with the device, you are notified about the method that the script uses.

See Configure a TFTP Server (see page 33) to enable configuration capture and loading for devices that use the SNMP/TFTP communication mode.

Device Family	SNMP/TFTP	Telnet/FTP	SSH/SCP	SSH/TFTP	Perl
Cisco CatOS	X				X
Cisco IOS	X	X			X
Cisco IOS-SSH Capable	X	X	X		X
Cisco NX OS					SSH
Cisco PIX OS					Telnet
Enterasys	X				X
Enterasys/Riverstone SSR	X				X
Extreme	X				X
Foundry	X				X
Juniper JUNOS			X		X
Lancom LCOS					TFTP/ Telnet
Nortel Baystack				X	X
Nortel Passport 8600	X				X

Device Family	SNMP/TFTP	Telnet/FTP	SSH/SCP	SSH/TFTP	Perl
Nortel Passport L3	X				X

SSH v2 Support

Network Configuration Manager supports SSH v2 only. Network Configuration Manager does not support SSH v1. The Cisco devices that support SSH v1 only are not automatically placed in the Cisco IOS-SSH Capable family.

Network Configuration Manager does not support the Juniper devices that support only SSH v1.

To support SSH v2, install or update the firmware on a Cisco or Juniper device. Add the device by following the steps in Place a Device in a Device Family (see page 55).

Cisco Devices and SCP

The Cisco devices must have Secure Copy (SCP) enabled to use the SSH communication mode.

For more information about SCP, see the documentation for the Cisco IOS Secure Copy feature at http://www.cisco.com.

Unsolicited Notifications of Device Configuration Changes

Network Configuration Manager attempts to capture device configurations immediately after any change occurs. An unsolicited notification of configuration change can be either traps or MIB objects that are sent from the device where the change occurred.

Some devices send SNMP traps when their configuration has changed. The SpectroSERVER then performs a capture and saves the configuration in the database to provide updated configuration data. Network Configuration Manager policies are tested against the most recent configuration captures. For more information, see Device Traps (see page 24).

Selected information can be parsed from these configuration trap notifications and shown in the Host Configuration table. For more information, see Configure Notification Trap Settings (see page 45).

Instead of or in addition to sending an SNMP trap, some devices update MIB attributes to signal configuration changes. SpectroSERVER then polls the MIB and captures new configurations when it recognizes changes in the attributes. For more information, see Device MIB Objects (see page 24).

Network Configuration Manager monitors notifications on a subset of supported devices. You can extend Network Configuration Manager to monitor more traps and MIB objects from other supported devices.

Enabling Unsolicited Notifications of Device Configuration Changes provides the most recent and up-to-date configuration captures for devices in your network. You can disable this feature to avoid unnecessary captures, which involve TFTP transfers that can degrade network performance. For more information, see Configure General Configuration (see page 27) and Configure Unsolicited Device Configuration Captures on a Single Device (see page 48).

Device Traps

Network Configuration Manager supports the following two traps:

- Cisco: ciscoConfigManEvent 1.3.6.1.4.1.9.9.43.2
- Juniper: jnxCmCfgChange 1.3.6.1.4.1.2636.4.5

When either of these traps are received, CA Spectrum generates event 0x00821029. This event then triggers Network Configuration Manager to perform a capture. If you want to trigger a capture for other supported devices, map more configuration change traps to that event.

Device MIB Objects

When any configuration changes occur, the Network Configuration Manager polls MIB objects through the model attributes to determine. This feature is supported on Cisco and Juniper devices that support the following MIB objects:

- CISCO-CONFIG-MAN-MIB: ccmHistoryRunningLastChanged 1.3.6.1.4.1.9.9.43.1.1.1
- JUNIPER-CFGMGMT-MIB: jnxCmCfgChgLatestTime 1.3.6.1.4.1.2636.3.18.1.2

You can extend the attribute polling mechanism to other supported devices. Use the Model Type Editor to create the attribute to poll for configuration change notifications, making it a polled attribute. Then, set the value of the Config_Change_AttrID attribute (0x12bf8) to the attribute ID of the newly created polled attribute. Network Configuration Manager then monitors this attribute for the notification of configuration changes and performs a capture.

Global Collections

A global collection lets you organize views of network devices. A global collection contains devices from multiple vendors. The global collections are useful when executing bulk tasks or creating the Network Configuration Manager policies.

For more information about Global Collections, see *Managing and Modeling Your IT Infrastructure Administrator Guide*.

More information:

Apply Policies to Global Collections (see page 140)
Associating Tasks with Global Collections (see page 107)

Maintenance Mode

Network Configuration Manager is disabled for any device that is in maintenance mode. To verify whether the device is in maintenance mode, select the device from the Explorer tab and then click the Information tab. Under the General Information view, see the In Maintenance option. If this option is set to “yes”, the device is in maintenance mode.

Network Configuration Manager Report Packs

Network Configuration Manager report options are included under the Network Configuration Management report pack in CA Spectrum Report Manager. Report Manager provides numerous report content, format, and report organization options. You can generate reports with the appropriate type and scope of information for different audiences in your organization who are interested in device configuration changes.

For more information, see Network Configuration Manager Reports from Report Manager (see page 80) and the *Report Manager User Guide*.

Chapter 2: Network Configuration Manager Configurations

This section contains the following topics:

Configure Network Configuration Manager

This section describes the fundamental configurations for Network Configuration Manager.

Perform General Configuration

Select some initial settings to determine how Network Configuration Manager performs configuration captures and correlates change events.

Follow these steps:

1. Select Configuration Manager in the Explorer tab.

   Information and settings appear in the Information tab of the Contents panel.

2. Expand the General Configuration subview.

   The General Configuration options appear.

3. Modify the following General Configuration options as needed:

   Unsolicited Device Configuration Captures

   Enables or disables Network Configuration Manager from capturing the configuration of a device when it receives an unsolicited notification from a device. An unsolicited notification of configuration change can be either traps or MIB objects that Network Configuration Manager is monitoring for changes.

   Correlation Event Period (seconds)

   Specifies the amount of time during which configuration change events are correlated. All configuration change events for a particular device that occur during this period is combined into a single event.

   Default: 120

Capture Newly Modeled Device's Configuration

Specifies how to handle newly modeled devices on your network at a global level. The available values are:

On Next Global Sync

Captures newly modeled devices according to the global synchronization schedule.

Do Not Capture

Disables Network Configuration Manager on the newly modeled device. To enable the Network Configuration Manager functionality, manually enable Network Configuration Manager on the device.

Immediately

Captures newly modeled devices immediately (once they have been modeled) rather than waiting for the global synchronization to run.

Task Work Queue Size

Specifies the maximum number of devices that are parallel processed on each CA Spectrum host.

When manually stopping a task that is running, all devices currently in the queue are processed after the stop command is received.

Default: 10

Select Configuration History Settings

The following procedure describes how to control storage of captured configurations. You can maintain captured configurations either by the number of configurations that are kept per device, or by a length of time.

Important! When specifying how to store captured configurations, consider the impact on the SpectroSERVER database. If too many configurations are retained, it is possible to fill the SpectroSERVER database with configuration file models.

Follow these steps:

1. Select Configuration Manager in the Explorer tab.

   Information and configurations display in the Information tab of the Contents panel.

2. Expand the Configuration History subview.

   The options that are used to control how captured configurations are stored appear.

3. Select one of the following options:

   - **Specify maximum number of configurations to be stored per device.** This option stores captured configurations per device that is based on a specified number.

     Maximum Stored Configurations Per Device

     Specifies the maximum number of stored configurations per device. For example, a number of 25 indicates that the latest 25 configurations for each device reside in the CA Spectrum database.

     Default: 25

   - **Specify maximum number of days configurations to be stored.** This option stores captured configurations that are based on a length of time.

     Maximum Days Host Configuration Stored

     Specifies the maximum number of days a host configuration is stored before being destroyed.

     Note: Depending on how frequently configurations are captured, specifying a large time period may cause the SpectroSERVER database to fill with configuration file models.

     Default: 30 (days)

     Minimum Stored Configurations Per Device

     Specifies the minimum number of host configurations that are stored per device. Configurations are maintained even if they have aged out to remain at this minimum value.

     Default: 5

Select Configuration Change Alert Settings

Configuration Change Alert settings control which configuration change events trigger alarms and the types of alarms that are generated. You can select Configuration Change Alert settings to determine the alarms that you see.

Follow these steps:

1. Select Configuration Manager in the Explorer tab.

   Information and configurations display in the Information tab of the Contents panel.

2. Expand the Configuration Change Alert subview.

   The Configuration Change Alert options display.

3. Modify the following Configuration Change Alert options as needed:

Alert Mode

Specify the events that trigger an alarm.

Alarm On Any Changes

An alarm is generated for configuration changes only.

Alarm On Any Reference Violations

An alarm is generated for reference configuration violations only.

Alarm On Any Reference Violations or Changes

An alarm is generated for both reference configuration violations and configuration changes.

No Alarm

No alarms are generated for any configuration changes.

Default: No Alarm

Reference Violation Alert Type

Specify the type of alarm or event that is asserted when a reference configuration violation occurs. The existing comparison mask is used to determine significant differences between current and reference configurations. Reference violation alarms are automatically cleared when the current configuration matches the reference configuration.

For information about setting a reference configuration, see Specify a Reference Configuration (see page 77).

Valid values are critical, major, and minor alarms and events only.

Default: Event Only

Configuration Change Alert Type

Specify what type of alarm or event only is asserted when any configuration change occurs.

Valid values are critical, major, and minor alarms and events only.

Default: Event Only

Approval Workflows

Approval workflows let you require configuration changes that are initiated through Network Configuration Manager to receive approval before being processed. Approval workflows can be set up to use CA Service Desk tickets or CA Spectrum authorization privileges for the approval process.

This section describes how to configure approval workflow options. It also describes how to approve tasks if the OneClick approval workflow mode is enabled.

For information about initiating configuration changes using tasks, see Network Configuration Manager Device-Level Tasks (see page 85) and Network Configuration Manager Bulk Tasks (see page 91).

Note: For more information, see the *CA Spectrum and CA Service Desk Integration Guide*.

Configure Workflow Options

Approval workflows let you require configuration changes that are initiated through Network Configuration Manager to receive approval before being processed. Configure approval workflow options to determine how approvals are requested and processed.

Follow these steps:

1. Select Configuration Manager in the Explorer tab.

   Information and configurations display in the Information tab of the Contents panel.

2. Expand the Workflow subview.

   The approval workflow options display.

3. Modify the following approval workflow settings as needed:

   Approval Workflow Mode

   Specifies whether approval is required for all operations that modify a device. These operations include Upload, Save to Startup, Load Firmware, Reload, and the Cancel Reload tasks.

   Disabled

   Specifies that configuration changes initiated in Network Configuration Manager do not require approval.

   ServiceDesk

   Specifies that configuration changes initiated in Network Configuration Manager must gain approval through CA Service Desk. When a task is created, a CA Service Desk ticket is generated. If approved, the task is placed into a state in which it can be processed.

If this option is selected, the Configure button is enabled. Click the Configure button to invoke the ServiceDesk Workflow Configuration page, where you can set the initial values for the following fields:

Error Type - Error type values are configured in Service Desk for integrated use with CA Spectrum. For more information about these values, see the *CA Service Desk Implementation Guide*.

Approved Status, Denied Status, Canceled Status, Awaiting Approval Status - Different status values are available depending on the error type. The Status values are configured in CA Service Desk for integration with CA Spectrum. For information about setting up these values, see the CA Spectrum and *CA Service Desk Integration Guide*.

Note: If Service Desk approval is enabled and the user who creates the task has Task Approver privileges, CA Service Desk approval is optional. For more information, see Network Configuration Manager Privileges (see page 223).

OneClick

Specifies that configuration changes that are initiated in Network Configuration Manager can be processed only if initiated or approved by a user with the Task Approver permission.

Default: Disabled

Include Configuration Changes in Approval Process

Specifies whether configuration content is included in the approval request.

Default: No

Note: A user must have the Hide Configuration Changes from Approval Requests permission for this option to take effect. For more information, see Network Configuration Manager Privileges (see page 223).

Approve a Task in OneClick

If the OneClick approval workflow mode is enabled, a user having the Task Approver permission must approve the tasks from the OneClick console.

Note: You can also approve or deny a task from an email notification. When approval is requested for a task, an email is generated and sent to the task approver for approval. Included in the email are links to let you approve or deny the task. Select the appropriate link. The State is updated to reflect whether the task is Approved or Denied.

Follow these steps:

1. Select 'task' in the Tasks folder under the Configuration manager in the Explorer tab.

   The available tasks appear in the List tab of the Contents panel.

2. Right-click the task and select Approve Task, Deny Task, or Cancel Approval Request, as appropriate, from the right-click menu.

   The task State is updated to reflect whether the task is Approved, Denied, or Canceled, respectively.

Configure a TFTP Server

This section describes how to start a Trivial File Transfer Protocol (TFTP) server on a SpectroSERVER system. TFTP transfers configuration files. This process consists of two steps:

- Setting up your system as a TFTP server. This step varies by platform.
- Specifying the TFTP Configuration settings in OneClick.

If you have a distributed SpectroSERVER (DSS) environment, the TFTP servers must be running on every SpectroSERVER to enable Network Configuration Manager functionality.

See Communication Modes (see page 22) for supported device family communication modes.

Note: Verify that each device in your network is properly modeled using the appropriate community name (read or write).

Set Up System as TFTP Server

This section describes how to set up your system as a TFTP Server. Instructions vary by platform.

Configure a Solaris Version 10 or 11 System to Support TFTP

The following procedure sets up your Solaris (Version 10 or Version 11) system to support TFTP.

Follow these steps:

1. Log in as root.
2. Create the /tftpboot directory and give all users read/write permission to the directory using the following commands:

   ```
   mkdir /tftpboot
   chmod 777 /tftpboot
   ```

   Note: Your TFTP server can run on a system other than the SpectroSERVER host system. But the SpectroSERVER computer must be able to access the root directory of the TFTP server, and the root directory on the SpectroSERVER computer must be shared with the TFTP server. For more information, see Considerations When Using Remote TFTP or FTP Servers (see page 39).
3. Verify that the /etc/services file contains a TFTP entry. To search for the entry, enter the following commands:

   ```
   cd /etc
   grep tftp services
   ```

   You see the following entry in the /etc/services file:

   ```
   tftp          69/udp
   ```

   If this entry does not appear, edit the services file and add it to the “Host specific functions” section.
4. In the /etc/inetd.conf file, find the following line and uncomment it by deleting the pound character (#) from the beginning of the line:

   ```
   #tftp dgram udp6 wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
   ```
5. Verify that the entry ends with the -s /tftpboot option. The ending specifies the tftp directory (in this case, /tftpboot).
6. Run the inetconv command.
7. Verify that the tftp service is enabled:

   ```
   svcs | grep tftp
   ```

   The following response is diplayed:

   ```
   online Apr_10 svc:/network/tftp/udp6:default
   ```
8. When your system is set up as a TFTP server, verify that devices are modeled with the read/write community string for TFTP transfer to work.
9. Configure the TFTP settings in OneClick as described in TFTP Configuration Settings (see page 36).

Configure a Linux System to Support TFTP

The following procedure sets up your Linux system to support TFTP.

Follow these steps:

1. Log in as root.
2. Verify that a TFTP server is installed on your system by running the following command:

   ```
   %rpm -q tftp-server
   ```

   The following message indicates that the TFTP server is installed:

   `tftp-server-<version>.EL3.1`

   If this message does not appear, a TFTP server is not installed. Take the following steps:

   a. Download the TFTP package from the Red Hat website at http://www.redhat.com.

   b. Run the following command:

      ```
      % rpm -i <package.rpm>
      ```

   c. Follow the instructions for installing the rpm package from the Red Hat website.

3. Create the /tftpboot directory and give all users read/write permission to the directory using the following commands:

   ```
   mkdir /tftpboot
   chmod 777 /tftpboot
   ```

   Note: Your TFTP server can run on a system other than the SpectroSERVER host system. But the SpectroSERVER computer must be able to access the root directory of the TFTP server, and the root directory on the SpectroSERVER computer must be shared with the TFTP server. For more information, see Considerations When Using Remote TFTP or FTP Servers (see page 39).

4. Change to the /etc/xinetd.d directory.
5. Edit the file named tftp as follows:

   ```
   Set disable=no
   ```

6. Save and close the file.

7. Run *one* of the following commands to restart xinetd services:

   - % service xinetd restart

     The following message appears:

     ```
     Stopping xinetd  OK
     Starting xinetd  OK
     ```

   or

   - % killall -HUP xinetd

8. Verify that the TFTP server is running.

   Note: One method of verification is to run a Network Configuration Manager capture. If you receive a TFTP timeout error /event 0x821001, it indicates that TFTP is not running.

9. Configure the TFTP settings in OneClick as described in TFTP Configuration Settings (see page 36).

TFTP Servers on Windows

A TFTP server is not typically available on Windows. If you use the TFTP communication mode for any device family, set up a TFTP server. Multiple free or commercial applications are available.

With a TFTP Server on a remote host, see Considerations When Using Remote TFTP or FTP Servers (see page 39) to use that server with Network Configuration Manager.

To configure your Windows system to support TFTP, complete the procedure that is described in TFTP Configuration Settings (see page 36). The steps in this procedure are applicable to any TFTP server that you install.

Configure a TFTP Server on Windows

This section describes how to configure TFTP settings in OneClick.

Note: Before you perform this procedure, make sure that your system has been configured as a TFTP server. For more information, see Set Up a System as a TFTP Server (see page 33).

Follow these steps:

1. Select Configuration Manager in the Explorer tab.

   Information and configurations display in the Information tab of the Contents panel.

2. Expand the TFTP Configuration subview.

   The TFTP Configuration table appears.

3. Modify the following as needed. Click set to edit a particular field, and press Enter when you have finished.

   Default TFTP Host

   TFTP server IP address for the landscape, by default, the host system running the SpectroSERVER.

   This field lets you change the IP address for the TFTP server globally. For considerations when using a remote host, see Considerations When Using Remote TFTP or FTP Servers (see page 39).

   Note: The attribute DefaultTftpHost can be configured in the Attribute Editor.

   Default TFTP Directory

   Pathname where TFTP is running. Click set, and enter a valid TFTP server path, such as:

   - For Unix systems, /tftpboot
   - For Windows, C:\win23app\SPECTRUM\NCM\tftp

   Note: Your TFTP server can run on a system other than the SpectroSERVER host system. But the SpectroSERVER computer must be able to access the root directory of the TFTP server, and the root directory on the SpectroSERVER computer must be shared with the TFTP server. For more information, see Considerations When Using Remote TFTP or FTP Servers (see page 39).

   TFTP Transfer Timeout (sec)

   Amount of time before a TFTP transfer times out. Click set, and specify a timeout value (in seconds) for contact with the TFTP server. The default is 50 seconds, which means there is a 50-second interval between data transfers.

   Landscape

   CA Spectrum landscape (for display only).

Configure an FTP Server

Configure Network Configuration Manager to use a local FTP server on a SpectroSERVER system (see Communication Modes (see page 22) for supported device family communication modes).

If you are deploying devices that use FTP for file transfers, configure an FTP server. We recommend installing and configuring a native FTP server for your platform. For the Windows platforms, the following links describe how to install and configure the native FTP service.

- Windows Server 2008: http://technet.microsoft.com/en-us/library/cc732769(WS.10).aspx
- Windows Server 2012: http://www.c-sharpcorner.com/UploadFile/cd7c2e/how-to-install-ftp-server-on-windows-server-2012/

Follow these steps:

1. Select Configuration Manager in the Explorer tab.

   Information and configurations display in the Information tab of the Contents panel.

2. Expand the FTP Configuration subview.

   The FTP Configuration table appears.

3. Modify the following settings as needed. Click set to edit a particular field and then press Enter.

   Default FTP Host

   FTP server IP address for the landscape. By default, the SpectroSERVER runs on this host system.

   This field lets you change the IP address for the FTP server globally. For more information, see Considerations When Using Remote TFTP or FTP Servers (see page 39).

   Note: The attribute DefaultFtpHost represents this value, which can be configured in the Attribute Editor.

   FTP Username

   FTP username.

   FTP Password

   FTP password.

   Default FTP Directory

   Pathname where FTP is running.

   Note: Your FTP server can run on a system other than the SpectroSERVER host system. But certain requirements apply to the directory. For more information, see Considerations When Using Remote TFTP or FTP Servers (see page 39).

   Landscape

   CA Spectrum landscape (for display only).

Considerations When Using Remote TFTP or FTP Servers

By default, the host system running the SpectroSERVER is also the host system for both the TFTP and FTP servers. However, you can set up your TFTP or FTP server to run on a different host system.

To set up your TFTP or FTP server to run on a different host globally, use the Default TFTP/FTP Host and Default TFTP/FTP Directory fields as described in TFTP Configuration Settings (see page 36) and Configure an FTP Server (see page 37). You can also override the default values for the host by using the Attribute Editor as described in Specify TFTP or FTP Server for a Single Device (see page 39).

Note: Although you can override the TFTP and FTP server host system by device, TFTP and FTP directory settings apply to the entire landscape.

When using a remote host for the TFTP or FTP server instead of the local system where the SpectroSERVER runs, consider the following points:

- Both the specified TFTP and FTP directories must be locally accessible from the CA Spectrum host system. Share the root directory of the TFTP or FTP server with the computer running the SpectroSERVER.
  - For Unix systems, the remote directory must be mounted using read/write nfs mount.
- When specifying the pathname, use the UNC paths only; local variables or locally mapped directories are not allowed. For example, to access the shared folder 'tftpboot' on the host 'tftpserver', specify the UNC path of \\tftpserver\tftpboot as the default TFTP directory.
- On the Windows systems, the UNC path cannot require a username and password and requires read and write privileges.

  Note: Because mapped drives are not supported, mapping the network drive and providing a username and password do not circumvent the requirement.

Specify TFTP or FTP Server for a Single Device

The following procedure describes how to specify a separate host system for the TFTP or FTP server at the device level.

Note: To set the TFTP or FTP host globally for the landscape, use the Default TFTP Host and Default FTP Host fields, as described in TFTP Configuration Settings (see page 36) and Configure an FTP Server (see page 37), respectively. Although you can override the TFTP and FTP server host system by device, TFTP and FTP directory settings apply to the entire landscape.

Follow these steps:

1. Select the devices that will use the TFTP or FTP servers on the separate host in the Explorer tab.
2. Click the List tab in the Contents panel and select the devices.
3. Select Utilities from the Tools menu, and select Attribute Editor.

   The Attribute Editor opens.
4. Select the User Defined folder, and click Add.

   The Attribute Selector window appears.
5. Enter “host” in the Filter field of the Attribute Selector window. Select the NCM_FTP_Host and NCM_TFTP_Host attributes and click OK.

   These two attributes now appear under the User Defined folder.
6. Select both the NCM_FTP_Host and NCM_TFTP_Host attributes and click the add arrow.

   Values that you can modify appear in the right pane.
7. Modify the following values for each attribute:

   No Change

   Clear the check box to enable the remaining fields.

   IP address

   Enter the IP address of the host system running the TFTP and FTP protocols.

   Note: If using NAT, use the public IP address.

   Set As Default

   If selected, all newly created devices automatically inherit this value.
8. Click OK. If a confirmation dialog opens, click Yes.

   The Attribute Edit Results page shows the results of the change.
9. Click Close.

Select Settings for Device Configuration Export

You can configure Network Configuration Manager to export device configurations to a text file for historical archiving purposes. You must manually manage this file system outside of CA Spectrum and OneClick.

Follow these steps:

1. Select Configuration Manager in the Explorer tab.

   Information and configurations appear in the Information tab of the Contents panel.

2. Expand the Export Configuration subview.

3. Click set next to Export Configuration. The default is "Do Not Export." Select one of the following options:

   Export Unique Configurations Only

   Export device configurations only if they differ from previously captured configurations.

   Export Unique and Global Sync Configurations

   Export device configurations only if they differ from previously captured configurations or on a global synchronization. For example, one file per device is generated each day if you have configured a global synchronization to run on a daily basis. See About Global Synchronization (see page 71) for more information.

   The export configuration displays next to Export Configuration.

4. Click set in the Export Directory column. Then specify a local directory in which to export configuration text files for UNIX (Solaris/Linux) and/or Windows. The export files are named with a device name and a timestamp. If you want to export configuration text files to a network share, specify the UNC path to the directory. For example, \\Shared_Server\Export\ExportFiles.

5. Press Enter.

   The export directory appears.

Configure a Device Family

The device family provides a central location to configure Network Configuration Manager interactions with devices in the device family. Configurations that are made to a device family take effect on all devices that are contained within the family. Device family settings can be overridden at the local device level. For more information, see Configure a Single Device to Override Device Family Settings (see page 47).

To access the configurations for a device family, select a device family from Device Families in the Explorer tab. Then select the Information tab in the Contents panel. Device family configurations are shown.

The Extension Utility lets you configure a Perl script to handle device interaction for any of the supported Network Configuration Manager operations. For more information, see Network Configuration Manager Extension Utility (see page 53).

Configure Device Family General Settings

The General Configuration subview contains the Configuration Manager settings. Configuration Manager lets you disable tasks for an entire device family. When Configuration Manager is set to disabled, Network Configuration Manager operations are not performed on any of the devices that are contained by this device family.

Note: Configuration Manager can also be disabled at the local device level if any devices in the Device Family require it. For more information, see Configure a Single Device to Override Device Family Settings (see page 47).

Follow these steps:

1. Navigate to device family configurations as described in Access Network Configuration Manager Device Family Configurations and expand the General Configuration subview.

   The general configurations for the selected device family appear.

2. Click set next to Configuration Manager to enable or disable Network Configuration Manager tasks and functionality for the device family. Configuration Manager is enabled by default.

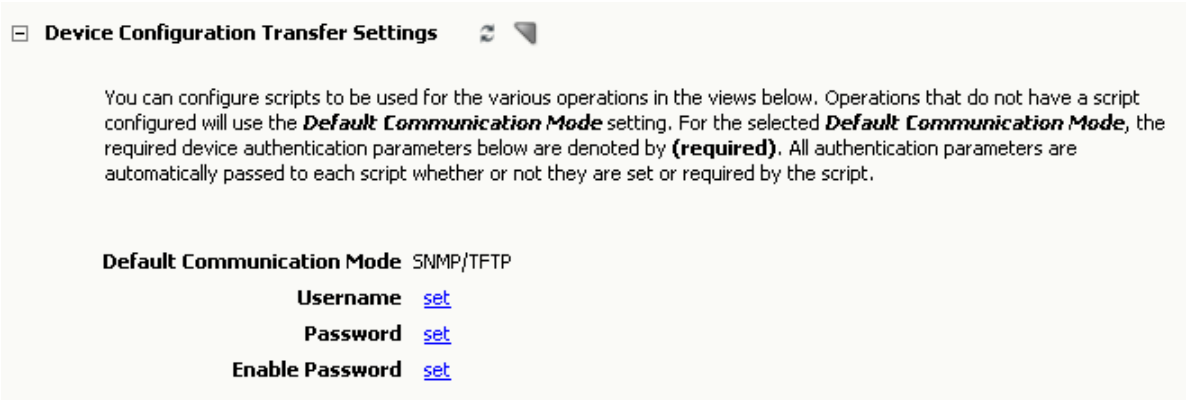
   The status of device family communication with Network Configuration Manager displays next to Configuration Manager.

Configure Device Family Communication Mode

All device families that are supported out-of-the-box have a communication mode that determines how Network Configuration Manager interacts with the associated devices. Some device families with default support let you select from multiple communication modes. Depending on the communication mode that is selected, the device username, password, and enable password can be required.

If not all devices in the family can be accessed using the same username, password and enable password, you can override the usernames and passwords at the local device. For more information, see Configure a Single Device to Override Device Family Settings (see page 47).

The following image shows the Default Communication Mode setting, which appears in the Device Configuration Transfer Settings subview:



Follow these steps:

1. Select a device family from Device Families in the Explorer tab, and then select the Information tab in the Contents panel.

   Device family settings appear.

2. Expand the Device Configuration Transfer Settings subview.

   The communication mode configurations for the device family display.

3. Select the default communication mode for the selected device family.

   The selected communication mode displays next to Default Communication Mode.

4. Modify the following fields as needed:

   Username

   Specifies the user name for accessing the devices.

   Password

   Specifies the password for accessing the devices.

   Enable password

   Specifies the second password for configuring the devices (supported for Cisco IOS, Cisco IOS-SSH Capable, and Foundry devices only).

   The communication mode for the selected device family is configured.

Configure Device Family Masks

Configure device family masks to exclude device configuration content from configuration comparisons or to hide sensitive information from unauthorized users. Mask configurations are discussed in the following sections.

Device Family Comparison Mask

The Comparison Mask is a list of regular expressions that conceal device configuration content during a comparison with a historical configuration. Any line in the device configuration file that matches a regular expression in the Comparison Mask is ignored during comparisons of configuration files. Network Configuration Manager provides a list of predefined masks that are displayed in the window next to Comparison Mask.

You can add or remove masks.

The mask setting can be overridden at the local device level. For more information, see Configure a Single Device to Override Device Family Settings. (see page 47)

Add a Device Family View Mask

The View Mask is a list of regular expressions that conceal device configuration content from users who lack the OneClick privilege to view the entire device configuration file. The View Unmasked Configurations privilege is required to view the contents of the View Mask field. Use this setting to hide passwords or other content from unauthorized users. You can override a mask setting at the local device level.

Follow these steps:

1. Select Add under Comparison Mask or View Mask.

   The Add dialog opens.

2. Type the mask for the selected device family. For example, for comment lines, enter: [!#]. Supply any regular expression.

3. Click OK.

   The content that you entered for the mask appears. You have set a mask for all devices in the device family.

4. Repeat the previous steps to enter more masks.

For more information about overriding device family settings at the local device, see Configure a Single Device to Override Device Family Settings. (see page 47)

Enter a Mask

You can enter a mask that applies to all devices in a device family.

Follow these steps:

1. Select Add under Comparison Mask or View Mask.

   The Add dialog opens.

2. Enter the mask for the selected device family. For example, for comment lines, enter: [!#] or enter any regular expression.

3. Click OK.

   The content that you entered for the mask displays. You have now set a mask for all devices in the device family.

Configure Notification Trap Settings

You can configure CA Spectrum to automatically capture device configuration based on trap notifications from a device. You can customize these trap settings for your installation. Specify the information that is parsed from the configuration change trap notifications from the device and displayed in the Host Configuration table. Network Configuration Manager uses these settings to correlate configuration change event information so that events are combined for a particular device.

Note: The Unsolicited Device Configuration Captures setting controls the automatic configuration capture for a device. For more information about this feature, see Unsolicited Notifications of Device Configuration Changes (see page 23).

Trap format information varies by device family. Out-of-the-box support is provided for Cisco CatOS, Cisco IOS, Cisco IOS - SSH Capable, and Juniper JUNOS device families. The following example shows the Syslog traps that are defaults for the Cisco IOS - SSH Capable device family:

```
Configured from {SOURCE} by {USER} on {LOCATION}
Configured from {LOCATION} by {SOURCE}
```

The following variables represent information that is parsed out from the trap message and shown in the Host Configuration table:

SOURCE

Corresponds to Source column in the Host Configuration table.

USER

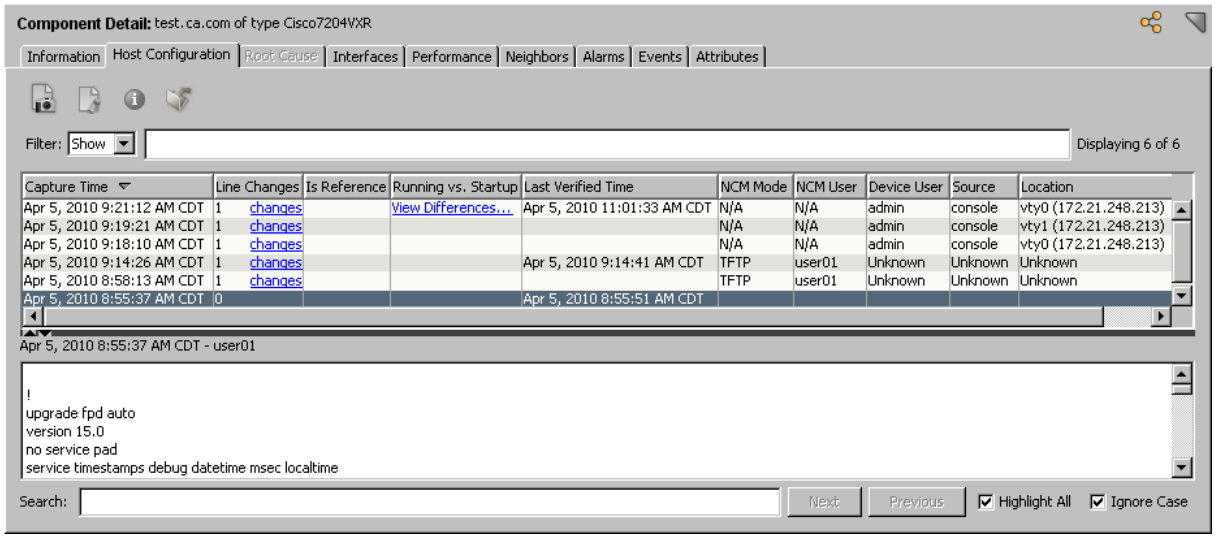
Specifies the user who was logged in on the device when the changes were made. This value corresponds to the Device User column in the Host Configuration table.

LOCATION

Corresponds to the Location column in the Host Configuration table.

You can also specify additional message formats if trap messages from the Syslog server are in non-default formats.

The following image shows the Host Configuration table for a Cisco IOS - SSH Capable device, including the table columns:



Information is correlated based on device traps, Syslog traps and events, Network Configuration Manager internals, and any other trap that is mapped to the generic change event. Correlation Event Period parameter in Network Configuration Manager General Configuration determines the amount of time during which configuration change events are correlated. For more information, see Configure General Configuration (see page 27).

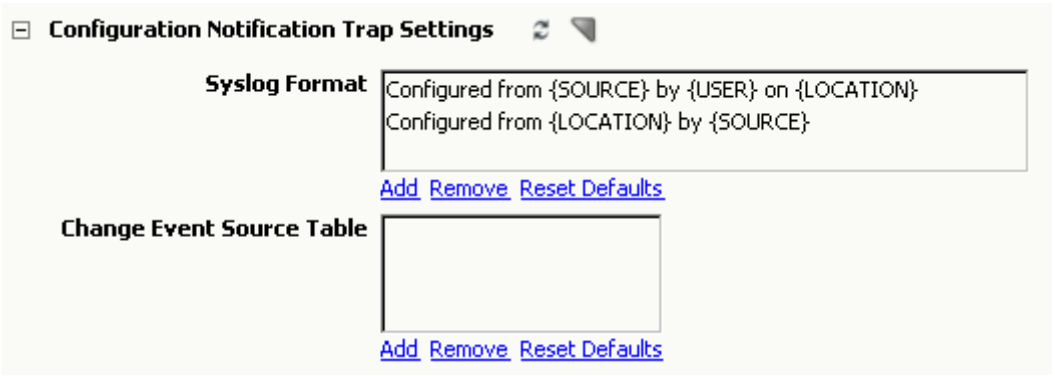
For more information about event messages, see Network Configuration Manager Events (see page 213).

Configure notification trap settings for a device family.

Follow these steps:

1. Navigate to device family configurations as described in Access Network Configuration Manager Device Family Configurations and expand the Configuration Notification Trap Settings subview.

The configuration notification trap settings for the selected device family appear. This subview is configured with the basic formats of the traps that are received from the Syslog server. The following image shows the default settings for the Cisco IOS device family:



2. To add a Syslog format, take the following steps:
   a. Click Add below the Syslog Format box.

      The Add dialog opens.

   b. Enter the format of the trap message with any column-specific information that can be parsed out from the message in {}, and click OK.

   The new Syslog format is added to the box.
3. To add an entry to the Change Event Source Table, take the following steps:
   a. Click Add below the Change Event Source Table box.

      The Add dialog opens.

   b. Enter a Source index entry, and click OK.

      The new entry is added to the table.

Configure a Single Device to Override Device Family Settings

This section describes how to configure a single device to override the configuration of its associated device family. Most device family settings can be overridden at the local device level.

Access Network Configuration Manager Settings on a Single Device

Network Configuration Manager settings for a single device are available in the Network Configuration Manager subview.

Follow these steps:

1. Select a device in the Explorer tab.

   Information and configurations appear in the Information tab of the Contents panel.

2. Scroll down the page and expand the Network Configuration Manager subview.

   The Network Configuration Manager device configuration options appear.

   The settings that you select here override the device family settings.

Enable or Disable Network Configuration Manager on a Single Device

All Network Configuration Manager operations can be disabled at the local device. Network Configuration Manager must be enabled on the associated device family for this setting to affect a device. For more information, see Configure Device Family General Configuration (see page 42).

Follow these steps:

1. Expand the Network Configuration Manager subview as described in Access Network Configuration Manager Settings on a Single Device (see page 48).

   The Network Configuration Manager device configuration options display.

2. Click set next to Configuration Manager to enable or disable Network Configuration Manager tasks and Network Configuration Manager functionality.

   Note: Configuration Manager is enabled by default.

   The current state of communication with Network Configuration Manager displays next to Configuration Manager.

Configure Unsolicited Device Configuration Captures on a Single Device

Unsolicited Device Configuration Captures can be enabled or disabled at the local device.

Note: Unsolicited Device Configuration Captures must be enabled globally for this local setting to have an effect.

For more information, see Unsolicited Notifications of Device Configuration Changes (see page 23).

Follow these steps:

1. Expand the Network Configuration Manager subview as described in Access Network Configuration Manager Settings on a Single Device (see page 48).

   The Network Configuration Manager device configuration options appear.

2. Click set next to Unsolicited Device Configuration Captures to enable or disable automatic device captures.

   The value displays next to Unsolicited Device Configuration Captures.

Specify Configuration Change Alert Settings on a Single Device

Configuration Change Alert settings can be enabled or disabled at the local device.

Follow these steps:

1. Expand the Network Configuration Manager subview as described in Access Network Configuration Manager Settings on a Single Device (see page 48).

   The Network Configuration Manager device configuration options appear.

2. Expand the Local Configuration Change Alert subview.

   The Local Configuration Change Alert options appear.

3. Click set next to 'Use Local Configuration Change Alert Settings' to override the global settings.

   The value appears next to 'Use Local Configuration Change Alert Settings'.

4. Modify the following Configuration Change Alert options as needed:

   Alert Mode

   Lets you specify the events that trigger an alarm.

   Alarm On Any Changes

   Triggers an alarm for configuration changes only.

   Alarm On Any Reference Violations

   Triggers an alarm for reference configuration violations only.

   Alarm On Any Reference Violations or Changes

   Triggers an alarm for both reference configuration violations and configuration changes.

   No Alarm

   Ensures that no alarms are triggered for any configuration changes.

   Default: No Alarm

Reference Violation Alert Type

Specifies the type of alarm or event that is asserted when a reference configuration violation occurs. The existing comparison mask is used to determine significant differences between current and reference configurations. Reference violation alarms are automatically cleared when the current configuration matches the reference configuration.

See Specify a Reference Configuration (see page 77) for information on setting a reference configuration.

Valid values are critical, major, and minor alarms and events only.

Default: Event Only

Configuration Change Alert Type

Specifies the only type of alarm or event that is asserted when any configuration change occurs.

Valid values are critical, major, and minor alarms and events only.

Default: Event Only

Configure Communication Mode on a Single Device

All out-of-the-box supported devices have a communication mode that determines how Network Configuration Manager interacts with the device. Some out-of-box supported devices let you select from among multiple communication modes. Depending on the selected communication mode, the device user name, password and enable password may be required.

For more information about configuring the communication mode for a device family, see Configure Device Family Communication Mode (see page 42).

The following image is an example of the Local Communication Configuration subview:

Configure the communication mode on a single device.

Follow these steps:

1. Expand the Network Configuration Manager subview as described in Access Network Configuration Manager Settings on a Single Device (see page 48).

   The Network Configuration Manager device configuration options appear.

2. Expand the Local Communication Configuration subview.

   The Local Communication Configuration options appear. The available options depend on the device type.

3. Modify the Communication Configuration options as needed:

   Use Local Communication Mode Settings

   Specifies whether to override the device family communication mode with the Local Default Communication Mode.

   Note: The Local Default Communication Mode is not used for an operation if a script is configured for that operation on the device family.

   Local Default Communication Mode

   Specifies the communication mode if your device lets you choose from multiple communication modes.

   Use Local Authentication Settings

   Specifies whether to override the device family authentication settings. When enabled, the values that are specified in the Local Username and Password fields are used.

   Local Username

   Specifies the user name for accessing the device.

   Local Password

   Specifies the password for accessing the device.

   Local Enable Password

   Specifies the second password for configuring the device (supported for Cisco IOS, Cisco IOS-SSH Capable, and Foundry devices only).

   The local communication configuration options for the selected device are set.

Configure a Mask on a Single Device

Configure masks to exclude script content from configuration comparisons or to hide sensitive information from unauthorized users. Masks configured at the local device level override the mask settings of the device's associated device family. Mask configurations on a single device are discussed in the following sections.

Comparison Masks

The Comparison Mask is a list of regular expressions that conceal device configuration content during comparison with a historical configuration. Any line in the device configuration file that matches a regular expression in the Comparison Mask is ignored during configuration file comparisons. Network Configuration Manager provides a list of predefined masks that are displayed in the window next to Comparison Mask. Masks on local devices override the mask settings of the device family.

View Masks

The View Mask is a list of regular expressions that conceal device configuration content from users who lack the OneClick privilege to view the entire device configuration file. Content in the View Mask field is only accessible to operators with the View Unmasked Configurations privilege. Use the mask to hide passwords or other content from unauthorized users. Masks on local devices override the mask settings of the device family.

For more information about the View Unmasked Configuration privilege, see Network Configuration Manager Privileges (see page 223).

Enter a Mask on a Single Device

You can enter a mask for a single device.

Follow these steps:

1. Expand the Network Configuration Manager subview as described in Access Network Configuration Manager Settings on a Single Device (see page 48).

   The Network Configuration Manager device configuration options display.

2. Expand the Local Mask Configuration subview.

   The local comparison and view masks options display.

3. Click set next to Use Local Comparison Mask or Use Local View Mask to override the device family settings.

   The value displays next to the option.

4. Select Add under Local Comparison Mask or Local View Mask.

   The Add dialog opens.

5. Enter the mask for the selected device. For example, for comment lines, enter: [!#] or enter any regular expression.

6. Click OK to accept your entries.

   The content that you entered for the mask displays. You have now set a mask for the selected device.

7. Repeat Step 4 to Step 6 to enter more masks.

Network Configuration Manager Extension Utility

The Network Configuration Manager Extension Utility lets you extend the basic functionality of Network Configuration Manager. You can create device families and manage additional devices and vendors by using Perl scripts for the operations that Network Configuration Manager executes on a device. You can customize trap settings and use them to correlate configuration change event information.

The following sections describe how to use the Extension Utility to expand Network Configuration Manager support.

Supported Operations

The Network Configuration Manager Extension Utility lets you use Perl scripts to extend Network Configuration Manager to additional devices and vendors. Network Configuration Manager can be extended by providing Perl scripts for any, or all, of the operations Network Configuration Manager performs on a device. The following list summarizes these operations:

Capture Startup Configuration

Capture device startup configuration.

Capture Running Configuration

Capture device running configuration.

Upload Running Configuration

Upload and merge specified content into the device running configuration.

Write Startup Configuration

Write the device current running configuration to its startup configuration.

Reload Device

Reboot a device.

Cancel Reload

Cancel the scheduled reboot of a device.

Load Device Firmware

Initiate a load of the specified firmware image on the device.

Scripts can be configured for each of these operations within device families that are created on demand. Any operation that lacks a script is handled as an unsupported operation for the given Device Family and all devices contained within it.

The Cisco PIX OS out-of-box device family provides an example of how scripts are used to extend Network Configuration Manager support. (Within these example scripts, the Net::Telnet perl module does *not* support IPv6.)

The utility also lets you use Perl scripts to alter Network Configuration Manager interactions with devices that belong to out-of-the-box device families.

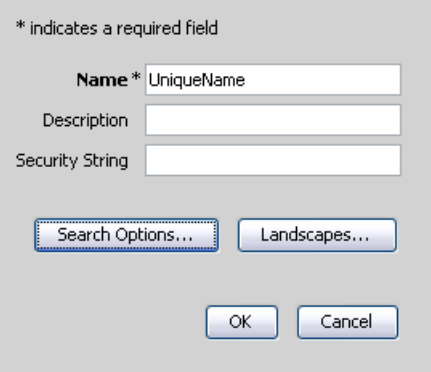
Create a Custom Device Family

Network Configuration Manager supports Cisco, Enterasys, Enterasys/Riverstone SSR, Extreme, Foundry, Juniper, Lancom, Nortel Baystack, and Nortel Passport device families out-of-box. The Network Configuration Manager Extension Utility lets you create custom device families.

Follow these steps:

1. Expand Configuration Manager in the Explorer tab of the Navigation panel.
2. Right-click Device Families, and select Create Device Family.

   The Create Device Family dialog opens as shown in the following image:



3. Enter a unique name in the Name field.
4. (Optional) Enter a description and security string.
5. (Optional) Click the Landscapes button to select the Landscapes where you want to place the device family.
6. Click the Search Options button to search for specific devices.

   The Search Options dialog opens. Like a Global Collection, a device family can have both static members that are manually added to the family, and dynamic members that are automatically added using specified search criteria. For more information, see the *Administrator Guide*.

   Note: A device can belong to only one device family. If multiple device families contain search criteria that apply to the same device, the first device family to execute the search contains the device.

7. Click OK when you have finished.

   The device family is created and appears under Device Families in the Explorer tab of the Navigation panel. Static members can now be added.

Place a Device in a Device Family

Network Configuration Manager automatically assigns out-of-the-box supported devices to the family. A device that is currently associated with a device family must be manually moved to a user-created device family. Manually-created device families that contain search criteria to define membership do not pull in devices that already belong to a device family. For the search criteria to pull in a new device, the device must not currently be a member of any device family.

You have several options for placing a device in a device family. You can manually make the association.

Follow these steps:

1. Locate the device.
2. Right-click the device and select Add To, Device Family.

   The Select Device Family dialog opens.
3. Select the device family that you want to associate with the selected device.

   If a suitable device family is not displayed, create a custom device family by clicking Create. See Create a Custom Device Family (see page 54) for more information.

   The device is now associated with the selected device family.

You can force a manually created device family to update using its defined search criteria.

Follow these steps:

1. Right-click the device family in the Navigation panel.
2. Select Update Device Family.

   The device family searches for and adds all devices that meet the search criteria if they do not currently belong to a device family.

For more information about device family search criteria, see Create a Custom Device Family (see page 54).

You can also restore a device to one of the out-of-box supported device families.

Follow these steps:

1. Right-click a device that is not currently associated with a device family.
2. Select Reconfiguration, Reevaluate NCM Device Family.

   Important! Cisco PIX devices do not support the Reevaluate NCM Device Family function.

   Network Configuration Manager reevaluates the device to determine whether it should belong to an out-of-the-box device family.

   If Network Configuration Manager determines that the placement is appropriate, the device is added to the device family.

Note: The Reevaluate NCM Device Family action on a device that is currently in a manually created device family has no effect.

For more information about out-of-the-box supported device families, see Supported Devices (see page 157).

Extension Utility Script Configuration

Perform all interactions with Network Configuration Manager scripts using OneClick. Network Configuration Manager handles all script administration within the CA Spectrum environment. The available scripting options are discussed in the following sections.

Scripting Considerations

When a script is configured for a Network Configuration Manager operation, the script is used for all devices in the family. For example, if scripts are configured for all of the supported operations in the Cisco IOS SSH Capable device family, the Communication Mode setting at the device family and any overridden Communication Mode settings at local devices will have no effect. In this example, the scripts for all Network Configuration Manager operations on all devices contained in the Cisco IOS SSH Capable Device Family will be used.

In the case where only a subset of the Network Configuration Manager operations have scripts configured, Network Configuration Manager uses the Communication Mode selected at the device family or overridden at the local device for the operations for which no script is configured.

Username, Password and Enable Password are always sent to the scripts as command line parameters. The values specified in the device family are used unless they are overridden at the local device in which case the locally overridden values are used.

Default Script Command Line Parameters

By default Network Configuration Manager provides the following parameters, in the order shown, to every script. If the script does not make use of these parameters, the script must still be written to accept them.

- Device IP.
- Absolute filename of file containing content to upload. (Upload operation only).
- Device Username.
- Device Password.
- Device Enable Password.

Additional Script Command Line Parameters

Optionally, unlimited additional command line parameters can be configured for each of the supported operations. The parameters are passed on the command line to the script after the default set of parameters. The parameters are passed in the order they are shown in the Additional Script Parameters list.

Upload Running Configuration and Load Device Firmware operations can have additional command line parameters configured in such a way that the user is prompted for a value at runtime. A label and default value can also be displayed when prompting at runtime.

Error Code Mappings

Network Configuration Manager provides the ability to map non-zero integer values returned by the script to a textual error message which displays in OneClick if the error occurs. This enables script creators to provide detailed information on the failure mode.

Script Error Handling

For Network Configuration Manager to report success of a script-based operation, the script must return a value of zero. Network Configuration Manager assumes the operation failed if a non-zero value is returned by the script.

Additional Error Detail Returned in STDERR Buffer

If a script returns a non-zero value, in addition to the error mapping above, Network Configuration Manager will also look for any output returned by the script in the STDERR buffer. If content is found, it will display in OneClick as additional error information.

Enter a Configuration Script

Network Configuration Manager can use Perl scripts for the following operations:

Capture Startup Configuration

This script must return the device startup configuration in the STDOUT buffer. All content that is returned in the buffer is considered to be the device startup configuration.

Capture Running Configuration

This script must return the device running configuration in the STDOUT buffer. All content that is returned in the buffer is considered to be the device running configuration.

Upload Running Configuration

This script reads the file that is identified by the Absolute Filename parameter (for more information, see Default Script Command Line Parameters (see page 57)). It then uploads and merges the content of the file to the device running configuration.

Write Startup Configuration

This script causes the device running configuration to be written to its startup configuration.

Reload Device

This script reboots a device.

Cancel Reload

This script cancels a pending or scheduled reboot of a device.

Load Device Firmware Configuration

This script uploads a new firmware image onto a device and executes all necessary operations to reload the device using this firmware image.

You can select a configuration script for these operations.

Follow these steps:

1. Select a device family from the Explorer tab.

   Information and configurations display in the Information tab of the Contents panel.

2. Expand the Device Configuration Transfer Settings subview.

   The script operation subviews appear.

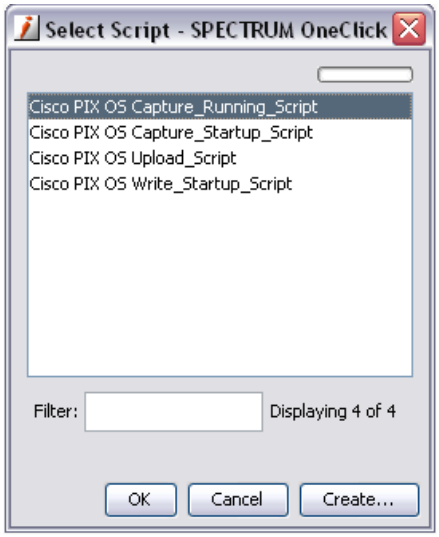
   Note: For the Cisco IOS and Cisco IOS - SSH Capable device families, the Load Device Firmware Script resides in the Device Firmware Transfer Settings subview.

3. Expand the appropriate script operation subview.

   The available script configuration fields display.

4. Click set next to the script name.

   The Select Script dialog opens as shown in the following example:

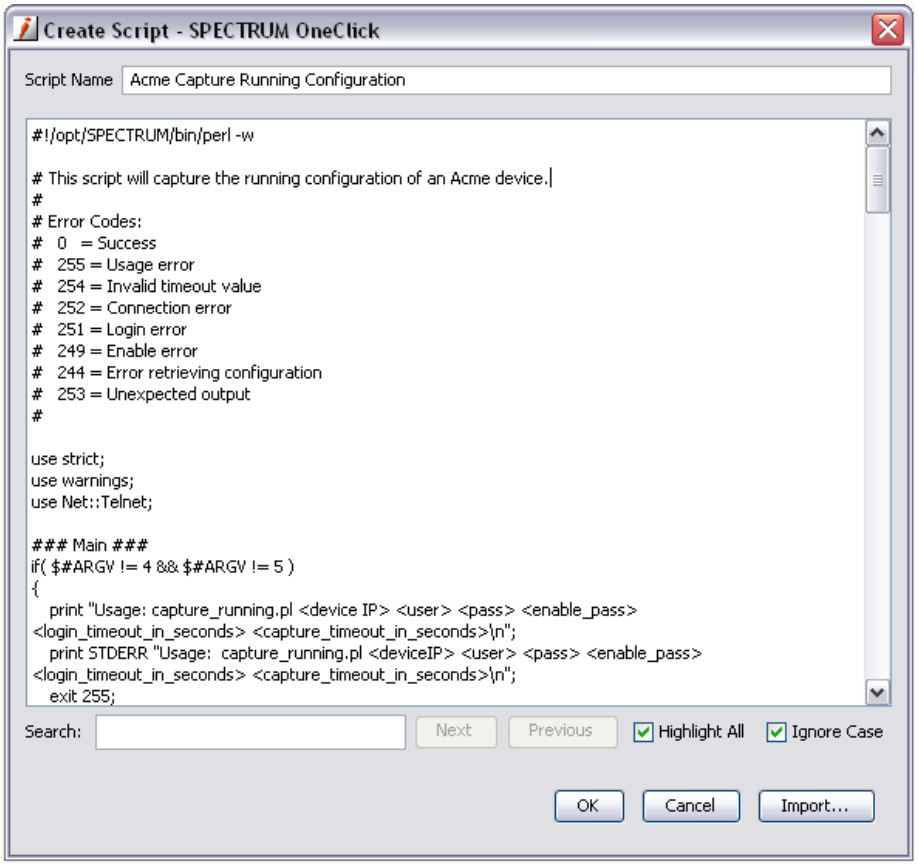


5. Take one of the following steps:

   - If a script that you want to use is available, select the script, click OK, and go to Step 10.
   - If you have not yet created a script for the selected device family, click Create to upload or create one.

6. Supply a unique name for the script in the Script Name field. Paste the script into the field under Script Name, or click Import to import a configuration file that is saved locally on your system.

The script content appears in the field under the Script Name field, as shown in the following example:



7. (Optional) Edit script content if necessary. Or enter criteria in the Search field to locate specific lines in the script file.
8. Click OK when you have finished importing and configuring the script.

   The script name appears in the Select Script dialog.
9. Select the script, and click OK.

   The script is loaded and is visible in the Script Content field.
10. Add any additional script parameters.

    Note: For more information, see Additional Script Command Line Parameters (see page 57).

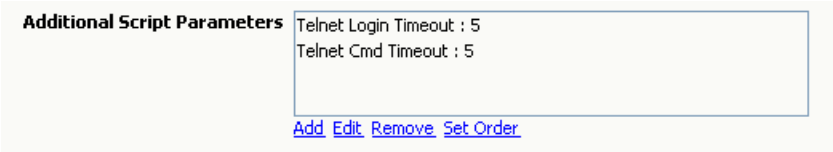
11. Click Add under the Additional Script Parameters field.

    The Add dialog opens.

    a. Enter the parameter name and value. If the operation is Upload, or the task is Load Firmware, you can configure the parameter to prompt you at run time for a value.

    b. Click OK.

       The parameter appears in the Additional Script Parameters field, as shown in the following example:



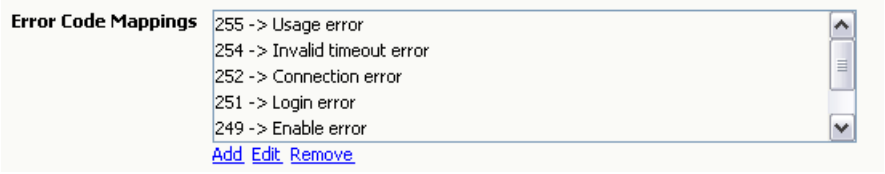
12. Add any error code mappings. For more information, see Error Code Mappings (see page 57).

13. Click Add under the Error Code Mappings field.

    The Add dialog opens.

14. Enter the error code in the Error Code field and the corresponding message in the Error Message field, and click OK.

    The error code appears in the Error Code Mappings field, as shown in the following example:



    The configuration script is ready to run.

Perl Modules

CA Spectrum ships all Perl Modules (for the Windows/Solaris platforms) required to run the Perl scripts that are provided out-of-box. That includes:

- Net::Telnet

In addition, CA Spectrum also comes with certain perl modules that may be useful in developing scripts for the Extension Utility. These include:

- Net::SSH
- Net::SSH::Expect

- Expect
- Net::TFTP
- Net::SCP
- Net::FTP

Perl modules that ship with CA Spectrum can be viewed at:

```
/opt/SPECTRUM/lib/perl5
```

Important! Perl modules not compiled and installed correctly may result in failure or other undesirable behavior.

Using SSH-based Perl Scripts for Network Configuration Manager Operations

CA Spectrum's out-of-the-box scripts-based support for Network Configuration Manager operations is based on the Net::Telnet module. If you want to use SSH-based scripts for Network Configuration Manager operations:

- **Windows and Solaris** — CA Spectrum includes a complete perl install and the Net::SSH::Expect module.
- **Linux** — You must install perl to a separate location on your system and configure CA Spectrum to use that perl.

This Perl installation and configuration on CA Spectrum will have to be done on a per landscape basis in a DSS. You will have to set up perl for each landscape on which you have devices modeled to use SSH-based scripts.

Note: If you want to continue to use CA Spectrum's out-of-box scripts once you have configured CA Spectrum to use your custom Perl install, then your custom Perl area must have the Net::Telnet perl module installed. You can download and install this module from www.cpan.org. Otherwise, CA Spectrum's out-of-box scripts will fail.

In order to set up SSH-based scripts, follow the instructions specific to your platform.

On Windows

1. Install Perl.

   CA Spectrum ships with Cygwin’s complete version of Perl, so you are not required to install anything more if you want to use scripts based on the Net::SSH::Expect module.

If you want to use scripts based on some other module, complete one of the following depending on the module you are using:

- If the perl module is compatible with a version of Perl other than Cygwin, then we recommend that you install that specific Perl onto your SpectroSERVER machine, then install your specific perl module, and then configure CA Spectrum to use your particular Perl install. (See Configuring CA Spectrum to Use a Custom Perl Install (see page 65).)
- If the perl module that you want to install is only compatible with Cygwin's perl, and is a change module (i.e., it does not require compilation of C libraries), then you can add it to the CA Spectrum Perl install. Just place the <Module_Name>.pm file in $SPECROOT/NT-Tools/SRE/lib/perl5/site_perl/5.8
- If the perl module that you want to install is only compatible with Cygwin's perl and also requires C libraries to be compiled, then this module will have to be compiled and shipped with CA Spectrum. Contact CA Spectrum support for this enhancement request.

2. Install SSH-based perl modules and SSH program.

   CA Spectrum ships with the Net::SSH::Expect (and its required) modules and the ssh program (that is required by Net::SSH::Expect). For instructions on how to develop scripts using this module, check the documentation for Net::SSH::Expect on www.cpan.org.

3. Configure CA Spectrum to use the custom Perl install.

   Since CA Spectrum's perl is set up for this purpose, you don't have to configure CA Spectrum to use a custom perl install.

On Solaris

CA Spectrum on Solaris comes with the Perl modules listed above. To use a perl module other than the ones that are shipped with CA Spectrum, you must install perl to a custom area.

1. Install Perl.

   Perl is available in many different versions for Solaris. You can download Perl that is compiled for your particular Solaris version from Sun Freeware (www.sunfreeware.com). Perl v5.8.8 has been tested for and is compatible with the Net::SSH::Expect perl module.

   Note: SunOS may come with its own version of perl (v5.005), but we do not recommend using this version for Network Configuration Manager script purposes as you may run into incompatibility issues with some of the modules required for communication.

2. Install SSH-based perl modules and the SSH program.

   If you want to use the Net::SSH::Expect module, all you need to do is set up the ssh program.

The Net::SSH::Expect module requires the ssh utility to be installed. If your system does not already contain the utility, you may download and install it from www.sunfreeware.com by installing the OpenSSH package.

If you want to use additional modules, you can download them from www.cpan.org.

Be sure to install these modules to the custom Perl area you installed above.

This can be done by specifying the full-path of the perl binary when you are installing the modules such as:

<PERL_FULL_PATH>`/perl Makefile.pl`

Note: Some Perl modules are dependent on C/C++ code libraries. In order to install such modules, you have to install the gcc compiler so that you can link against the libraries. This can also be obtained from www.sunfreeware.com.

3. Configure CA Spectrum to use the custom Perl install.

   See Configuring CA Spectrum to Use a Custom Perl Install (see page 65) and point CA Spectrum to the perl install area from Step 1 above.

On Linux

1. Install Perl.

   The OS already has Perl installed (check /usr/bin/). This pre-installed Perl can be used for Network Configuration Manager scripts.

2. Install SSH-based perl modules and the SSH program.

   You will need to download and install the Net::SSH::Expect module, its dependent modules and the ssh utility.

   The dependency tree for Net::SSH::Expect looks like:

   Net::SSH::Expect -> Expect -> IO::Pty

   where the '->' represents a "requires" relationship.

   You can download all of these modules from www.cpan.org

   Be sure to install these modules to the custom Perl area you installed above.

   This can be done by specifying the full-path of the perl binary when you are installing the modules such as:

   <PERL_FULL_PATH>`/perl Makefile.pl`

   Note: Some Perl modules are dependent on C/C++ code libraries. In order to install such modules, you have to install the gcc compiler so that you can link against the libraries. You can install the gcc compiler by using rpm to add the latest gcc package.

3. Configure CA Spectrum to use the custom Perl install.

   See Configuring CA Spectrum to Use a Custom Perl Install (see page 65) and point CA Spectrum to the perl install area from Step 1 above.

Configuring CA Spectrum to Use a Custom Perl Install

CA Spectrum is configured by default to use the Perl that is shipped with it. If you want to use additional perl modules that are not shipped with CA Spectrum, and have installed them to a perl area, you can configure CA Spectrum to use your custom perl install. To set this up, click the Configuration Manager model in the Explorer tab in OneClick. In its Information view, expand the Perl Configuration subview. You will find a table that contains the Perl directory configuration per landscape.

Note that the Use Custom Perl option has to be set to Enabled to be able to specify a custom perl directory. Otherwise, the default Perl that comes with CA Spectrum is used. You can point CA Spectrum to a custom Perl location that you have installed on a particular SpectroSERVER system.

Follow these steps:

1. On a given landscape, set the Use Custom Perl to Enabled.
2. Once you have enabled the use of a custom Perl area, specify the Custom Perl Directory.

   Note: The Custom Perl directory must contain the full pathname of the directory that contains the perl.exe (Windows) or the perl program (Solaris/Linux).

For example, if the perl program is located in /usr/local/bin/, specify Custom Perl Directory as /usr/local/bin.

Note: You can continue to use the CA Spectrum default scripts once you have configured CA Spectrum to use your custom Perl install. But your custom Perl area must have the Net::Telnet perl module installed. You can download and install this module from www.cpan.org. Otherwise, the CA Spectrum default scripts fail.

You can also disable the use of your custom Perl area and use the default CA Spectrum Perl.

Set the Use Custom Perl to Disabled (use CA Spectrum default). Note that when you disable the use of a custom Perl area, the Custom Perl Directory cannot be seen or edited. But when you enable Use Custom Perl again, your previously specified Custom Perl Directory will be restored.

Using Additional Perl Modules

If you want to use scripts based on your preferred perl module, you must install the perl module to the area that will be used.

On Windows

Depending on the module that you want to use you have three options:

- If the perl module is compatible with a version of Perl other than Cygwin, then we recommend that you install that specific Perl onto your SpectroSERVER machine, then install your specific perl module and then configure CA Spectrum to use your particular Perl install. (See Configuring CA Spectrum to Use a Custom Perl Install (see page 65)).
- If the perl module that you want to install is only compatible with Cygwin's perl, and is a text-based module (i.e., it does not require compilation of C libraries), then you can add it to the CA Spectrum Perl install. Just place the <*Module_Name*>.pm file in

  $SPECROOT/NT-Tools/SRE/lib/perl5/site_perl/5.8
- If the perl module that you want to install is only compatible with Cygwin's perl and also requires C libraries to be compiled, then this module will have to be compiled and shipped with CA Spectrum. Contact CA Spectrum support for this enhancement request.

On Solaris and Linux

It is required that you install Perl to a separate area on your SpectroSERVER, then install the required perl modules using that Perl and configure CA Spectrum to use the Perl install area. Once you have installed Perl, refer to the installation instructions of the specific perl module that you want to install. Then refer to Configuring CA Spectrum to Use a Custom Perl Install (see page 65). You may refer to the Using SSH-based Perl Scripts for Network Configuration Manager Operations (see page 62) for details about how to use scripts based on the Net::SSH::Expect module but you may use the procedure as a guideline for integrating any perl module.

Import and Export Scripts

Network Configuration Manager lets you import and export scripts in bulk. The scripts are exported to or imported from the file system of the host server that is running the OneClick client.

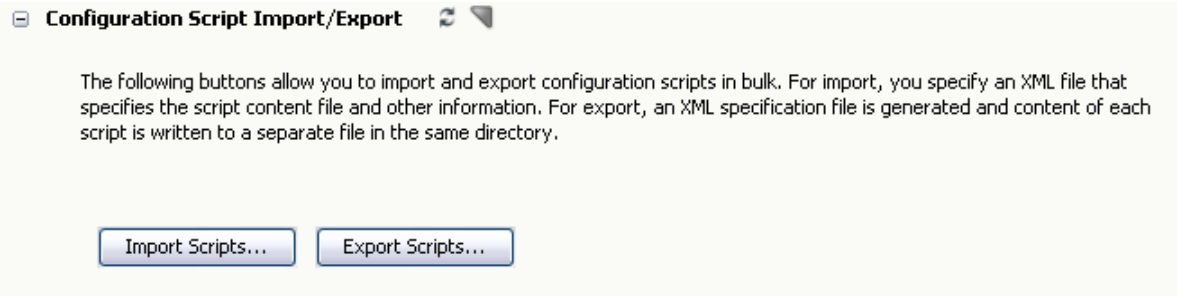
Follow these steps to export scripts:

1. Select Configuration Manager in the Navigation panel.
2. Select the Information tab in the Contents panel.

   Information and configurations display.

3. Expand the Configuration Script Import/Export subview.

   The Import Scripts and Export Scripts buttons display.



4. Click Export Scripts.

   The Select Scripts To Export dialog opens.

5. Select the script to be exported. Or select multiple scripts.

   The Save as dialog opens.

6. Select the location to save, and supply a name for the XML specification file that is automatically generated during export. The export process generates a file for each selected Perl script using its designated name and the .pl extension. The export process also generates the XML specification file that contains the list of scripts that were exported and the error mapping information for each. The XML specification file can then be used to import the scripts on the same or different CA Spectrum environment.

   The selected Perl scripts are exported to the location that you specified.

Follow these steps to import scripts:

1. Select Configuration Manager in the Navigation panel.
2. Click the Information tab in the Contents panel.

   Information and configurations display.

3. Expand the Configuration Script Import/Export subview.

   The Import Scripts and Export Scripts buttons display.

4. Click Import Scripts.

   The open dialog opens.

5. Select the XML specification file that describes the Perl scripts to be imported into Network Configuration Manager. If you are importing scripts that were previously exported from CA Spectrum, you can use the XML specification file that was generated during that export.

The XML specification file may also be generated manually by following the format shown in the following example.

```
<scripts>
  <script>
    <file-name>ABC_Vendor_Capture_Running_Configuration.pl</file-name>
    <display-name>ABC Vendor Capture Running Configuration</display-name>
    <error-message errorCode="255">Usage</error-message>
    <error-message errorCode="99">Invalid Enable Password</error-message>
    <error-message errorCode="98">Unexpected Response</error-message>
    <error-message errorCode="97">Illegal Telnet Timeout Value</error-message>
  </script>
  <script>
    <file-name>XYZ_Vendor_Capture_Running_Configuration.pl</file-name>
    <display-name>XYZ Vendor Capture Running Configuration</display-name>
    <error-message errorCode="255">Usage</error-message>
    <error-message errorCode="99">Response Timed out</error-message>
    <error-message errorCode="50">Connection Error</error-message>
  </script>
  <script>
    <file-name>XYZ_Vendor_Capture_Startup_Configuration.pl</file-name>
    <display-name>XYZ Vendor Capture Startup Configuration</display-name>
  </script>
</scripts>
```

file-name

The name of the Perl file to be imported. This file must exist in the same directory as the XML specification file at the time of import.

display-name

The name that is used in OneClick to identify this script.

error-message

(Optional) Describes a mapping of an error code that is returned by the script to a textual error message that is displayed in OneClick if the error occurs. Multiple error-message elements can be specified for each script.

The Perl script XML is imported. The scripts will be available when configuring Network Configuration Manager operations on device families.

Note: The import process does not associate the scripts with a device family.

Maintaining a Script Backup and History

Scripts are stored as models in the CA Spectrum database and therefore are backed up each time CA Spectrum performs a backup. The script export feature provides an additional backup and means of tracking the history of Network Configuration Manager scripts that is easily accessed and imported back into CA Spectrum if desired.

Customized Traps

You can extend the functionality of Network Configuration Manager by configuring customized trap settings for your installation. These settings are used to correlate configuration change event information so that events are combined for a particular device. These settings are configured at the device family level. For more information, see Configure Notification Trap Settings (see page 45).

Chapter 3: Global Synchronization Task

This chapter describes how to set up the Global Synchronization task on your network with Network Configuration Manager. When you run the Global Synchronization task, Network Configuration Manager captures and saves all device configurations.

Note: We recommend that you capture device configurations prior to configuring Network Configuration Manager policies.

This section contains the following topics:

About Global Synchronization

A Global Synchronization task gathers running configurations for the devices on your network that have Network Configuration Manager enabled. You can schedule this task to run regularly. You select a time period and recurrence frequency to capture configurations from all network-wide supported devices. For example, capture device configurations after 9 PM and no later than 5 AM on a daily basis. By capturing the configurations for all devices on your network, you maintain a running configuration history.

You can set Global Synchronization to verify whether the startup configurations are the same as the running configurations. If they differ, you can configure Network Configuration Manager to generate an alarm. A Global Synchronization captures the startup configuration and compares it to the running configuration to detect changes. See Types of Configurations (see page 15) for descriptions of startup and running configurations.

Note: You can also gather running configurations for selected devices on your network and view the results in real time by creating an automatic Sync task. See Create Sync Task (see page 94) for details.

About Enterasys/Riverstone SSR Devices

Configuration captures performed on Enterasys/Riverstone SSR devices provide the startup configuration and not the running configuration. Therefore, the device configuration history maintained by Network Configuration Manager is a history of the startup configurations on SSR devices. See Determine How an Enterasys/Riverstone SSR Device Responds to an Upload Task (see page 93) for details about how SSR devices handle Network Configuration Manager configuration uploads.

Configure Global Synchronization

Configure settings for Global Synchronization, such as a schedule. Global Synchronization is performed by the Global Sync Task, which appears under Tasks in the Explorer tab.

Follow these steps:

1. Select Configuration Manager in the Explorer tab.

   Information and configurations display in the Information tab of the Contents panel.

2. Expand the Global Synchronization subview.

   Global Synchronization options appear.

3. Modify the following options as needed:

   Global Synchronization Schedule

   Specify a schedule for the Global Sync Task. Click the Schedule button to access the Select Schedule dialog from which you can select a default schedule or create a custom one. More information on scheduling the Global Sync Task is available in Schedule Global Synchronization (see page 73).

   If Sync Task Not Completed in Allotted Time, Assert Task Alarm

   Specify a minor, major, or critical alarm if you want to be notified by alarm if the global synchronization task did not complete properly. If you manage many devices and run a scheduled global sync task periodically, a Sync task stops at the end of the scheduled period because capturing configurations can consume bandwidth on slow links.

   Include Devices and Device Families on which NCM has been Disabled

   Specify whether to include in the Failed Device List those devices for which Network Configuration Manager has been disabled.

   Default: Yes

Verify Startup Equals Running Configuration

Enable this option if you want to compare a startup configuration against a currently running configuration for devices in your network.

When Startup Differs, Assert Device Alarm

Specify a minor, major, or critical alarm if you want to generate an alarm for devices with startup configurations that differ from running configurations.

Schedule Global Synchronization

You can schedule a global synchronization to gather running configurations for all devices on your network. Devices are processed in random order.

If a scheduled global synchronization does not complete in the allotted time, the next execution first randomly processes the unprocessed devices from the previous execution. All remaining devices are then processed in random order.

Important! Do not schedule a "one-shot" global synchronization if CA Spectrum landscapes exist in multiple time zones. Performing this type of task causes the global synchronization to run only in the earliest time zone.

Follow these steps:

1. In Explorer, select Global Sync Task in the Tasks folder.
2. Select the List tab in the Contents panel.
3. Click the Schedule button in the toolbar.

   The Select Schedule dialog opens.
4. Take one of the following steps:
   - Select a default schedule and click OK.
   - Create a custom schedule. Click Create, specify schedule options, and click OK.

     The custom schedule is added to the list of available schedules. Select the new schedule and click OK.

   The Global Sync Task is now scheduled. The schedule appears in the Schedule column of the List table, and the schedule icon appears next to the task in the Tasks folder.

Run an On-Demand Global Sync Task

Run a Global Sync task to gather running configurations for all devices on your network. Devices are processed in random order.

Follow these steps:

1. In Explorer, select Global Sync Task in the Tasks folder.
2. Select the List tab in the Contents panel.
3. Click the Start Selected Task icon.

   The Sync Task Results dialog shows a list of processed devices and the results of the Global Sync.

View Configuration History for a Single Device

You can view the configuration history for a single device in OneClick. For details about uploading configurations to network devices, see Manually Upload Configurations to a Single Device (see page 85).

Follow these steps:

1. Select a device in the Explorer tab.
2. Verify that the List tab is selected in the Contents panel, and select the Host Configuration tab in the Component Detail panel.

   The following details appear in the Host Configuration table:

   Capture Time

   Lists the time (M-DD-YYY HH:MM:SS) that configuration in this row was first captured on the device.

   Captured By

   Identifies the CA Spectrum OneClick user who configured the task.

   Line Changes

   Lists the number of relevant changed lines when compared with the previous configuration on the device. Relevant changes include added lines, removed lines, and changed lines. Irrelevant changes are any lines that match the comparison mask. The comparison mask is managed in Mask Configuration settings for the device family. For more information, see Configure Device Family Masks (see page 43).

   Total Line Changes

   Lists the total number of changed lines (relevant and irrelevant) when compared with the previous configuration on the device. Displays the changes hyperlink if any changes are detected.

Is Reference

Indicates the reference configuration for this device.

Running vs. Startup

Shows configuration differences in the startup and running configuration files (if applicable). Displays the View Differences hyperlink if differences exist.

Last Verified Time

Lists the last time (M-DD-YYY HH:MM:SS) Network Configuration Manager verified that the configuration still existed on the device.

Last Verified User

Identifies the last user to have accessed the device.

NCM Mode

Identifies the method that was used to transfer new configuration content to the device when a change was initiated with Network Configuration Manager.

NCM User

Identifies the CA Spectrum user who initiated the configuration change on the device using Network Configuration Manager.

Device User

Identifies the user who accessed the device and made the configuration change.

Source

Identifies the source of the configuration change.

Location

Identifies the location of the configuration change.

Violated Policies

Identifies policies that were in violation after this configuration change.

Compliant Policies

Indicates policies that were compliant after this configuration change.

A new row is created when one or more changes are detected by Network Configuration Manager.

3. Select a row in the Host Configuration table.

   The captured host configuration content appears in the box below the table.

4. (optional) Click the changes hyperlink (if applicable) in the Line Changes column in the Host Configuration table to view added, removed, changed, and irrelevant lines in the configuration of the selected device.

   The Configuration Differences dialog opens. The highlighted text uses the following colors to indicate status:

   - **Green—**These lines were added.
   - **Red—**These lines have been removed.
   - **Blue—**These lines have changed.
   - **Grey—**These lines are irrelevant. Irrelevant changes are lines that match the comparison mask.

   Note: Click Next or Previous to navigate through the differences in the file.

5. (optional) Click the View Differences hyperlink (if applicable) in the Running vs. Startup column in the Host Configuration table to view added, removed, changed, and irrelevant lines.

   The Running vs. Startup dialog displays differences in running and startup configuration files for the captured device. The startup configuration appears in the right column. The highlighted text uses the colors listed in the previous step to indicate status.

Compare Any Two Configurations

You can compare any two host configurations, even if they belong to different devices.

Follow these steps:

1. Select a device in the Explorer tab.
2. Verify the List tab is selected in the Contents panel and select the Host Configuration tab in the Component Detail panel.
3. Right-click a configuration in the Host Configuration table that you want to compare and select Start Compare.
4. Select the second configuration to include in the comparison. Select a configuration for the same device, or select a different device in the Explorer tab. Verify that its configuration information is displayed in the Host Configuration table.

5. Right-click the second configuration to include in the comparison in the Host Configuration table, and select Compare With <*name_of_first_configuration*>.

   The Configuration Differences dialog opens. The highlighted text uses the following colors to indicate status:

   - **Green—**These lines were added.
   - **Red—**These lines have been removed.
   - **Blue—**These lines have changed.
   - **Grey—**These lines are irrelevant. Irrelevant changes are lines that match the comparison mask.

   Note: Click Next or Previous to navigate through the differences in the file.

Specify a Reference Configuration

You can specify a reference configuration for a device with an associated alarm. An alarm can be generated on the device whenever Network Configuration Manager determines that the current configuration differs significantly from the reference.

Note: For more information about alarm settings, see Configure Configuration Change Alert (see page 29).

Follow these steps:

1. Select a device or device family in the Explorer tab.

   Verify the List tab is selected in the Contents panel.

2. Select one or more devices in the List tab whose most recent configuration you want to set as a reference.

3. Right-click the selection and select Set NCM Reference Configuration.

   A confirmation dialog opens.

4. Select Yes.

   The most recent configuration is set as reference for each device selected. The 'Is Reference' field in the Host Configuration table displays a check and the user who set the reference.

You can also manually specify a reference configuration.

Follow these steps:

1. Select a device in the Explorer tab.

   Verify the List tab is selected in the Contents panel and select the Host Configuration tab in the Component Detail panel.

2. Right-click the configuration to use as reference and select Set Reference.

   The configuration is designated as the reference configuration for this device. A check and the user who set the reference appear in the Is Reference field in the Host Configuration table.

You can change or remove a reference configuration specification after you set it. Only one configuration can be set as the reference configuration for a device. If you use the Set Reference or the Set NCM Reference Configuration option on another configuration when one is already set, the original one is automatically cleared, and the new one becomes the designated reference configuration. To clear a reference configuration, use the Unset Reference command from the right-click menu for the configuration in the Host Configuration table.

Configuration Alarms

You can specify alarms to be triggered when certain configuration changes occur. This section describes how to view the differences between configurations that triggered an alarm.

For more information about determining when configuration change alarms are triggered, see Configure Configuration Change Alert (see page 29) and Specify Configuration Change Alert Settings on a Single Device (see page 49).

View Reference and Running Configuration Differences

You can view and compare reference and current running differences for a single device from the Alarm Details tab.

Follow these steps:

1. Select a device, a device family, or a global collection from the Explorer tab.
2. Select the Alarms tab in the Contents panel.

   Alarms for the selected item are displayed.
3. Select an alarm that displays “Reference and Current Running Configurations are Different” in the Alarm Title column.
4. Select the Alarm Details tab in the Component Detail panel.

   Alarm details are displayed.
5. Click the View Differences hyperlink.

   The Configuration Differences screen displays differences in the reference and current running files for the captured device. The reference configuration appears in the right column.

View Startup and Running Configuration

You can view and compare startup and running configuration for a single device from the Alarm Details tab.

Follow these steps:

1. Select a device, a device family, or a global collection from the Explorer tab.
2. Select the Alarms tab in the Contents panel.

   Alarms for the device, device family, or global collection are displayed.
3. Select an alarm that displays “Startup and Running Configurations are Different” in the Alarm Title column.
4. Select the Alarm Details tab in the Component Detail panel.

   Alarm details are displayed.
5. Click the View Differences hyperlink.

   The Running vs. Startup screen displays differences in running and startup configuration files for the captured device.

   The startup configuration appears in the left column.

View Global Sync Task Results

You can view lists of devices for which global synchronizations failed and succeeded.

Note: You can control whether to include devices with Network Configuration Manager disabled in the Failed Device List. For more information, see Configure Global Synchronization (see page 72).

Follow these steps:

1. Expand Configuration Manager, and select Tasks in the Explorer tab.
2. Select the Global Sync Task.

   Information and results appear in the Information tab of the Contents panel.
3. Enter a name, type, condition, or device family in the Filter field to filter the results lists.

Network Configuration Manager Reports from Report Manager

Network Configuration Manager report options are included under the Network Configuration Management report pack in CA Spectrum Report Manager. Report Manager provides numerous report content, format, and report organization options. As a result, you can generate reports with the appropriate type and scope of information for different audiences in your organization who are interested in device configuration changes.

Report Manager Options

Report Manager provides you with multiple options for generating and managing your Network Configuration Manager reports:

- Generate reports on demand to view the most recent test results.
- Schedule test report generation on a one-time or periodic basis.
- Specify how long you want Report Manager to retain scheduled test reports or how many reports to retain.
- Specify email recipients for scheduled test reports.
- Schedule test reports for other Report Manager users.
- Publish reports in PDF, text, and spreadsheet formats.

Note: For detailed information about Report Manager features, see the *Report Manager User Guide*.

The following reports are available:

Configuration Changes: All

Displays a summary of changes for all devices that have configuration changes. Each row represents a device to be associated with data that describes its configuration changes.

Configuration Changes: Group

Displays a summary of changes for devices in a given global collection. Each row represents a device to be associated with rolled up statistics describing its configuration changes.

Configuration Changes: Individual Device

Displays a list of configuration changes on a given device. Each row displays the time of the change, who made the change, and how many lines were changed. In addition, each row contains a web link to a Java applet that displays the difference between the current configuration and the previous configuration.

Detailed Configuration Event Log: All

Displays a reverse chronological list of events for all devices and models within CA Spectrum with Network Configuration Manager activity. Each entry in the list includes the IP address (if applicable), event text, event code, and event creator.

Detailed Configuration Event Log: Group

Displays a reverse chronological list of events for all devices and models with Network Configuration Manager activity for a specified global collection. Each entry in the list includes the IP address (if applicable), event text, event code, and event creator.

Detailed Configuration Event Log: Selected Device or Model

Displays a reverse chronological list of events for a specified device or model with Network Configuration Manager activity. Each entry in the list includes the IP address (if applicable), event text, event code, and event creator.

Top-N Configuration Changes: All

Displays a summary of changes for the "Top-N" devices that have configuration changes, where "Top-N" is defined as the maximum number of records based on the current sorting criteria. Each record represents a device to be associated with rolled-up statistics that describe its configuration changes.

Top-N Configuration Changes: Group

Displays a summary of changes for the "Top-N" devices that have configuration changes in a global collection. The "Top-N" is defined as the maximum number of records based on the current sorting criteria. Each record represents a device to be associated with rolled-up statistics that describe its configuration changes.

Generate Network Configuration Management Reports with Report Manager

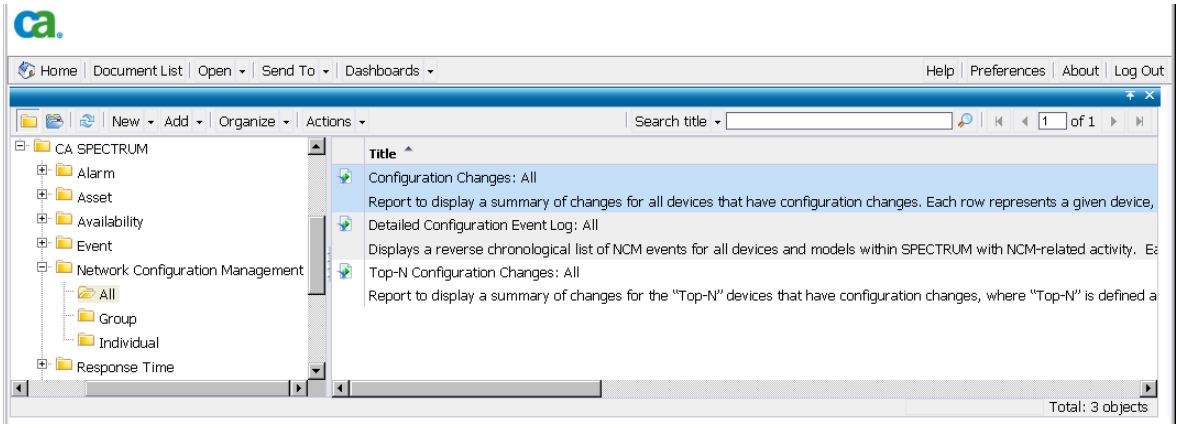
You can generate Network Configuration Management reports using the CA Spectrum Report Manager.

Note: The following example only provides an overview of the Network Configuration Management reports and features available in Report Manager. For more information, see the *Report Manager User Guide.*

Follow these steps:

1. Select the type of test to generate.

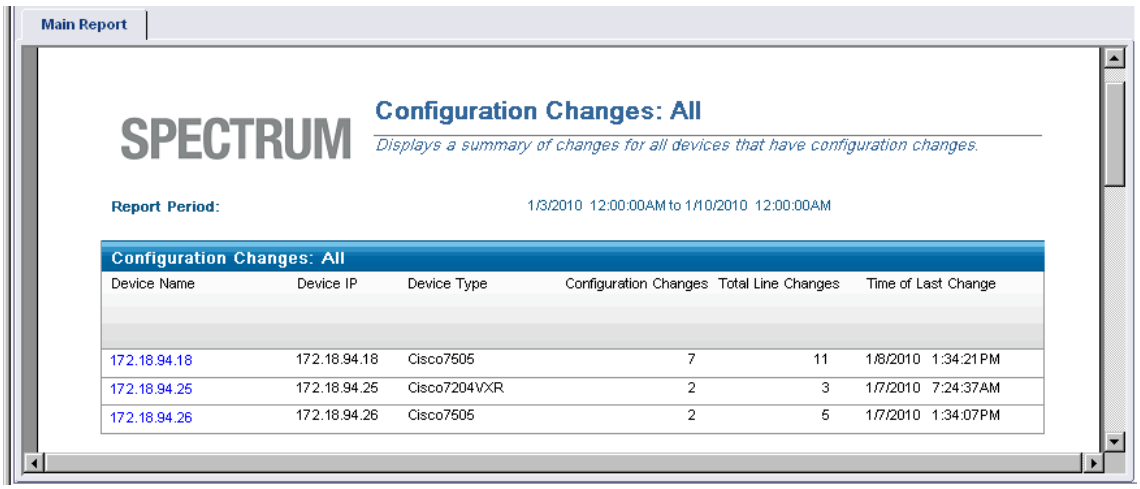
   The following image shows the Network Configuration Management report options:



2. Configure the report. Select options for date and time range, supply a report title and subtitle, and select the landscape.

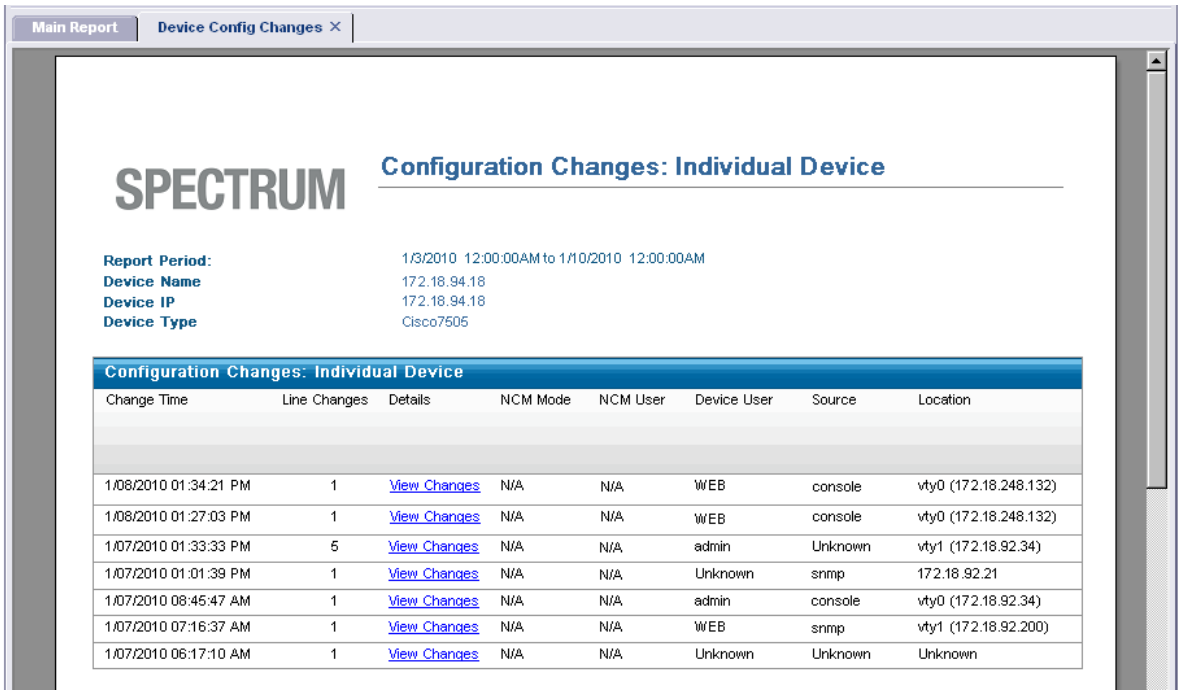
3. Click View Report to generate the report.

   The report displays. The following image shows an example of report results:



4. Click a Device Name hyperlink to examine results at the device level.

   The following image shows an example. From this view, you can click the View Changes hyperlink to view added, removed, changed, and irrelevant lines in the configuration of the selected device.



Chapter 4: Network Configuration Manager Device-Level Tasks

This chapter describes how to manually capture, export, and upload configurations for devices in your network using Network Configuration Manager.

This section contains the following topics:

Manually Capture Configurations

Network Configuration Manager attempts to capture device configurations immediately after any change occurs. An unsolicited notification of configuration change can be either traps or MIB objects that are sent from the device where the change occurred. When it receives an unsolicited notification, the SpectroSERVER performs a capture and saves the configuration in the database to provide updated configuration data. You can also manually capture device configurations in OneClick.

Follow these steps:

1. Select a single device in the Explorer tab.

   The device appears in the List tab of the Contents panel.

2. Select the Host Configuration tab in the Component Detail panel.

   The results of any previous captures display.

3. Click the Capture Configuration icon.

   The results of the capture appear. Either a new configuration appears in the list or the last verified time is updated for the current configuration.

Manually Upload Configurations to a Single Device

You can manually upload a configuration file to a single device on your network. When you upload a configuration file, you merge it into the existing configuration file. You can use this feature to bring a newly installed device or a replacement/standby remote device quickly online.

When uploading to a device in the Juniper JUNOS device family, use JUNOScript API format. For more information, see Juniper JUNOS Devices (see page 20).

Note: You can upload configurations and view the results in real time by creating a bulk Upload task. For more information, see Create Upload Task (see page 91).

Approval Not Required

The process to upload a device configuration to a single device varies depending on whether approval workflow is enabled. The following procedure describes the process when approval is not required.

Note: For information on workflow approval options, see Configure Workflow (see page 31).

Follow these steps:

1. Select a single device or device family in the Explorer tab.

   The device or devices associated with the selected device family appear in the List tab of the Contents panel.

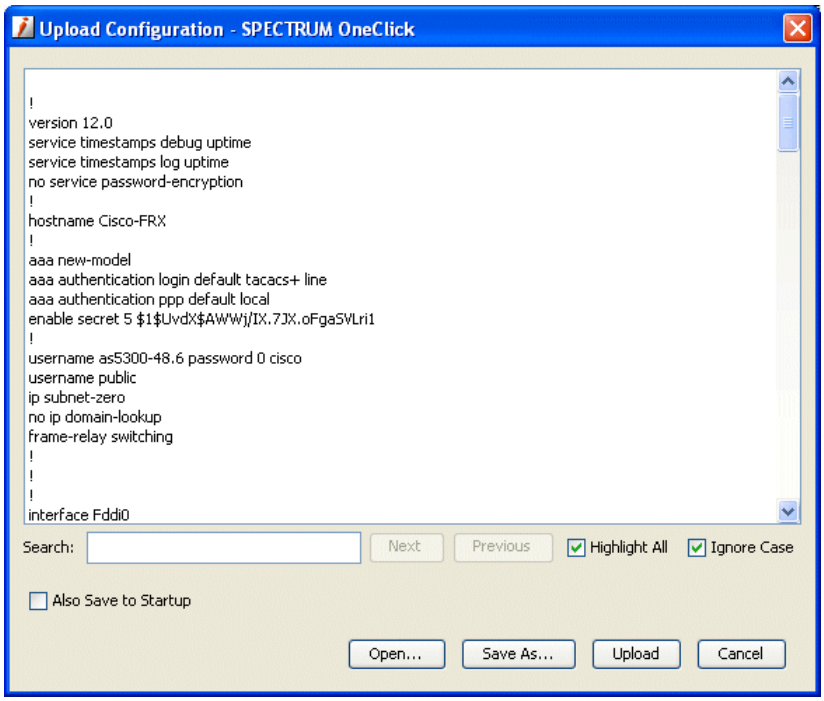
2. Select the Host Configuration tab in the Component Detail panel.

   The results of any previous captures display.

3. Click the Upload icon.

   Note: If approval is required, the Approval Required dialog appears. Go to Approval Required (see page 88) to create a request for approval.

   The Upload Configuration screen appears with the last known configuration information for the selected device as shown in the following example:



4. Perform any of the following optional steps:
   - Edit configuration content as desired.
   - Enter criteria in the Search field to locate specific lines in the configuration file to change content or to verify content prior to an upload.
   - Select Also Save to Startup to write this configuration to the startup configuration. This will cause the configuration file to be loaded into the device when rebooted.

     Note: This feature is only supported for Cisco, Foundry, and Nortel Passport L3 devices.
   - Click Open to import a previously exported configuration file that is saved locally on your system.
   - Click Save As if you want to save and export this configuration file in txt or html format.
5. Click Upload to upload the configuration file to the selected device.

   The message "The configuration upload succeeded" appears when the procedure is complete.

   Note: Scheduling tasks is an available feature of bulk tasks. If you want to schedule your Upload task, see Network Configuration Manager Bulk Tasks (see page 91).

Upload Configurations to a Single Device (Approval Required)

If approval workflow is enabled, your configuration changes must be approved before they can be processed. This is accomplished by creating a task for the upload request which can then be run after approval.

Note: For information on approval workflow options, see Configure Workflow (see page 31).

Follow these steps:

1. Select a single device or device family in the Explorer tab.

   The device or devices associated with the selected device family appear in the List tab of the Contents panel.
2. Select the Host Configuration tab in the Component Detail panel.

   The results of any previous captures display.
3. Click the Upload icon.

   The Approval Required dialog appears.
4. Click Yes to continue.

   The Create NCM Task appears.

5. Create the task as follows:

   a. Enter a unique name in the Name field.

      Note: Network Configuration Manager provides a default name (<*task type*>.YY-MM-DD_HH:MM.<*user name*>). For example, Upload.2006-10-17_15:48:04.Administrator.

   b. Enter a description for the task in the Description field.

   c. Select Reusable Task if you want the task to be available after it has run.

   d. Click Edit to specify content for uploading and merging into the device configuration in the Upload Content box. You can also click Open to import content from a text file. After you have made changes, you can click Save As to save and export this configuration file in txt or html.

   e. (optional) Enter criteria in the Search field to locate specific lines in the configuration file.

   f. Select Commit to Startup (if applicable) to copy the entire running configuration to the startup configuration after new content is merged.

   g. Select Alarm device on failure to generate an alarm on each device on which the task fails.

   h. Click Request Approval.

   The Approval Required dialog appears.

6. Select a user and enter an email address for a Task Approver, enter a task description (optional), and click OK to generate the request.

   A confirmation dialog appears indicating the request creation was successful. An email is sent to the Task Approver and the generated task appears in the Tasks folder in the Explorer tab.

   Note: For email configuration information, see the *Administrator Guide*.

7. Check approval status and run the task as described in Start a Task (see page 112).

Chapter 5: Network Configuration Manager Bulk Tasks

This chapter describes how to create an on-demand bulk Upload task, Sync task, and Save to Startup task with Network Configuration Manager. These tasks interact with devices by capturing and uploading host configurations. You can create a task to run anytime on a single device or on a list of devices. These on-demand tasks are useful if you want to roll out the same configuration (with minor differences such as IP addresses) to multiple devices on your network.

A task can be defined as reusable. A reusable tasks persists after execution and can be run again. If a task is not reusable, once it is run, it is sent to the Lost and Found view and purged within 24 hours.

This section contains the following topics:

Create Upload Task

Create an automatic Upload task to perform bulk configuration uploads. A bulk Upload task merges new content into the running configurations of one or more selected devices. Devices are processed in random order.

Important! If you are uploading to Enterasys/Riverstone SSR devices, see Determine How an Enterasys/Riverstone SSR Device Responds to an Upload Task (see page 93) before continuing with this task. If you are uploading to a device in the Juniper JUNOS device family, you must use JUNOScript API format; for more information, see Juniper JUNOS Devices (see page 20).

Follow these steps:

1. Select a single device, device family, global collection, a search result entry, or a container (such as Universe) in the Explorer tab.
2. Click the List tab and select the devices for the Upload task.
3. Select Upload Task from the Create NCM Task icon on the toolbar.

   The Upload Task dialog opens.

   Note: If the selected devices do not appear in the Allow tab, click Disallow to display devices that are either disabled from Network Configuration Manager tasks or lack the necessary privileges.

4. Click Continue.

   The Create Task dialog appears.

5. Enter task information as follows:

   a. (Optional) Enter a unique name in the Name field.

      Note: Network Configuration Manager provides a default name (<*task type*>.YY-MM-DD_HH:MM.<*user name*>). For example, Upload.2006-10-17_15:48:04.Administrator.

   b. (Optional) Enter a description for the task in the Description field.

   c. Select Reusable Task to make the task reusable.

   d. Click Edit to specify content for uploading and merging into the device configuration in the Upload Content box. You can also click Open to import content from a text file. After you have made changes, you can click Save As to save and export this configuration file in txt or html.

   e. Enter criteria in the Search field to locate specific lines in the configuration file.

   f. Select Commit to Startup (if applicable) to copy the entire running configuration to the startup configuration after new content is merged.

   g. Select Alarm device on Failure to generate an alarm on each device on which the task fails.

6. If approval is required (as indicated by the Request Approval button), take the following steps:

   a. Click Request Approval.

      The Approval Required dialog appears.

   b. Select a user and enter an email address for a Task Approver, enter a task description (optional), and click OK to generate the request.

      A confirmation dialog indicates that the request was created successfully. An email message is sent to the Task Approver ,and the generated task appears in the Tasks folder in the Explorer tab.

      Note: For email configuration information, see the *Administrator Guide*.

   c. Check approval status and run the task as described in Start a Task (see page 112).

   Note: For information on approval workflow options, see Configure Workflow (see page 31).

7. If approval is not required (as indicated by the Save button):

   a. Click Save.

      The Task Saved dialog appears.

b. Take one of the following steps:

- Click Upload to upload the task to the selected device.

  The Upload Task Results dialog appears, and the generated task appears in the Tasks folder in the Explorer tab. For more on the results dialog, see View Task Results in Real Time (see page 114).

- Click Schedule to schedule the task for future execution. Scheduling is described in Schedule a Task (see page 110).

  The task is saved and runs according to its schedule.

- Click Close to save the task; it is available to run at a future time. You can edit and run the task by selecting it from Tasks in the Explorer tab under Configuration Manager.

Determine How an Enterasys/Riverstone SSR Device Responds to an Upload Task

Enterasys/Riverstone SSR devices do not respond consistently to configuration uploads. Some of these devices replace both the running and startup configurations with uploaded content. Others merge the uploaded content into both the running and startup configuration. Configuration captures performed on Enterasys/Riverstone SSR devices provide the startup configuration and not the running configuration. Therefore, we recommend testing devices that are running Enterasys firmware to verify the running and startup configurations.

Follow these steps:

1. Select a single SSR device from a search result or container (such as Universe) in the Explorer tab.
2. Click the List tab in the Contents panel.
3. Click the Host Configuration tab in the Component Detail panel.

   Previously captured configurations display.
4. Select the Capture Configuration icon to capture the current configuration of the selected device.
5. Select the Upload icon.

   The Upload Configuration screen appears. The content of the current startup configuration displays in the bottom pane.

6. Edit the existing configuration in the Upload Configuration screen. For example, remove the location line value (or remove a line):
   `system set location "value"`
7. Select the Upload icon again to upload the modified device configuration. Select the Capture Configuration icon again to capture the new configuration from the device.

   If the location is not present in the newly captured configuration, it indicates that the device is replacing (not merging) both the running and the startup configuration with the uploaded content.

Create Sync Task

Create an automatic Sync task to capture and verify policy-compliant device configurations for selected devices on your network and view the results in real time. When a Sync task captures device configuration, it checks the configuration against all policies pertaining to the device and, if specified, against the device startup configuration. Devices are processed in random order.

See Network Configuration Manager Policies (see page 117) for details about Network Configuration Manager policies.

See About Global Synchronization (see page 71) for details about running global sync tasks in background mode.

Follow these steps:

1. Select a single device, device family, global collection, a search result entry, or a container (such as Universe) in the Explorer tab.
2. Click the List tab in the Contents panel and select the devices that you want to include in the Sync task.
3. Click Sync Task from the Create NCM Task icon on the toolbar.

   The 'Select device(s) for Sync Task' dialog opens.

   Note: If the selected devices do not appear in the Allow tab, click Disallow to display devices that are either disabled from Network Configuration Manager tasks or do not have necessary privileges.
4. Enter task information as follows:
   a. Enter a unique name in the Name field.

      Note: Network Configuration Manager provides a default name (<*task type*>.YY-MM-DD_HH:MM.<*user name*>). For example, Sync.2010-09-09_15:48:04.Administrator.

   b. Enter a description for the task in the Description field.

c. Select 'Alarm on device if startup differs' and appropriate severity to generate an alarm on each device where the captured configuration differs from its startup configuration.

d. Click Edit Schedule to schedule the task for future execution. Scheduling is described in Schedule a Task (see page 110).

e. Select Reusable Task to make the task reusable.

5. Take one of the following steps:

   - Click Save to save the task; it is available to run at a future time. You can run the task by selecting it from Tasks in the Explorer tab under Configuration Manager.
   - Click Run Sync Task Now.

     The Sync Task Results dialog opens, and the generated task appears in the Tasks folder in the Explorer tab. For more information, see View Task Results in Real Time (see page 114).

Create a Save to Startup Task

Create an automatic Save to Startup task to write a current running configuration to the startup configuration of one or more selected devices. A device saves its configuration in NVRAM (Nonvolatile Random Access Memory).

Devices are processed in random order.

Follow these steps:

1. Select a single device, device family, global collection, a search result entry, or a container (such as Universe) in the Explorer tab.
2. Click the List tab in the Contents panel and select the devices to upload.
3. Click Save to Startup Task from the Create NCM Task icon on the toolbar.

   The Save to Startup Task dialog opens.

   Note: If the selected devices do not appear in the Allow tab, click Disallow to display devices that are either disabled from Network Configuration Manager tasks or lack the necessary privileges.

4. Enter task information as follows:
   a. (Optional) Enter a unique name in the Name field.

      Note: Network Configuration Manager provides a default name (<task type>.YY-MM-DD_HH:MM.<user name>). For example, WriteStartup.2006-10-17_15:48:04.Administrator.

   b. (Optional) Enter a description for the task in the Description field.

   c. Select Reusable Task to make the task reusable.

5. If approval is required (as indicated by the Request Approval button), take the following steps:
   a. Click Request Approval.

      The Approval Required dialog appears.

   b. Select a user and enter an email address for a Task Approver, enter a task description (optional), and click OK to generate the request.

      A confirmation dialog indicates that the request was created successfully. An email is sent to the Task Approver and the generated task appears in the Tasks folder in the Explorer tab.

      Note: For email configuration information, see the *Administrator Guide*.

   c. Check approval status and run the task as described in Start a Task (see page 112).

   Note: For information about approval workflow options, see Configure Workflow (see page 31).

6. If approval is not required, take any of the following steps:
   - Click Schedule to schedule the task for future execution. Scheduling is described in Schedule a Task (see page 110).
   - Click Save.

     The task is saved for future execution.
   - Click Run Save to Startup Task Now.

     The Save to Startup Task Results dialog opens, and the generated task appears in the Tasks folder in the Explorer tab. For more information, see View Task Results in Real Time (see page 114).

Note: Any “Startup Versus Running Configurations are Different” alarms on task devices are automatically cleared by this task. For more information, see View Startup and Running Configuration Differences (see page 79).

Chapter 6: Firmware Upload

This section describes how to upload firmware for Cisco IOS and Cisco IOS - SSH Capable devices. Uploading firmware can be accomplished by either of two methods:

- Using the Load Firmware task
- Using Extension Utility scripting

Important! Uploading firmware is an advanced user feature and requires an expert level of knowledge. Modifying device firmware incorrectly may leave the device in an inoperative state.

This section contains the following topics:

About Firmware Upload

Firmware Upload is supported in that if a script is present it will use the script. If no script is present and the device supports the CISCO-FLASH-MIB, the MIB will be used.

Firmware Upload must accomplish certain tasks successfully and in a specific order for the transfer to be successful. This section describes these tasks and the firmware upload process.

Note: These tasks are handled by the Load Firmware Task, which is described in Create Load Firmware Task (see page 100), or by a custom script.

These tasks are:

1. **Upload firmware image from the server to the device.** The device must be instructed to load the firmware image from a well-known server (the image server) to a specified flash or file system name. This upload can take minutes to hours to complete depending on the size of the image file and the network bandwidth.

2. **Upload boot command configuration to the device.** This occurs in three steps:
   a. Capture configuration. The configuration must be captured so that the new command can be inserted into the current configuration.
   b. Upload change.
   c. Write to NVRAM. The modified configuration must be written to startup so that the device will reload the specified image at boot time.
3. **Run reload script.** The reload command is written directly to enable mode and is not part of the configuration.

The system will use the default protocols or an override script for each phase as appropriate.

Important! If an error occurs in any of these steps, there is no rollback. The device is left in the last successful state.

Privileges

When uploading firmware as described in these sections, the following Network Configuration Manager privileges may be required:

- Load the Device Firmware
- Reload Device
- Schedule a Reload

For more information, see Network Configuration Manager Privileges (see page 223).

Configure Device Firmware Transfer Settings

The section describes how to configure the protocol and server settings used to transfer the firmware image to the device. These settings are made at the device family level and reside in the Device Firmware Transfer Settings subview, which is available for the Cisco IOS and Cisco IOS - SSH Capable device families only. The devices in these device families support the CISCO-FLASH-MIB.

Note: Firmware Upload is supported out-of-box for Cisco IOS and Cisco IOS - SSH Capable device families only. For all other devices, the Extension Utility may be used to specify a Load Device Firmware script. See Network Configuration Manager Extension Utility (see page 53) for more information.

Follow these steps:

1. Select the Cisco IOS or Cisco IOS - SSH Capable device family from Device Families in the Explorer tab.

   Information and configurations appearin the Information tab of the Contents panel.

2. Expand the Device Firmware Transfer Settings subview.

   Firmware transfer options let you configure a firmware image transfer from a server or provide a custom script.

3. Take one of the following steps:

   - Modify the Firmware Image Transfer Protocol as needed.
   - Enter a Load Device Firmware script. For details on entering a script, see Enter a Configuration Script (see page 58).

   Important! If a script is present, the script is used, regardless of what is specified for the Firmware Image Transfer Protocol.

Display Cisco Flash Partition Information

In order to successfully upload a new firmware image to a device, you must have enough disk space available to support the image. This section describes a convenient way to review the available resources on a device before attempting a firmware upload.

Note: You can also display partition information for the device when creating the Load Firmware Task using the View Partitions button on the Create NCM Task dialog. For more information, see Create Load Firmware Task (see page 100).

To display Cisco flash partition information

1. Select a device from either the Cisco IOS or Cisco IOS - SSH Capable device families in Device Families in the Explorer tab.

   Information and configuration settings for the device display in the Information tab of the Contents panel.

2. Expand the Cisco Flash Partitions subview.

   The following information appears:

   Name

   Partition name.

   Number of Files

   Number of files within the partition.

Free Space

Amount of space available in the partition. There must be enough free disk space to support the new firmware image to be uploaded.

Total Space

Total amount of space allocated to the partition.

Create Load Firmware Task

This section describes how to create a Load Firmware task, which is used to upload firmware to Cisco IOS and Cisco IOS - SSH Capable devices.

Note: To complete this task, you need to specify where on the device to upload the new firmware image. The target location must have enough space available to support the new image. To review the available resources on the device before creating the task, see Display Cisco Flash Partition Information (see page 99).

Follow these steps:

1. Select a device from either the Cisco IOS or Cisco IOS - SSH Capable device families in Device Families in the Explorer tab.
2. Click the List tab in the Contents panel and select the devices for the Load Firmware task.
3. Select Load Firmware Task from the Create NCM Task icon on the toolbar.

   The Select Device(s) for Load Firmware Task dialog opens.

   Note: If the selected devices do not appear in the Allow tab, click Disallow to display devices that are either disabled from Network Configuration Manager tasks or do not have necessary privileges.
4. Click Continue.

   The Create NCM Task dialog appears.
5. Create the task as follows:
   a. Enter a unique name in the Name field.

      Note: Network Configuration Manager provides a default name (<*task type*>.YY-MM-DD_HH:MM.<*user name*>). For example, LoadFirmware.2006-10-17_15:48:04.Administrator.

   b. Enter a description for the task in the Description field.

   c. Select Reusable Task to make task reusable.

d. Enter Image Information:

Firmware Image Name

The file name of the firmware image on the image server.

Destination

The file name of the image as it will be on the device. Often this is the same name as that on the server and the value will auto-fill.

Boot Command

The name of the image to boot from. This will auto-fill with the destination name.

Default: boot system flash

Backup Boot Command

The name of the image to boot from if an error occurs. This should be set to the current bootable image on the device. This will auto-fill with the destination name.

Default: boot system flash

Reload the device after firmware upload

If selected, the Reload Information fields are enabled and the device will be reloaded after the firmware upload is successful.

View Partitions

Click View Partitions to display the Device Partitions dialog, which displays the available resources on the device. The target location must have enough space available to support the new image.

e. Enter Reload Information (if applicable):

Reload Immediately

Select Reload Immediately to reload the device immediately after firmware upload is successful. If this option is not selected, use the Timing fields to schedule the reload.

Save to Startup (if modified)

If the running configuration has been modified but not saved, indicate whether to copy it to startup before the reload begins.

Telnet Login Timeout

The timeout value (in seconds) to be used for the telnet connection while attempting to log in to the device.

Telnet Command Timeout

The timeout value (in seconds) to be used while attempting to execute commands over the telnet connection.

f. Click Server Settings and enter the following on the Edit Server Settings dialog to override transfer settings set at the device family level:

Protocol

The protocol to be used.

Server Address

The image transfer server address from which the device will copy the firmware image.

Time out (seconds)

The time out period before the device will fail the copy from the firmware image server.

Image Dir

The subdirectory on the image transfer server from which the file will be served.

Note: This may be required if the images are not served from the root directory of the image server.

User Name

The user name required by the image transfer server.

Note: This may not be required by the specified protocol.

Password

The password required by the image transfer server.

Note: This may not be required by the specified protocol.

6. If approval is required (as indicated by the Request Approval button), take the following steps:

a. Click Request Approval.

The Approval Required dialog opens.

b. Select a user, and enter an email address for a Task Approver.

c. (Optional) Enter a task description, and click OK to generate the request.

A confirmation dialog indicates that the request was created successfully. An email message is sent to the Task Approver and the generated task appears in the Tasks folder in the Explorer tab.

Note: For information about email configuration , see the *Administrator Guide*.

d. Check approval status and run the task as described in Start a Task (see page 112).

Note: For information on approval workflow options, see Configure Workflow (see page 31).

7. If approval is not required (as indicated by the Save button):
   a. Click Save.

      The Task Saved dialog opens.

   b. Do one of the following:
      - Click Upload Firmware to process the task.

        The Load Firmware Task Results dialog opens, and the generated task appears in the Tasks folder in the Explorer tab. For more information, see View Task Results in Real Time (see page 114).
      - Click Schedule to schedule the task for future execution. Scheduling is described in Schedule a Task (see page 110).

        The task is saved and runs according to schedule.
      - Click Close to save the task; it is available to run at a future time. You can edit and run the task by selecting it from Tasks in the Explorer tab under Configuration Manager.

Create Reload Task

Create a Reload task to reload a device after firmware has been uploaded. This task is available for Cisco IOS and Cisco IOS - SSH Capable devices.

Note: The functionality provided by the Reload task is also optionally available in the Load Firmware task.

Follow these steps:

1. Select a device from either the Cisco IOS or Cisco IOS - SSH Capable device families in Device Families in the Explorer tab.
2. Click the List tab in the Contents panel and select the devices for the Reload task.
3. Select Reload Task, Reload Task from the Create NCM Task icon on the toolbar.

   The Select Device(s) for Reload Task dialog opens.

   Note: If the selected devices do not appear in the Allow tab, click Disallow to display devices that are either disabled from Network Configuration Manager tasks or lack the necessary privileges.
4. If approval is required (as indicated by the Request Approval button), take the following steps:
   a. Click Request Approval.

      The Approval Required dialog opens.

b. Select a user, and enter an email address for a Task Approver.

c. (Optional) Enter a task description, and click OK to generate the request.

A confirmation dialog indicates that the request was successfully created. An email message is sent to the Task Approver, and the generated task appears in the Tasks folder in the Explorer tab.

Note: For information about email configuration, see the *Administrator Guide*.

d. Check approval status and run the task as described in Start a Task (see page 112).

When you start the task after it has been approved, the Reload Task dialog appears

Note: For information on approval workflow options, see Configure Workflow (see page 31).

5. If approval is not required, click Run Reload Task Now.

The Reload Task dialog appears.

6. Create the task as follows:

a. Enter Reload Information:

Reload Immediately

Select Reload Immediately to reload the device immediately. If this option is not selected, use the Timing fields to schedule the reload.

Warm

Reload Warm (skip copying the image to NVRAM and uncompressing it).

Save to Startup (if modified)

If the running configuration has been modified, indicate whether to copy it to startup before the reload begins.

Telnet Login Timeout

The timeout value (in seconds) to be used for the telnet connection while attempting to log in to the device.

Telnet Command Timeout

The timeout value (in seconds) to be used while attempting to execute commands over the telnet connection.

b. Click OK.

The Reload Device Task Results dialog opens, and the generated task appears in the Tasks folder in the Explorer tab. For more information, see View Task Results in Real Time (see page 114).

Create Cancel Reload Task

A Cancel Reload task is used to cancel a pending reboot that has been scheduled on a device. This task is available for Cisco IOS and Cisco IOS - SSH Capable devices.

Follow these steps:

1. Select a device from the Cisco IOS or Cisco IOS - SSH Capable device family in Device Families in the Explorer tab.
2. Click the List tab in the Contents panel and select the devices for the Reload task.
3. Select Reload Task, Cancel Reload Task from the Create NCM Task icon on the toolbar.

   The Select Device(s) for Cancel Reload Task dialog appears.

   Note: If the selected devices do not appear in the Allow tab, click Disallow to display devices that are either disabled from Network Configuration Manager tasks or do not have necessary privileges.
4. If approval is required (as indicated by the Request Approval button), take the following steps:

   a. Click Request Approval.

      The Approval Required dialog opens.

   b. Select a user and enter an email address for a Task Approver.

   c. (Optional) Supply a task description.

   d. Click OK to generate the request.

      A confirmation dialog indicates that the request was successfully created. An email message is sent to the Task Approver, and the generated task appears in the Tasks folder in the Explorer tab.

      Note: For information about email configuration, see the *Administrator Guide*.

   e. Check approval status and run the task as described in Start a Task (see page 112).

   Note: For information about approval workflow options, see Configure Workflow (see page 31).

5. If approval is not required, perform any of the following tasks:
   - Click Schedule to schedule the task for future execution. Scheduling is described in Schedule a Task (see page 110).
   - Click Save.

     The task is saved for future execution. Exit this procedure.
   - Click Run Cancel Reload Task Now.

     The Cancel Reload Device Task Results dialog opens, and the generated task appears in the Tasks folder in the Explorer tab. For more information, see View Task Results in Real Time (see page 114).

Load Device Firmware Script

The Load Device Firmware Script can be used to initiate a load of the specified firmware image on a device as an alternative to the internal MIB-based support for Load Firmware Task (only for the Cisco devices that support CISCO-FLASH-MIB). For more information on using scripts, see Network Configuration Manager Extension Utility (see page 53).

Chapter 7: Managing Tasks

This section contains the following topics:

Associating Tasks with Global Collections

Tasks can be associated with global collections. By associating a task with a global collection, the task runs on all members of the collection that support the task type at execution time. Associating a task with a global collection can occur during initial task creation or after the task already exists.

Note: The 'Include Global Collection in NCM Task' privilege is required for a user to associate a task with a global collection. For more information on privileges, see Network Configuration Manager Privileges (see page 223).

More information:

Global Collections (see page 25)

Associate a New Task

You can associate a task with a global collection when you create the task.

Follow these steps:

1. Select the Global Collections node in the Explorer tab.

   A list of defined global collections appears in the List tab of the Contents panel.

   Note: If no global collections exist, you must create one before you can continue. For more information, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

2. On the List tab, select the global collection with which to associate a task.

   The global collection is highlighted and the Create NCM task icon is enabled.

3. Click the Create NCM task icon and select the task that you want to create and associate with this global collection.

   The 'Select device(s)' dialog for the task appears.

4. Continue with the creation of the task as described in Network Configuration Manager Bulk Tasks (see page 91) or Firmware Upload (see page 97), depending on the task.

   When you have finished:

   - The new task appears in the NCM Tasks subview on the Information tab for the global collection.
   - The new task appears in the Tasks folder in the Explorer tab. When viewing the Information tab for the task, the global collection with which the task is associated appears in the Global Collections subview.

   When the task is executed, it runs on all members of the global collection that support the task type at the time of execution.

Associate an Existing Task

You can associate an existing task with a global collection, and you can also perform the association while creating the task (see page 107). The following procedure can be used to add another global collection to an existing task or to remove a collection.

Follow these steps:

1. Select the task from the Tasks folder under Configuration Manager in the Explorer tab.

   Information for the task appears in the Information tab of the Contents panel.

2. Expand the Global Collections subview.

   Any global collections that are associated with the selected task appear in the table.

3. Click the Add or Remove Global Collections icon above the table.

   The Task Members Editor dialog opens.

4. Select global collections from the Available Global Collections pane (on the right). Use the arrows to move them into the Associated Global Collections pane (on the left) to be associated with this task.

   Global collections that are in the Associated Global Collections pane will be associated with this task.

5. Click Save, and then Yes in the subsequent confirmation dialog.

   The associated global collections appear in the table. When the task is executed, it will run on all members of the associated global collections that support the task type at the time of execution.

Scheduling Bulk Tasks

Bulk tasks can be scheduled. Scheduling can be accomplished either at the time of creation of a task or after the task has run (in the case of reusable tasks).

The following tasks can be scheduled: Upload Task, Sync Task, Save to Startup Task, Load Firmware Task, and Cancel Reload Task.

Note: Reload tasks cannot be scheduled through this mechanism; instead, the internal scheduling mechanism of a device is used. If you define a script to accomplish the reload operation, the script must leverage the scheduling mechanism of the device to schedule reload tasks. For more information, see Enter a Configuration Script (see page 58).

A task can be associated with only one schedule. If a task already has an existing schedule when a new schedule is specified, the previous schedule is removed. You must manually delete recurring tasks; no automatic cleanup is performed.

Tasks are essentially distributed. Each "local" task runs at the scheduled time, based on the local time zone of the local landscape. The recommended best practice is to have all SpectroSERVERs working with the same time zone setting. The Time Completed column in the Succeeded Device List and Failed Device List tables show at what time the task operation was attempted on a particular device. This capability can help determine the time when a task is run in a DSS with multiple landscapes in different time zones.

Note: The Network Configuration Manager Schedule NCM Tasks privilege is required to schedule bulk tasks.

Reusable Tasks

Defining a task as reusable allows you the ability to save and run a task multiple times without having to redefine it. You can also create a recurring schedule to automatically run the task at predetermined times.

For information on scheduling a task, see Schedule a Task (see page 110).

Note: A task with a recurring schedule will automatically be created as a Reusable task.

A task is designated as reusable when the Reusable Task option is specified during task creation.

The task is identifiable as reusable in following areas:

- In the Reusable field in the List table in the Contents panel
- Within General Task Information in the Information tab in the Component Detail panel

Schedule a Task

Scheduling a task lets you define a task and then specify a future date and time when it runs. Schedule a task to run one time only or on a recurring basis. You can set up the schedule at the time of task creation. Use the Schedule or Edit Schedule button. Or, for reusable tasks, you can set up a schedule at any time.

Note: Tasks run from the Host Configuration tab cannot be scheduled.

Follow these steps:

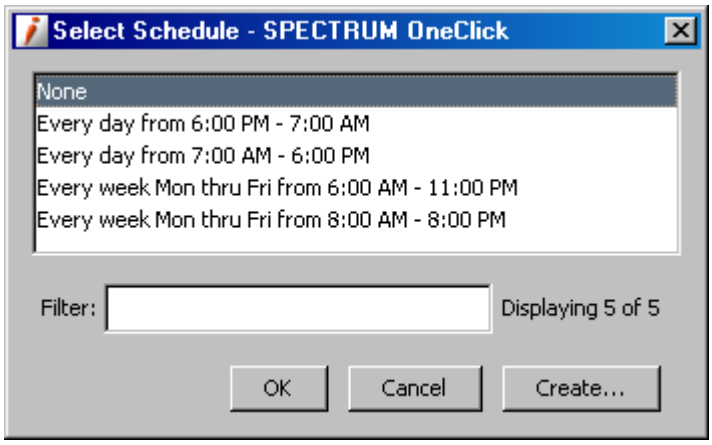
1. Follow the procedures outlined in Network Configuration Manager Bulk Tasks (see page 91) and Firmware Upload (see page 97) to create any of the following tasks: Upload Task, Sync Task, Save to Startup Task, Load Firmware Task, and Cancel Reload Task.

   The Schedule or Edit Schedule button appears on the creation dialog where it is available.

   Note: If Approval Workflow is enabled, the Schedule button is not available during task creation; only approved tasks can be scheduled. You must set up a schedule after the task has been created. See below for the procedure.

2. Select the Schedule or Edit Schedule button.

   The Select Schedule dialog appears as shown in the following image:



3. Take one of the following steps:

   - Select a default schedule, and click OK.
   - Create a custom schedule: click the Create button, specify schedule options, and click OK.

     The custom schedule is added to the list. Select the new schedule and click OK.

   The task is now scheduled. The schedule appears next to the Schedule button.

   Note: To remove the schedule for a task, select the default schedule of None.

4. If you want to run this task multiple times, select Reusable Task. If you specified a recurring schedule in the previous step, the task should be created as a reusable task.

   Note: Reusable tasks will not be cleaned up automatically.

5. Take one of the following steps:

   - Save task. If you have specified a schedule and want to run the task from the List tab in the Tasks folder at a later time, click the Save button. The task is created with the associated schedule (if any).
   - Run task. If you want to run the task right away, click the Run button.

   The task is saved and appears in the Tasks folder in Explorer with the Scheduled Task icon  .

   Schedule information is available in the Schedule field in the List table in the Contents panel and within General Task Information in the Information tab in the Component Detail panel.

You can also create or modify a schedule after task creation for any of the following reasons:

- Before setting up the task to run on a recurring basis, you want to test the task thoroughly.
- Because a task that requires approval cannot be scheduled until after it has been approved, you must first create the task and then wait for the approval.
- Site situations have changed, requiring schedule modification.

Follow these steps:

1. Select Tasks in Explorer and the List tab in the Contents panel.

   All defined tasks appear.

2. Select a task whose schedule you want to create or modify. The following conditions must be met for a task to be eligible for scheduling:

   - Task must be eligible to be run. Either it is a reusable task (Reusable = Yes) or if it is not reusable, then it has not been run yet (Inactive state).
   - If Approval Workflow is enabled, task must be in Approved state.

   The Schedule button in the toolbar is enabled for the task if it can be scheduled.

   Note: If the Schedule button is not enabled, verify that the eligibility conditions are met.

3. Click the Schedule button.

   The Select Schedule dialog opens.

4. Select or create a schedule.

Starting and Stopping Tasks

This section describes how to start, stop, resume, and delete tasks.

Start a Task

This procedure describes how to start a task that has already been created. Tasks can be started if they are not already running and they are reusable tasks or, if they are not reusable tasks, have not been run at all. If approval is enabled, then the tasks have to be in the Approved state.

Note: Any configuration change task that requires approval must be approved before it can be run.

Follow these steps:

1. Select the task from the Tasks view under Configuration Manager in the Explorer tab.
2. Select the List tab in the Contents panel.

   Information about the task displays in the List table. A value of Awaiting Approval in the State column indicates the request has been generated but not yet approved; a value of Approved indicates the request has been approved and can be run.
3. Select a task to start.

   The Start button is enabled if the task can be started.
4. Click the Start Selected Task icon to run the task.

   If information is required for a task, refer to the section for that task. Otherwise, the task starts and the Task State value is updated.

   Depending on the task, a results dialog can appear. For more information, see View Task Results in Real Time (see page 114).

Stop a Task

You can stop a task while it is running.

Follow these steps:

1. Select Tasks under Configuration Manager in the Explorer tab.
2. Click the List tab in the Contents panel, and select a task.

   Note: Only tasks with a State of Running can be stopped.
3. Click the Stop Selected Task icon in the toolbar.

   The task stops, and the Task State value is updated.

Resume a Task

A task can be resumed if it has been stopped and has devices left in the Remaining Device List. When you resume a task, Network Configuration Manager only attempts to run the operation on those devices in the Remaining list. The operation is not reattempted on those devices that previously succeeded or failed and were removed from the Remaining list.

Follow these steps:

1. Select Tasks under Configuration Manager in the Explorer tab.
2. Click the List tab in the Contents panel and select a task to be resumed.

   Note: Only tasks that have devices remaining, as represented by a positive value in the Remaining column, can be resumed.
3. Click the Resume Selected Task icon in the toolbar.

   The task starts, and the State value is updated.

Delete a Task

You can delete tasks in OneClick.

Note: Tasks that are running or locked for edit cannot be deleted.

Follow these steps:

1. Select Tasks under Configuration Manager in the Explorer tab.
2. Click the List tab in the Contents panel and select a task for deletion.
3. Click the Delete selected tasks icon in the toolbar.

   The Confirm Delete dialog appears.
4. Click Yes to delete.

   The selected task is deleted.

Viewing Task Information

This section describes how to view information for tasks that have been created and that have been run.

View Task Results in Real Time

After you have started an Upload, Sync, Save to Startup, Load Firmware task, Reload, or Cancel Reload task, a results dialog opens. The name, condition, type, and status (Pending, Failed, or Succeeded) of the task are shown in the Results tab. If Failed, the results appear in the Cause of Failure field.

Note: The task statistics are updated on a 10-second poll cycle.

While the task is running, you can do the following on the results dialog:

- Click the Content tab to view the content that you are uploading.

  Note: The Content tab is available on the Upload Task Results dialog and Load Firmware Task Results dialog only.

- Click Stop to cancel the task. The task finishes processing any devices that are in progress. It then stops processing any remaining devices.
- Click Close to run the task in the background.

View Critical Statistics on All Bulk Tasks

You can view critical statistics for all bulk tasks simultaneously.

Follow these steps:

1. Select Tasks under Configuration Manager in the Explorer tab.
2. Select the List tab in the Contents panel.

   Statistics for all bulk tasks display.

View Detailed Statistics for a Bulk Task

Take different steps to view detailed statistics for a single bulk task.

Follow these steps:

1. Select a task from Tasks folder in the Explorer tab.
2. Click the Information tab in the Contents panel.

   Information on the task displays.

Task State and Status Values

The Task State (State) and Task Status values identify the current stage of execution for the task. The Task State (State) and Task Status are available when viewing task results or statistics. To access these views, see Viewing Task Information (see page 113).

Task State

The following are possible Task State (State) values:

Approved

Approval workflow mode has been enabled for this task. The task has been approved by the appropriate Task Approver and can be run.

Awaiting Approval

Approval workflow mode has been enabled for this task. A request for this task has been generated but not yet approved.

Completed

The task has run successfully and is reusable. A task that is on a recurring schedule and has run at least once will have this state.

Completed awaiting Destroy

The task has run and is not reusable. The task will be purged within 24 hours.

Denied

Approval workflow mode has been enabled for this task. A request for this task was generated and has been denied by the appropriate Task Approver.

Inactive

The task has been scheduled but not yet run.

Initializing

Task preparation within CA Spectrum has started.

Running

The task is currently running. Tasks in this state can be stopped.

Stopping

The task started and then was stopped by the user.

Task Status

The following are possible Task Status values:

Failed

The task did not complete successfully. The results are displayed in the Cause of Failure field.

Pending

The task is currently running. Tasks in this state can be stopped.

Succeeded

The task has completed successfully.

Chapter 8: Network Configuration Manager Policies

This chapter describes how to create and configure Network Configuration Manager policies. Network Configuration Manager policies monitor content in configurations and verify that device content is compliant.

Note: We recommend that you have configurations captured prior to setting up Network Configuration Manager policies. See Global Synchronization Task (see page 71) to set up a global synchronization task on your network.

This section contains the following topics:

About Network Configuration Manager Policies

A Network Configuration Manager *policy* defines criteria that are used to monitor content for a device host configuration. A policy is checked and compared every time a device host configuration file is captured. Devices that violate the policy can generate an alarm and receive remediation.

Policies can be created and applied to single devices and to global collections. When it is applied to a global collection, the policy is enforced on all global collection members per device family. See Network Configuration Manager and Global Collections (see page 25) for details about setting up global collections.

You can create two types of policies: single-line policies and multi-line block policies. They are described in the following sections.

Note: Configuration captures that are performed on Enterasys/Riverstone SSR devices provide the startup configuration and not the running configuration. Therefore, the startup configuration is used when determining whether a device is compliant with Network Configuration Manager policies. See Determine How an Enterasys/Riverstone SSR Device Responds to an Upload Task (see page 93) for information about how SSR devices handle Network Configurations Manager configuration uploads.

Single Line Policies

A single line policy compares the currently-defined host configuration to the policy definition one line at a time. Each line of data in the host configuration will be analyzed against the policy. This type of policy is useful when checking for the existence of a single command throughout the entire configuration.

Example

Suppose your site has a regulation that all switches must have http enabled. A switch is brought online with the following in its configuration:

```
#http configuration
set ip http server disable
set ip http port 80
```

For this device to comply with site regulations, "set ip http server disable" should be "set ip http server enable". To identify and correct this situation, you can create a single line policy to check if the configuration has the line "set ip http server enable". If this line is missing from the configuration, you can specify that an alarm is generated so that the condition can be repaired. From the alarm, the policy violation can be viewed and you then have the option to repair the device by scheduling a task to upload the corrected content.

Multi-line Block Policies

A multi-line block policy compares the currently-defined host configuration to the policy a block at a time. The policy attempts to match corresponding blocks between the policy and the current host configuration. A block is designated by start and end tags; only data within qualifying blocks will be analyzed by the policy. This type of policy is useful when monitoring settings for a block of configuration text such as an interface configuration. Most devices have multiple interfaces where unique settings for individual interfaces appear in the same configuration file.

There are two options available when enforcing a block policy: the configuration content can be compared to a pre-defined set of policy criteria, or it can be compared with the previous configuration or reference configuration in the configuration history.

When comparing with a previous or reference configuration, lines that have been changed, added, or removed are identified. Comparing with a previous or reference configuration is useful for highlighting changes that occur in the context of the block; changes that occur outside of a designated block will be shown as masked or irrelevant changes.

When comparing with pre-defined policy criteria, lines that violate the criteria will be highlighted. Lines re-ordered within a block may also be highlighted.

Example

Suppose you want to shut down certain interfaces that have been identified by the word "shutdown" appearing in their descriptions. You can identify such devices by defining multi-line block policies in the following ways:

- By comparing to specified contents. You can search for all interfaces that do not contain "shutdown" in the description as the policy definition. This will highlight all the interfaces that *do* contain "shutdown" in the description as violators of the policy.
- By comparing to another configuration. You can monitor content by comparing newly captured configurations to a reference configuration every time a capture occurs. When "shutdown" is added to the description for an interface, it will be highlighted as a violator of the policy because it does not match the reference configuration.

After the devices are identified, the shutdown command can then be issued easily for those interfaces marked for shutdown as part of the recommended upload for corrective action.

Implementation of this example is described in detail in Multi-line Block Policy Example (see page 142).

Create a Policy

A policy defines criteria that are used to monitor content for a device host configuration. Policies can be created and applied to single devices and to global collections. You can create two types of policies: single-line policies and multi-line block policies. The following procedure describes how to create a Network Configuration Manager policy.

Note: An example is provided in Multi-line Block Policy Example (see page 142).

Follow these steps:

1. Select a single device in the Explorer tab.

   Information for the device displays in the Information tab of the Contents panel.

2. Expand the Network Configuration Policies subview.

   The Network Configuration Policies table appears.

3. Click the Create policy icon.

   The Select Policy Type dialog appears.

4. Click the type of policy you want to create:
   - **Single Line Policy.** Creates a policy where only a single line of configuration is compared at a time. The Create NCM Policy dialog opens.
   - **Multi-line Block Policy.** Creates a policy where a host's configuration is compared by qualifying blocks. The Create NCM Block Policy dialog opens.
5. In the Policy ID section, enter a name and description for the policy.
6. In the Policy Criteria section of the dialog, configure policy criteria as follows:
   - For single line policies, see Single Line Policy Criteria (see page 122).
   - For multi-line block policies, see Multi-line Block Policy Criteria (see page 122).
7. In the Policy Actions section of the dialog, do the following:
   a. Enter alarm criteria as follows:

      Alarm device on violation

      Indicates whether to alarm a device when a device is non-compliant with this policy. This is a single alarm on each non-compliant device, viewable in the Alarms tab. You can also select the severity of the alarm (Critical, Major, or Minor). You must enable the policy for this option to take effect.

      Alarm policy on violation

      Indicates whether to alarm the policy when at least one device is non-compliant. This is a single alarm on a single policy, viewable in the Alarms tab. You can also select the severity of the alarm (Critical, Major, or Minor). You must enable the policy for this option to take effect.

   b. Enter a Recommended Upload for Corrective Action.
      - For single line policies, see Single Line Policy Corrective Action (see page 129).
      - For multi-line block policies, see Multi-line Block Policy Corrective Action (see page 129).

   c. Select the 'Commit to Startup' option to indicate whether to copy the entire running configuration to the startup configuration after the new content is merged.
8. Click Save.

   The Save NCM Policy or Save NCM Block Policy dialog appears.

9. Click Continue.

   Note: If you click Exit, the policy becomes inactive and devices will not be checked for compliancy with this policy; however, you can enable the policy at a future time by selecting it from Policies in the Explorer tab.

   The Test NCM Policy or Test NCM Block Policy dialog opens. The policy is tested against stored configurations for one or more devices in the CA Spectrum database. Policy results, including corrective action if applicable, are displayed for your review. Alarms are not generated when testing a policy.

10. If the device is non-compliant:

    a. Click View Violation for information on why the device is non-compliant.

       The View Violation dialog appears. For more information on the View Violation dialog, see Single Line Policy Violations (see page 131) or Multi-line Block Policy Violations (see page 132).

    b. Click Close.

11. Click Repair to upload and merge the corrective content to the device to make it compliant with the policy. See Repair Non-Compliant Devices from the Policy Table (see page 137) for details.

    Note: Repair is enabled only if corrective action has been provided.

12. Select Enable Policy to apply this policy immediately by checking configurations in the database and generating alarms if applicable and when necessary.

    Note: You can also enable (or disable) policies from the Network Configuration Policies dialog. See Enable and Disable Policies from the Policy Table (see page 139) for details.

13. Click Finish.

Policy Criteria

The types of policy criteria that you can specify differs between single line and multi-line block policies. This section describes how to specify policy criteria according to the type of policy you have defined. This section contains the following topics:

- Single Line Policy Criteria (see page 122)
- Multi-line Block Policy Criteria (see page 122)
- Policy Criteria Dialog (see page 127)

Single Line Policy Criteria

Use the following procedure to specify comparison criteria for a single line policy.

To specify criteria for a single line policy

1. On the Create NCM Policy dialog in the the Policy Criteria section, click Add to create criteria for comparison.

   The Policy Criteria dialog opens.

2. Configure policy criteria as described in Policy Criteria Dialog (see page 127).

   After the Policy Criteria dialog is completed, the new criteria for comparison appears in the table.

3. To add more criteria or to modify existing criteria, use the Add, Edit, and Delete buttons.

The remainder of this dialog, including saving of the policy, is described in Create a Policy (see page 119).

Multi-line Block Policy Criteria

When defining a multi-line block policy, you must specify two types of criteria: block definition criteria and comparison criteria. Block definition criteria defines what constitutes the start and end of a block; comparison criteria defines content that is used to compare against the current host configuration.

This section describes how to define this criteria and contains the following topics:

- About Blocks (see page 123)
- Specify Multi-line Block Policy Criteria (see page 124)
- Compare with Specified Contents (see page 125)
- Compare with Matching Block from Reference or Previous Configuration (see page 126)

About Blocks

When using multi-line block policies, you need to know what constitutes a block in the host configuration file for your device. In the following example for a Cisco IOS - SSH Capable device, a block similar to the following exists for each interface. This block would be delimited by the line "interface *name*" and the comment character "!":

```
interface Loopback0
 description "test 123"
 ip address 138.42.96.6 255.255.255.255
 ip pim sparse-dense-mode
 no ip route-cache cef
 no ip route-cache
 ipv6 address 2002:8A2A:5E12:8A2A:6006::1/128
 ipv6 enable
 ipv6 rip IPv6-1 enable
!
```

This information is used when defining the policy. In block policy terminology, this block would be defined by:

Start Tag: interface *name*

End Tag: !

You can use either text or regular expressions to define what constitutes the start and end of a block. The following describes how the two options differ when determining what qualifies as a start or end tag.

Note: The values defined as Start Tag and End Tag will be included as part of the block.

Using Text

When using text, the entire line that contains the matching text will be matched to that field. For example, if you use "interface" of Text type as the start tag, this will match every line that contains the word "interface" and regard it as the starting line for a block.

Using Regular Expressions (Regex)

When using regular expressions, only an exact match of the regular expression pattern (and not the entire line) will be matched to that field. For example, if you specify "interface abc" as the end tag, then only content up to "interface abc" will be considered as the end of the block. If, instead, you specified "interface abc.*" (where ".*" is a wildcard pattern in regular expressions that matches any characters in a line), then the entire line that matched "interface abc" would be considered as the end of the block.

Specify Multi-line Block Policy Criteria

The following procedure describes how to specify criteria for a multi-line block policy.

Follow these steps:

1. On the Create NCM Block Policy dialog in the the Policy Criteria section, specify the following Block Definition criteria.

   You can use either text or regular expressions to define what constitutes the start and end of a block. For additional explanation on how the two options differ, see About Blocks (see page 123).

   Note: The values defined as Start Tag and End Tag will be included as part of the block.

   Start Tag

   Specifies characters that designate the start of the block that is used in the comparison. The policy looks for this delimiter tag in the host configuration to identify the start of a block. The value can be in the form of text or regular expressions, as indicated by the selection of the Text or Regex button. The following example is a regular expression that represents "interface":

   ```
   (?m)^interface .*
   ```

   Using this example, the policy looks for a line that begins with "interface ".

   End Tag

   Specifies characters that designate the end of the block that is used in the comparison. The policy will look for this delimiter tag in the host configuration to identify the end of a block. The value can be in the form of text or regular expressions, as indicated by the selection of the Text or Regex button. The following example is a regular expression that represents the character "!":

   ```
   (?m)^!.*
   ```

   Using this example, the policy looks for the first comment character ("!") after the start of the block to denote the end of the block.

2. In the Comparison Criteria section, select one of the following options:

   - **Compare with Specified Contents**

     Specifies that the policy compares the current host configuration against user-defined content specified in this policy. For more information, see Compare with Specified Contents (see page 125).

   - **Compare with Matching Block from**

     Specifies that the policy compares the current host configuration to content from a previous or reference configuration. For more information, see Compare with Matching Block from Reference or Previous Configuration (see page 126).

The remainder of this dialog, including saving of the policy, is described in Create a Policy (see page 119).

Compare with Specified Contents

When defining a multi-line block policy, you can specify explicitly what content to check for in each block of the current configuration. This procedure describes how to set up user-defined criteria in a multi-line block policy.

To set up user-defined comparison criteria

1. On the Create NCM Block Policy dialog with the 'Compare with Specified Contents' option selected, specify the Order. The following are available options:

   Order Doesn't Matter

   Indicates that the order of the criteria is not considered when comparing with the current host configuration. The policy will be violated based on content only.

   Preserve Order (Allow Extra Lines)

   Indicates that the specified content must appear in the order specified to comply with the policy; however, additional content interspersed between what is specified is allowed. The policy will be violated if some of the specified content does not exist in the configuration or if it exists in a different order. The policy will ignore unmatched lines.

   Preserve Order with No Extra Lines

   Indicates that the specified content must appear both in the order specified and contiguously to comply with the policy. The policy will be violated if the configuration block does not match exactly with the specified content; any extra lines in the block content that were not explicitly defined by the specified content will violate the policy.

2. Click Add to create criteria for comparison.

   The Policy Criteria dialog appears.

3. Configure policy criteria as described in Policy Criteria Dialog (see page 127).

   After the Policy Criteria dialog is closed, the new criteria for comparison appears in the table. The order of the criteria in the table will be used if you have specified that order is preserved when comparing to the host configuration.

4. To add more criteria or to modify existing criteria, use the Add, Edit, and Delete buttons.

Compare with Matching Block from Reference or Previous Configuration

When defining a multi-line block policy, you can specify that the policy compare the current host configuration to the previously-captured configuration or to content saved as a reference configuration. Content will be compared block by block. This procedure describes how to set up the policy to compare content to either a reference or the previously-captured configuration.

Note: A reference or previous configuration must exist for the device when testing the policy; otherwise, a Policy Status of Untestable will result.

To compare content with reference or previous configuration

1. On the Create NCM Block Policy dialog with the 'Compare with Matching Block from' option selected, specify the type of configuration with which to compare content. The following are available options:

   Previous Configuration

   Indicates that the current host configuration will be compared, block by block, to the most recent captured configuration.

   Reference Configuration

   Indicates that the current host configuration will be compared, block by block, to the configuration designated as reference. For information on setting a reference configuration, see Specify a Reference Configuration (see page 77).

   Reference or Previous Configuration

   Indicates that the current host configuration will be compared, block by block, to a saved configuration. First, the policy will look for a reference configuration. If a reference configuration has not been set for a particular device, then block content will be compared against the previous known configuration.

   Note: If a reference or previous configuration does not exist for the device when testing the policy, a Policy Status of Untestable will result.

2. (Optional) Do the following steps to specify a block identifier.

   The block identifier is used to match corresponding blocks between two configurations. You can pick out specific text from within a block and use it as a block identifier. For example, to compare interfaces labeled "interface Loopback*n*" between two configurations, you must identify 'interface Loopback.*' as the block identifier.

If a block identifier is not specified, the first line of the block is used as the block identifier. This default is sufficient in most cases to identify the matching block between two configurations.

a. Click Advanced.

   The Specify Block Identifier dialog opens.

b. Specify the Block Identifier and whether the value is Text or Regex.

   The following is an example of a regular expression that will match corresponding lines that begin with "interface":

   ```
   (?m)^interface .*
   ```

   The following is an example of a regular expression that represents "interface *name*", where only the name of the interface (as opposed to the entire line) will be used to match corresponding blocks:

   ```
   (?m)^interface ([a-z||A-Z||0-9||/]*)
   ```

   Note: When using regular expressions, regular expression capturing groups are leveraged to pick out the block identifier. This is an advanced regular expression concept. Capturing Group 1 will be used as the block identifier when using regular expressions. In this example, Group 1 is ([a-z||A-Z||0-9||/]*), which identifies the name of the interface.

   For more information on using text and regular expressions in multi-block policies, see About Blocks (see page 123).

c. Click OK.

   The Block Identifier dialog closes.

Policy Criteria Dialog

This procedure describes how to complete the Policy Criteria dialog, which is used for defining comparison criteria for single line and multi-line block policies. The content you specify will be checked and compared every time a device's host configuration file is captured. The Policy Criteria dialog is invoked from the Create NCM Policy dialog.

To define criteria using the Policy Criteria dialog

1. Select a comparison type for the policy. Available comparison types are:

   Has line

   Indicates that the host configuration file contains all lines specified. If met, the policy is compliant and passes.

   Does not have line

   Indicates that the host configuration file does not contain the lines specified. If met, the policy is compliant and passes.

Contains

Indicates that the host configuration file contains these words or symbols. If met, the policy is compliant and passes.

Does not contain

Indicates that the host configuration file does not contain these words or symbols. If met, the policy is compliant and passes.

Contains regular expression

Indicates that the host configuration file matches these regular expressions. If matched, the policy is compliant and passes.

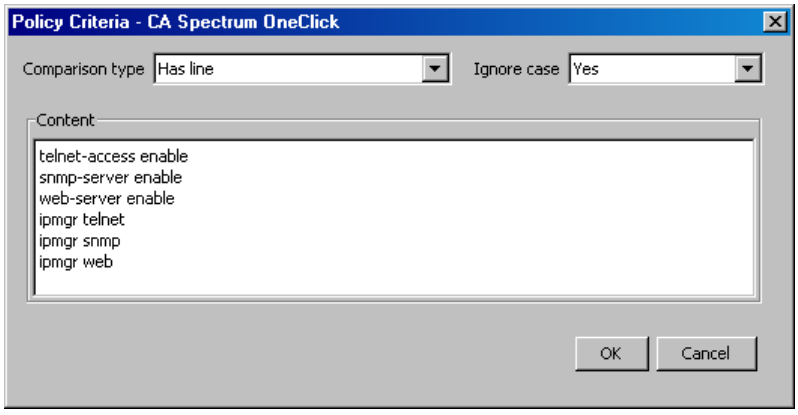
Does not contain regular expression

Indicates that the host configuration file does not match these regular expressions. If not matched, the policy is compliant and passes.

2. Specify whether to ignore upper or lower case for the content that you enter.

   Note: This setting is not available when using regular expressions.

3. Click in the Content box and enter content (full line, sub-string, or regular expression). The following is an example:



4. Click OK.

   The Policy Criteria dialog closes and you return to the Create NCM Policy or Create NCM Block Policy dialog, where the new criteria appears in the table.

Recommended Upload for Corrective Action

The setup for recommended upload for corrective action differs slightly between single line and multi-line block policies. This section describes how to configure corrective action according to the type of policy you have defined. This section contains the following topics:

- Single Line Policy Corrective Action (see page 129)
- Multi-line Block Policy Corrective Action (see page 129)

Single Line Policy Corrective Action

The recommended upload for corrective action for a single line policy involves specifying content that once merged into the running configuration will make the device compliant with the policy. This procedure describes how to set up this content.

To enter corrective action for a single line policy

1. Click Edit under the Recommended Upload for Correction Action group.

   Note: You can also click Open to import content from a text file.

   The Edit Corrective Action dialog opens.

2. Enter one or more lines that will repair a non-compliant device. This is the content that once merged into the running configuration will make the device compliant with this policy.

3. Click OK.

   The Edit Corrective Action dialog closes and the corrective lines are displayed.

Multi-line Block Policy Corrective Action

The recommended upload for corrective action for a multi-line block policy involves specifying content that once merged into the running configuration will make the device compliant with the policy. Because block policies by nature deal with multiple blocks or occurrences of non-compliant data, you must set up the corrective action to handle this accordingly. This procedure describes how to set up this content.

To enter corrective action for a multi-line block policy

1. Select 'Repeat for each violating block' if you want the corrective action to be effected for each block where a violation occurs. If unchecked, the corrective action will be uploaded as-is for the first violating block only.

2. Click Edit under the Recommended Upload for Correction Action group.

   Note: You can also click Open to import content from a text file.

   The Edit Corrective Action dialog opens.

3. Enter one or more lines that will repair a non-compliant device. This is the content that once merged into the running configuration will make the device compliant with this policy. Use the Insert Extracted Content button to insert the <extracted_text> tag into your corrective action, which will be replaced by block-specific content when the policy runs. The following shows an example corrective action:

   ```
   interface <extracted_text>
   description "policy violation detected on <extracted_text> by Spectrum"
   !
   ```

   Important! The repair text must be a valid and complete device configuration statement, especially when the repair action is repeated. For example, if the "!" is omitted from the end of the previous example, the corrective action may not be implemented properly and unexpected results may occur. This is because the statement is not ended correctly: a description needs to end with a new line character or a new line with a "!" character.

4. Click Configure Extracted Content.

   The Edit Extracted Content dialog opens.

5. Enter content to be extracted from each block, and select whether it is Text or a regular expression (Regex).

   - If text, this value will be inserted wherever the <extracted_text> tag is found in the corrective action.
   - If regular expression, the value returned from evaluating the regular expression will be inserted wherever the <extracted_text> tag is found in the corrective action.

   The following is an example of a regular expression that represents "interface *name*":

   ```
   (?m)^interface ([a-z||A-Z||0-9||/]*)
   ```

   Using this example, the policy will extract the name of the interface from each block and will insert it into the corrective action.

   Note: For more information on using text and regular expressions in multi-block policies, see Multi-line Block Policies (see page 118).

6. Click OK.

   The Edit Corrective Action dialog closes and the corrective lines are displayed.

View Violations

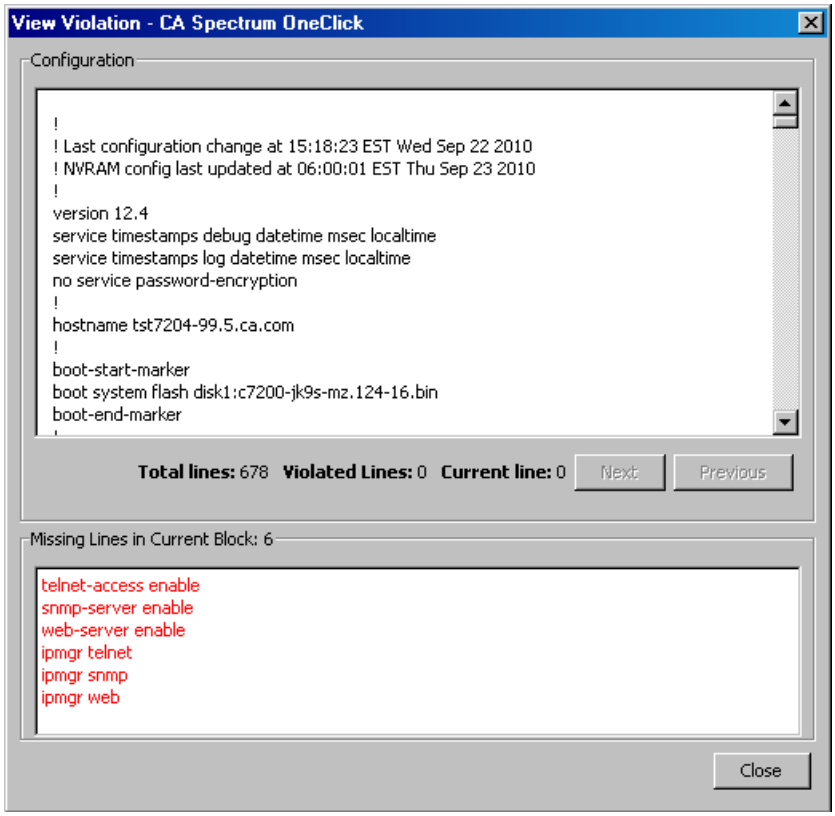
When a device is non-compliant, a View Violations dialog provides information as to the reason why. The dialog that is invoked and the information presented varies based on the policy definition. This section contains the following topics:

- Single Line Policy Violations (see page 131)
- Multi-line Block Policy Violations (see page 132)

Single Line Policy Violations

Violations for all single line policies are displayed in the View Violation dialog.

The following example shows certain required commands that are missing in the configuration for the device and thus the policy is violated.



The View Violation dialog for all single line policies contains the following information:

Configuration

Displays the captured host configuration in its entirety with any violated lines highlighted.

Total lines

Provides the total number of lines in the configuration file.

Violated Lines

Provides the total number of lines that violate the policy.

Current line

Provides the current location within the configuration file.

Next

Allows you to quickly advance to the next violation.

Previous

Allows you to move back to the previous violation.

Missing Lines in Current Block: *total_number_of_lines*

Displays those lines defined in the policy that were not found in the configuration file.

Note: For single line policies, there is only one block.

Multi-line Block Policy Violations

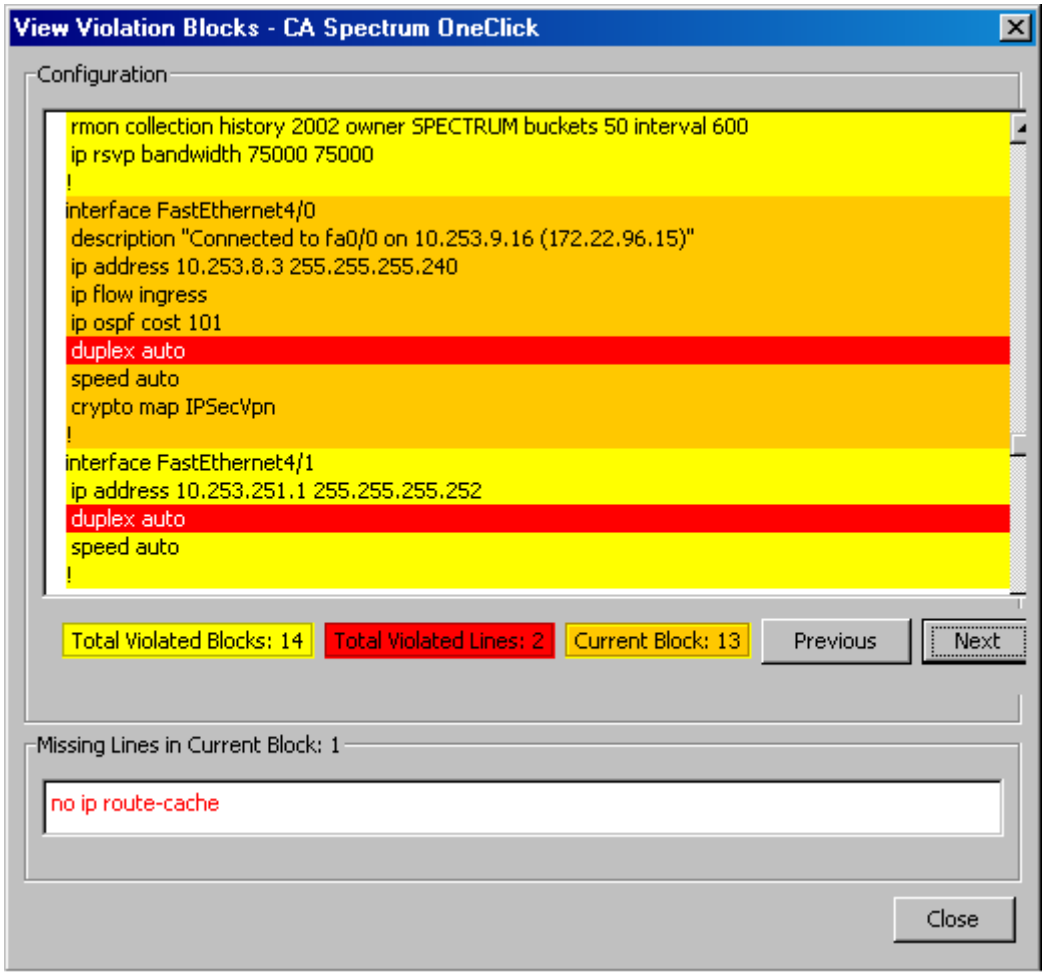
There are two types of criteria that can be used for comparison in a multi-line block policy: user-defined criteria and content from a saved configuration. Because of this, the view violation dialog that appears will be different depending on the violation content to be displayed.

Violations when Compared with Specific Contents

When user-defined criteria is used for comparison in a multi-line block policy, violations are shown on the View Violation Blocks dialog.

The following are examples of View Violation Blocks dialogs for multi-line block policies where the current host configuration is compared to user-defined criteria.

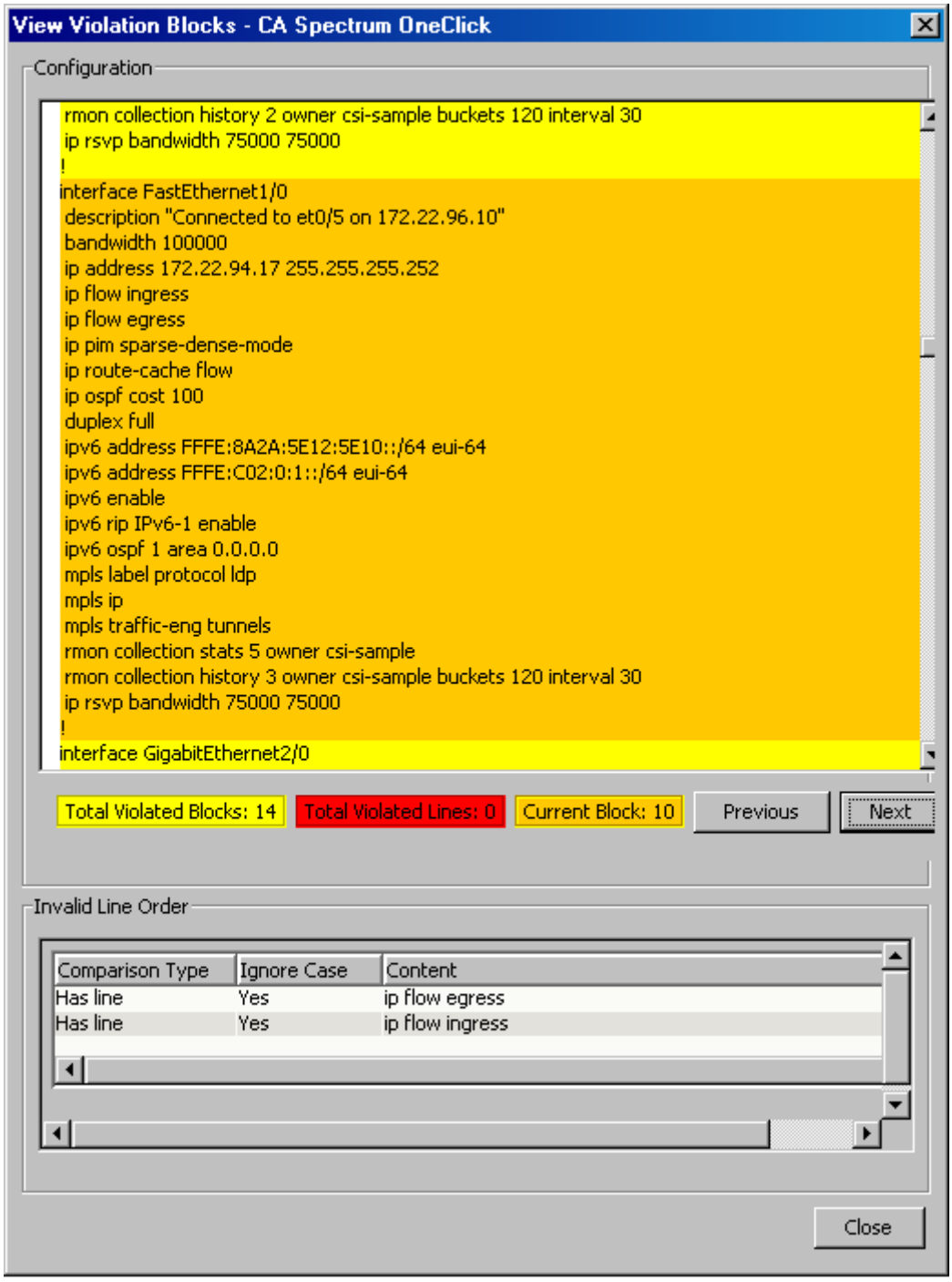
In this example, a policy has been set up to check that 'duplex auto' is not present and 'no ip route-cache' is present for each interface configuration. The violations are identified as follows:



In the next example, a policy has been set up to so that a configuration is compliant if the following commands appear and that they appear in the following order:

```
ip flow egress
ip flow ingress
```

The current configuration violates this policy because although the commands appear, they are not in the correct order, as shown in the following image:



The View Violation Blocks dialog may contain the following information, depending on the violation:

Configuration

Displays the captured host configuration in its entirety with any violated lines highlighted:

- **Red—**These lines contain violations.

Blocks are distinguishable by color:

- **Orange—**These lines constitute the current block.
- **Yellow—**These lines are included in a block other than the current block.

Total Violated Blocks

Provides the total number of blocks that contain violations.

Total Violated Lines

Provides the total number of lines that violate the policy.

Current Block

Provides the current location within the configuration file. Distinguishable blocks are numbered for identification.

Previous

Allows you to move back to the previous block containing a violation.

Next

Allows you to quickly advance to the next block containing a violation.

Missing Lines in Current Block: *total_number_of_lines*

Displays those lines defined in the policy that were not found in the configuration file.

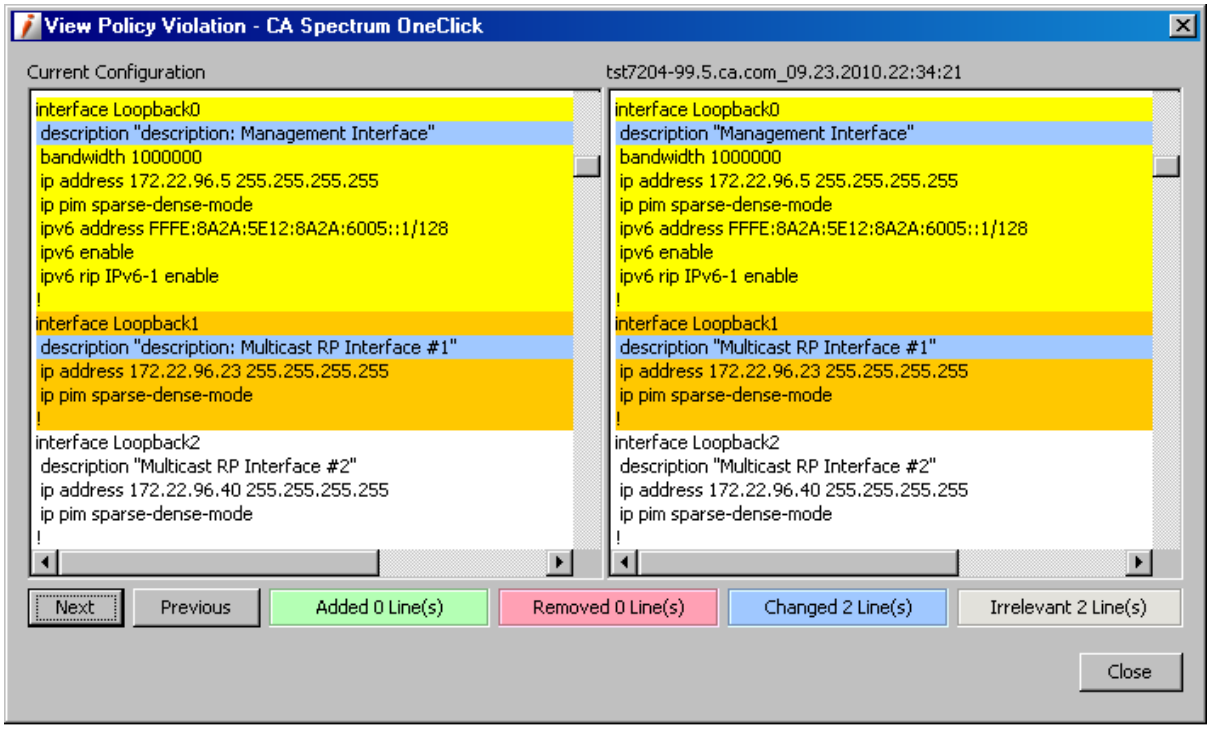
Invalid Line Order

Displays content criteria that has been violated due to its order of appearance in the configuration file.

Violations when Compared with Another Configuration

When a saved configuration is used for comparison in a multi-line block policy, violations are shown on the View Policy Violation dialog.

The following is an example of a View Policy Violation dialog for a multi-line block policy where the current host configuration is compared to a reference configuration and lines have changed; thus, the policy is violated.



The current host configuration is in the left pane and the reference configuration is displayed in the right. Differences between the two configurations are highlighted according to the following key.

Blocks containing differences are highlighted in their entirety and distinguishable by color:

- **Yellow**—These lines constitute a block where a violation occurs.
- **Orange**—These lines constitute a block where a violation occurs.

Individual lines denoting differences are identified as follows:

- **Green**—These lines were added.
- **Red**—These lines have been removed.
- **Blue**—These lines have changed.
- **Grey**—These lines differ but are outside of a qualifying block.

Click Next or Previous to navigate through the differences in the file.

Repair Non-Compliant Devices

In addition to repairing non-compliant devices when setting up policies, you can also initiate repair of non-compliant devices after violations occur. This section contains the following topics:

Repair Non-Compliant Devices from the Policy Table

You can check and repair policies from the policy table by selecting a single device or global collection. For example, you can repair a non-compliant device.

Follow these steps:

1. Select an individual device or a global collection that has a configured policy in the Explorer tab.
2. Select the Information tab in the Contents panel.

   Information about the device or global collection appears.
3. Expand Network Configuration Policies.

   The Network Configuration Policies table appears. Policies with non-compliant devices have a non-zero value in the Violators column.
4. Select a policy that has a non-compliant device, and click the 'Launch repair dialog' icon.

   The Repair Devices in Violation dialog appears.
5. Click the Content tab to view the content to be uploaded to perform the repair.
6. Click View Violation to view the violation of each device.
7. Click Repair.

   The Creating Task status box appears. The Upload Task Results dialog show the results of the operation.

Note: You can automate and minimize the above process by running a Jar executable through AlarmNotifier. Contact CA Spectrum support team to get the executable file and the steps to use it.

Repair Non-Compliant Devices from a Policy Violation Alarm

You can view a violation and upload or merge the correct content to the device to make it compliant with the policy from the Alarm Details tab. Repair a non-compliant device directly from a policy violation alarm.

Follow these steps:

1. Select an individual device, a global collection that has a configured policy, or a policy (from the Policy node) in the Explorer tab.
2. In the Alarms tab in the Contents panel, select an alarm with “NCM Policy Violated” in the Alarm Title column.
3. Click View Violation Details in the Alarm Details tab in the Component Detail panel.

   The Repair Devices in Violation page opens.
4. Click Content to view the content to be uploaded to perform the repair. Click View Violation to view the violation of each device.

   The View Violation page appears.
5. Click Repair.

   The Creating Task status box appears, followed by the Upload Task Results page.

Manage Policies

After a policy has been created, you can edit, enable or disable, apply to a global collection, and delete it. This section contains the following topics:

Edit Policies

You can edit an existing Network Configuration Manager policy. After you edit a policy, you must save and enable it.

To edit a policy

1. Select a policy under the Policies node in the Explorer tab.
2. Select the List tab in the Contents panel.

   A list of policies appears.

3. Select the policy and click the Edit icon in the toolbar.

   The Edit NCM Policy dialog appears.

4. Make changes as necessary and click Save.

   The policy is disabled. Enable the policy as explained in Enable and Disable Policies from the Policy Table (see page 139).

   Note: Optionally, you can edit a policy by selecting a global collection, clicking the Information tab, and editing the associated policy. You can also select an individual device, click the Information tab, click Network Configuration Policies, and edit the associated policy.

Enable and Disable Policies

You can enable and disable Network Configuration Manager policies from the policy table.

Follow these steps:

1. Select a policy under the Policies node in the Explorer tab.
2. Select the List tab of the Contents panel.

   A list of policies appears.

3. Select a policy and click the 'Enable selected policies' icon.

   Enabling a policy causes any specified alarms to immediately appear for all non-compliant devices and violated policies.

4. (Optional) Select a policy and click the 'Disable selected policies' icon to disable that policy.

   Disabling a policy immediately clears any existing alarms on non-compliant devices and violated policies.

Note: You can also enable and disable a policy by selecting a global collection or an individual device. Use the Information tab to manage the associated policy.

Apply Policies to Global Collections

After a policy is created, it can be applied to a global collection. When a policy is applied to a global collection, the policy is then enforced on all global collection members per device family.

To apply a policy to a global collection

1. Select a global collection in the Explorer tab.

   Information for the global collection appears in the Information tab of the Contents panel.

2. Expand the Network Configuration Policies subview.

   The Network Configuration Policies table appears.

3. Click the 'Add/Remove policies to/from the global collection' icon.

   The Adds/Removes Policies to the Global Collection dialog appears.

4. Select those policies that you want enforced on this global collection and move to the Applied To window.

   Note: You can also create policies directly from this dialog using the Create button.

5. Click OK.

   The applied policy appears in the Network Configuration Policies table and will be enforced on all global members per device family.

More information:

Global Collections (see page 25)

Delete Policies

To delete a policy that you no longer need, right-click the policy from Policies in the Explorer tab and select Delete.

Note: Optionally, you can delete a policy by selecting a global collection, clicking the Information tab, and deleting the associated policy. You can also select an individual device, click the Information tab, click Network Configuration Policies, and delete the associated policy.

View Policy Information

This section describes how to view policy information and includes the following topics:

View Policy Details

You can view component details for Network Configuration Manager policies.

Follow these steps:

1. Select a single device or a global collection in the Explorer tab that has an associated policy.
2. Click the Information tab in the Contents panel.

   Information and configurations for the selected device or global collection appear.
3. Expand Network Configuration Policies, and click 'View the Component Detail for the selected model'.

   The Component Detail panel for the selected policy appears.

   Note: You can also access this screen by selecting a policy from Policies in the Explorer tab.

View Critical Statistics for All Policies

You can view critical statistics for policies by selecting Policies under Configuration Manager in the Explorer tab and selecting the List tab in the Contents panel.

Statistics for all policies appear.

View Critical Statistics for All Policies Applied to a Single Device

You can view critical statistics for policies that are applied to a single device.

Follow these steps:

1. Select a device, and then click the Information tab.

   Information about the device appears.

2. Select Network Configuration Policies.

   Statistics for all policies applied to a single device appear.

View Critical Statistics for Policies Applied to a Global Collection

You can view critical statistics for policies that are applied to a global collection.

Follow these steps:

1. Select an existing Global Collection from the Explorer tab. Select the Information tab of the Contents panel.

   Information appears in the Contents panel.

2. Select Network Configuration Policies.

   Statistics for all policies that are applied to a collection appear.

Multi-line Block Policy Example

This section provides an example of how to use multi-line block policies. The same use case is implemented in two different ways: by comparing to specified contents and by comparing to another configuration.

Note: The content provided in this section is intended to provide a sample use case at a high level. For additional information on any of the concepts or items referenced in this section, please refer to the appropriate parent topic.

This section contains the following topics:

Scenario

Suppose you want to shut down certain interfaces that have been identified by the word "shutdown" appearing in their descriptions. You can identify such devices by defining multi-line block policies in the following ways:

- By comparing to specified contents. You can search for all interfaces that do not contain "shutdown" in the description as the policy definition. This will highlight all the interfaces that *do* contain "shutdown" in the description as violators of the policy.
- By comparing to another configuration. You can monitor content by comparing newly captured configurations to a reference configuration every time a capture occurs. When "shutdown" is added to the description for an interface, it will be highlighted as a violator of the policy because it does not match the reference configuration.

After the devices are identified, the shutdown command can then be issued easily for those interfaces marked for shutdown as part of the recommended upload for corrective action.

Getting Started

Before you begin defining a policy, you must do the following:

- Identify what constitutes a block.
- Establish a reference configuration (if comparing to a reference configuration).

You can gather this information by reviewing captured host configurations for the device. Configurations are captured using the Global Sync task, the Sync task, and the Capture Configuration icon.

To view a captured host configuration for a device

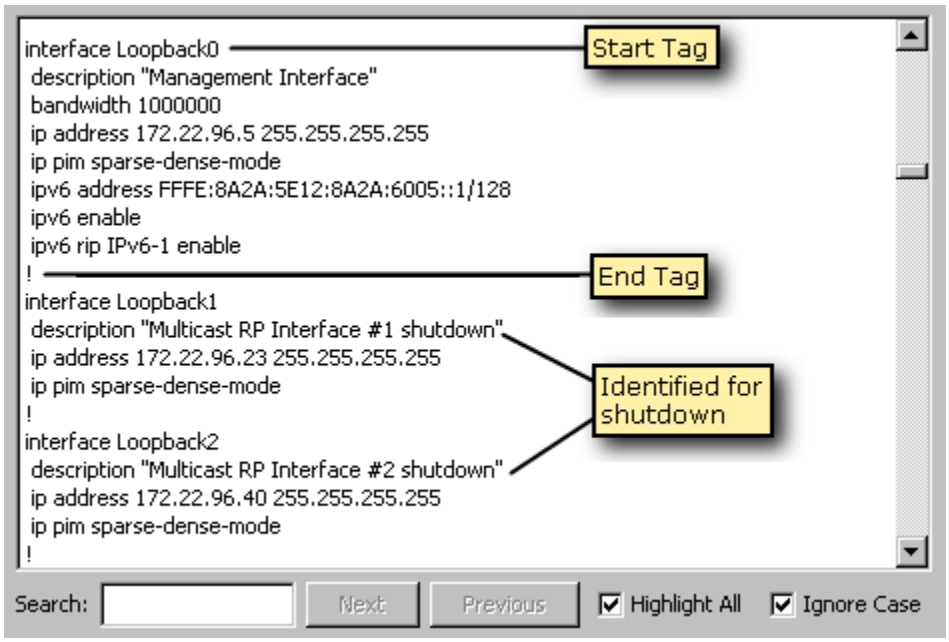
1. Select a device in the Explorer tab.
2. Verify the List tab is selected in the Contents panel and select the Host Configuration tab in the Component Detail panel.
3. Click the row in the Host Configuration table for the captured host configuration that you want to view.

   The captured host configuration appears in the box below the table.

Note: For more information, see View Configuration History for a Single Device (see page 74).

Identify what constitutes a block

The following image shows a portion of the configuration file for a device. You can see that each interface on this device has a similar format and is delimited by a start tag and an end tag. Also, notice the appearance of "shutdown" in the descriptions for a couple of the interfaces.



In block policy terminology, each block in this example would be defined by:

Start Tag: interface

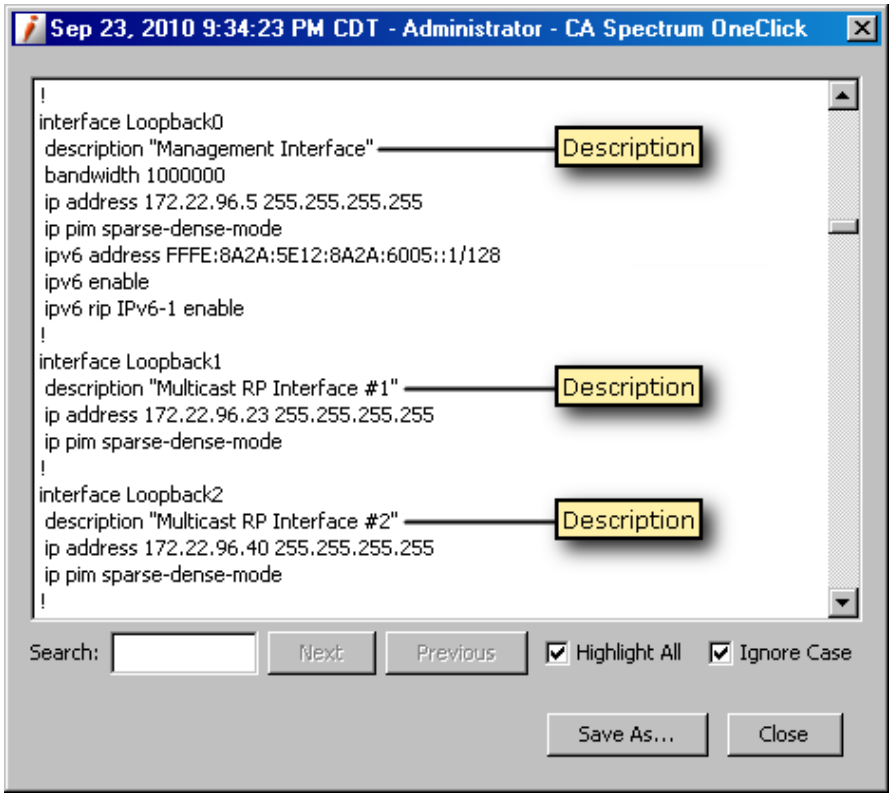
End Tag: !

Establish a reference configuration (if comparing to a reference configuration)

Use the procedure outlined in "To view a captured host configuration for a device" to identify a host configuration that contains ideal settings for the device, and specify this configuration as its Reference Configuration. For information on setting a reference configuration, see Specify a Reference Configuration (see page 77).

Note: You can also use the last captured configuration for comparison instead of the reference configuration.

The following image shows a portion of the configuration file that will be used as the reference configuration. Notice that this configuration does not contain "shutdown" in the description for any of the interfaces.



More information:

Global Synchronization Task (see page 71)
Specify a Reference Configuration (see page 77)
Manually Capture Configurations (see page 85)
Create Sync Task (see page 94)

Defining the Policy

After you have established what constitutes a block and have specified a reference configuration (if applicable), the multi-line block policy can be defined.

Refer to the steps outlined in Create a Policy (see page 119) to create a multi-line block policy and subsequently invoke the Create NCM Block Policy dialog, which contains the following sections:

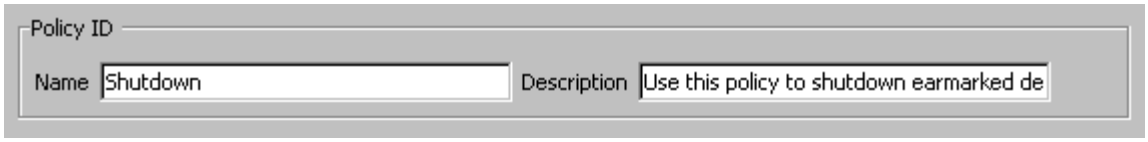
- Policy ID
- Policy Criteria
- Policy Actions

Each of these sections will be described separately.

Note: Additional detailed information for each of the fields mentioned in this section is available in the Create a Policy (see page 119) section.

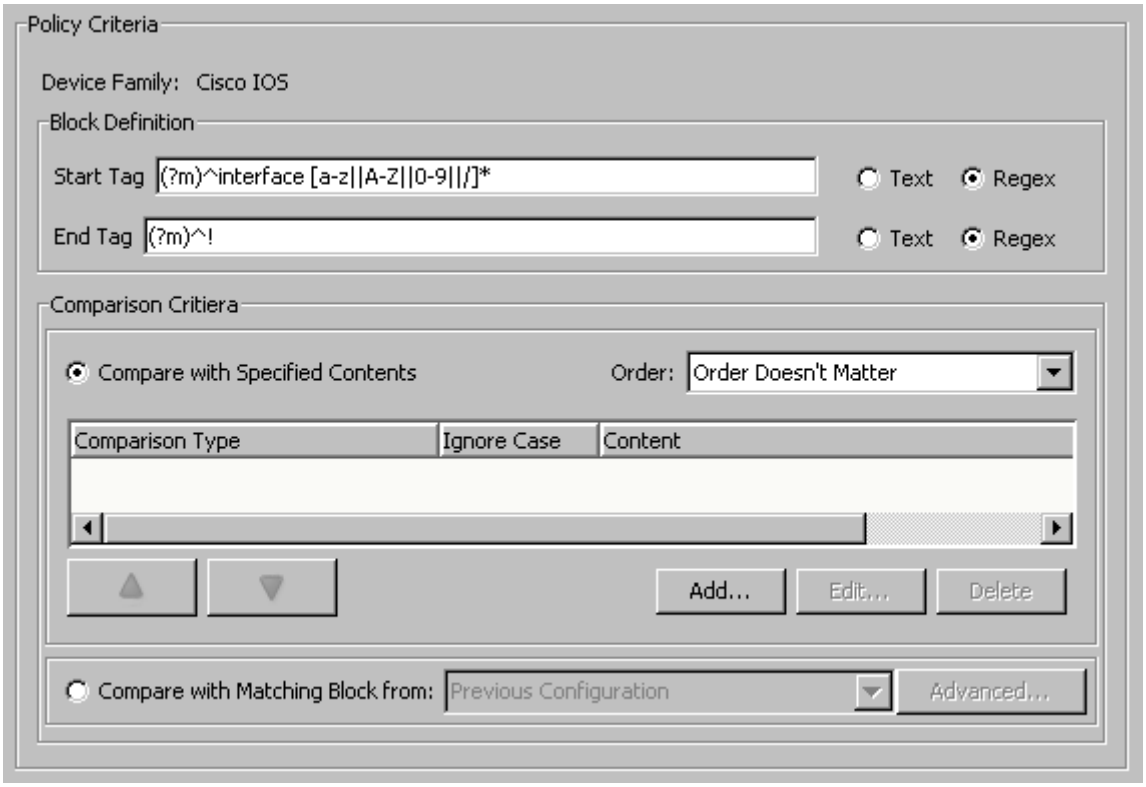
Policy ID

The Policy ID information identifies the policy. Use these fields to name the policy according to standards in place at your site.



Policy Criteria

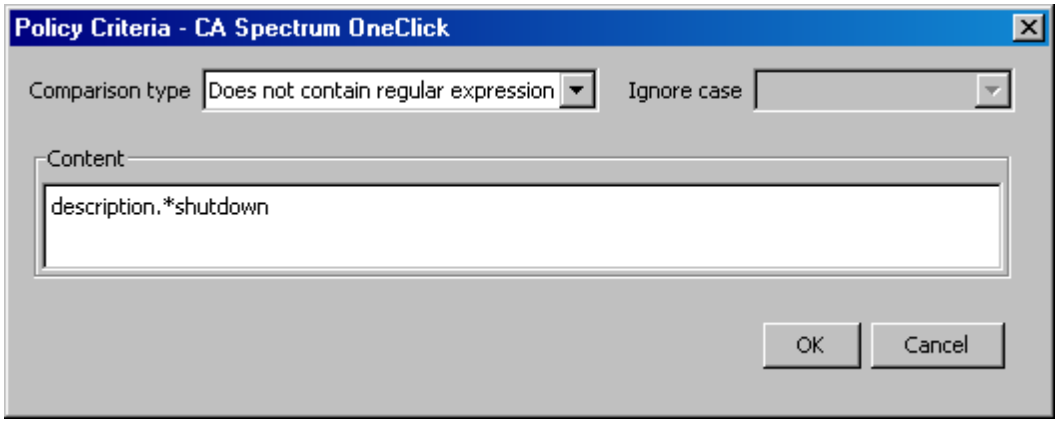
The Policy Criteria information defines the block-delimiting fields and the comparison criteria, which are described following the image.



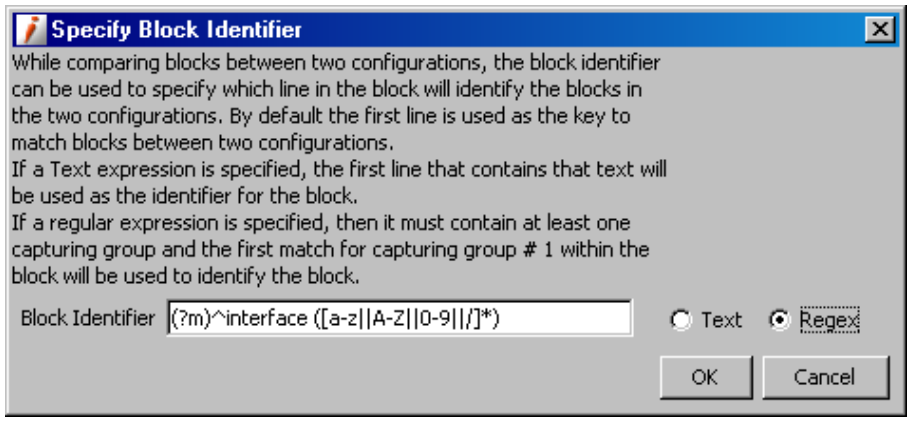
- **Block Definition.** The Start Tag and End Tag fields define strings that are used to identify the beginning and end of a block. In this example, regular expression values are used to designate that each block begins with the string "interface *name*" and ends with the character "!". These values are included as part of the block.
- **Comparison Criteria.** This section controls the method by which a newly captured configuration is evaluated against the policy. You can specify whether to compare the configuration against specific, user-defined criteria or against another configuration.

  Note: Only one set of criteria can be included in a single policy. Both sets of criteria are shown here for demonstration purposes only.

- The option to 'Compare with Specified Contents' indicates that each configuration that is captured after the policy is enabled will be compared to user-defined criteria. Click the Add button to display the Policy Criteria dialog. The following image shows criteria that looks for lines that begin with "description" and contain "shutdown". When this policy runs, interfaces that do contain "shutdown" in the description will be identified as violators.

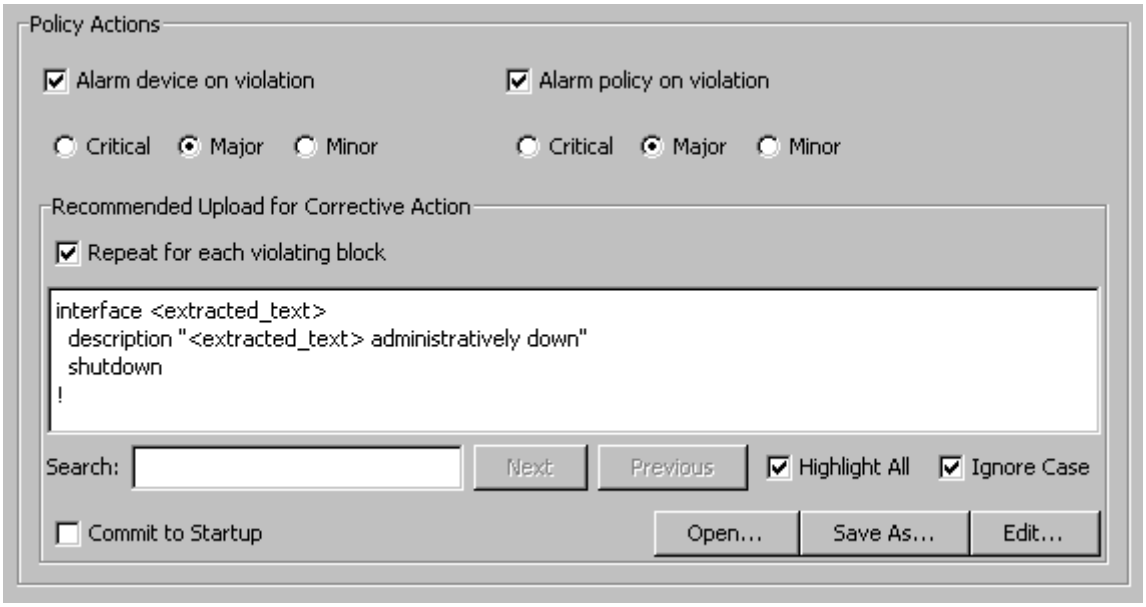


- The option to 'Compare with Matching Block from Reference Configuration' indicates that each configuration that is captured after the policy is enabled will be compared to the configuration that has been designated as the Reference Configuration for the device. Click the Advanced button to specify the Block Identifier, which is used to match corresponding blocks between the current configuration and the reference (or previous, if specified) configuration. The following example will match up based on "interface *name'":*

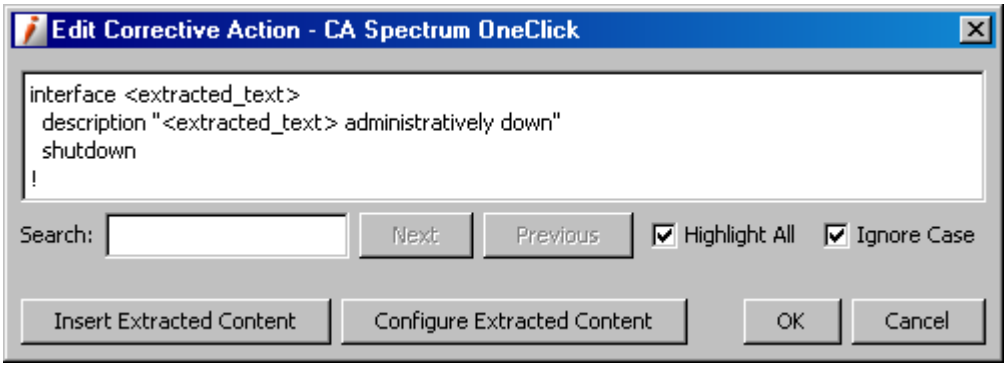


Policy Actions

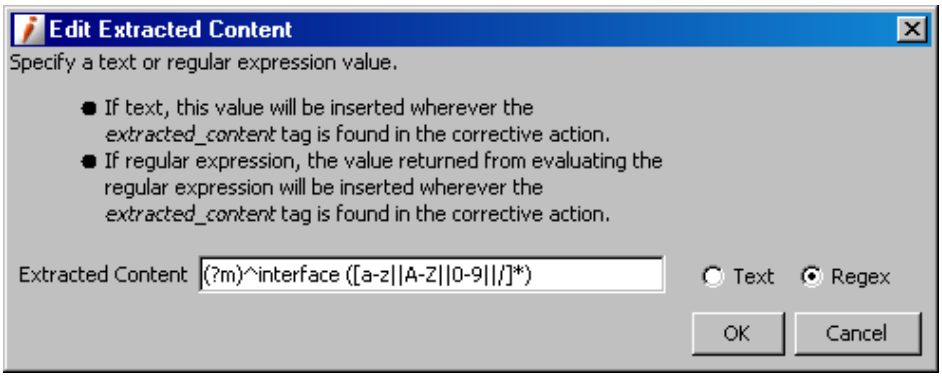
The Policy Actions options define how alarms should be generated and the corrective action to be uploaded should non-compliance occur. The following image shows this section (already populated) and will be described subsequently:



- Specify alarm preferences for when a violation occurs. Alarms can be associated with the device, the policy, or both.
- To define the 'Recommended Upload for Corrective Action,' click the Edit button to display the Edit Corrective Action dialog. In the box, enter the content that will be uploaded to the device. The following image shows content that will upload a modified description and the shutdown command to the device:



In this example, the <extracted_text> tag will be replaced by block-specific content when the policy runs. To insert this tag into your corrective action, use the Insert Extracted Content button. To configure what will be used to replace the tag, click the Configure Extracted Content button, which opens the following dialog:



In this example, the name of the interface will be extracted from each block and used to create corrective action content.

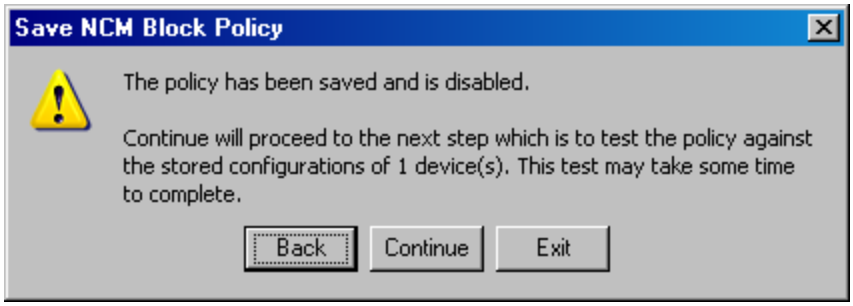
After the corrective action content is defined, it appears in the Recommended Upload for Corrective Action box. Select the 'Repeat for each violating block' option if you want this change to be made for each occurrence of a violation; if it is left blank, the change will only be made for the first occurrence.

Saving and Testing the Policy

After the policy is initially defined, it should be tested before being enabled to make sure it operates as expected.

To proceed with testing of the policy, click Save on the Create NCM Block Policy dialog to save your settings. On the ensuing Save dialog, shown in the next image, click Continue to test the policy.

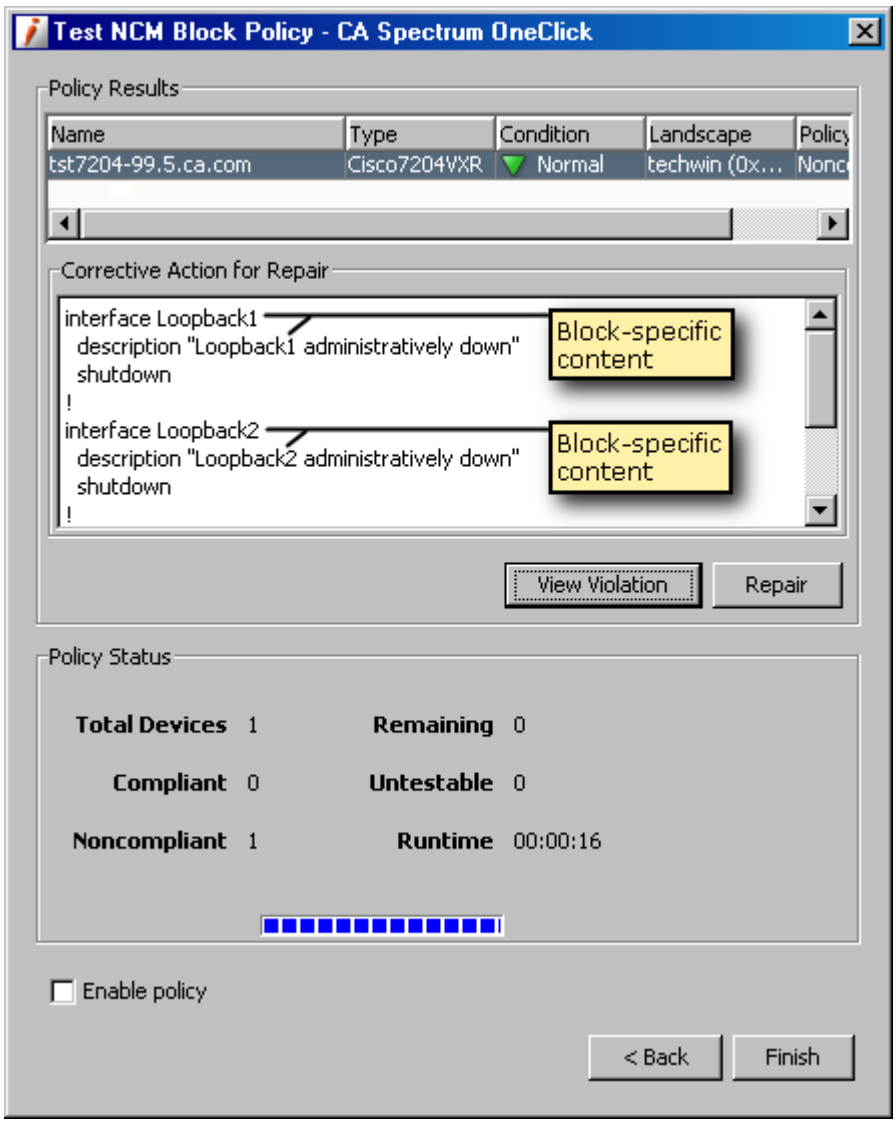
Note: You can also select Back to make additional changes to the policy definition. If you click Exit, the policy is saved but disabled.



The Test NCM Block Policy dialog opens, the test begins, and the status bar indicates its progress. During the test, current configurations are captured and compared to criteria specified in the policy. Blocks are matched based on the block identifier and the contents of corresponding blocks are compared.

Note: Depending on the number of devices included, the test may take a while to complete.

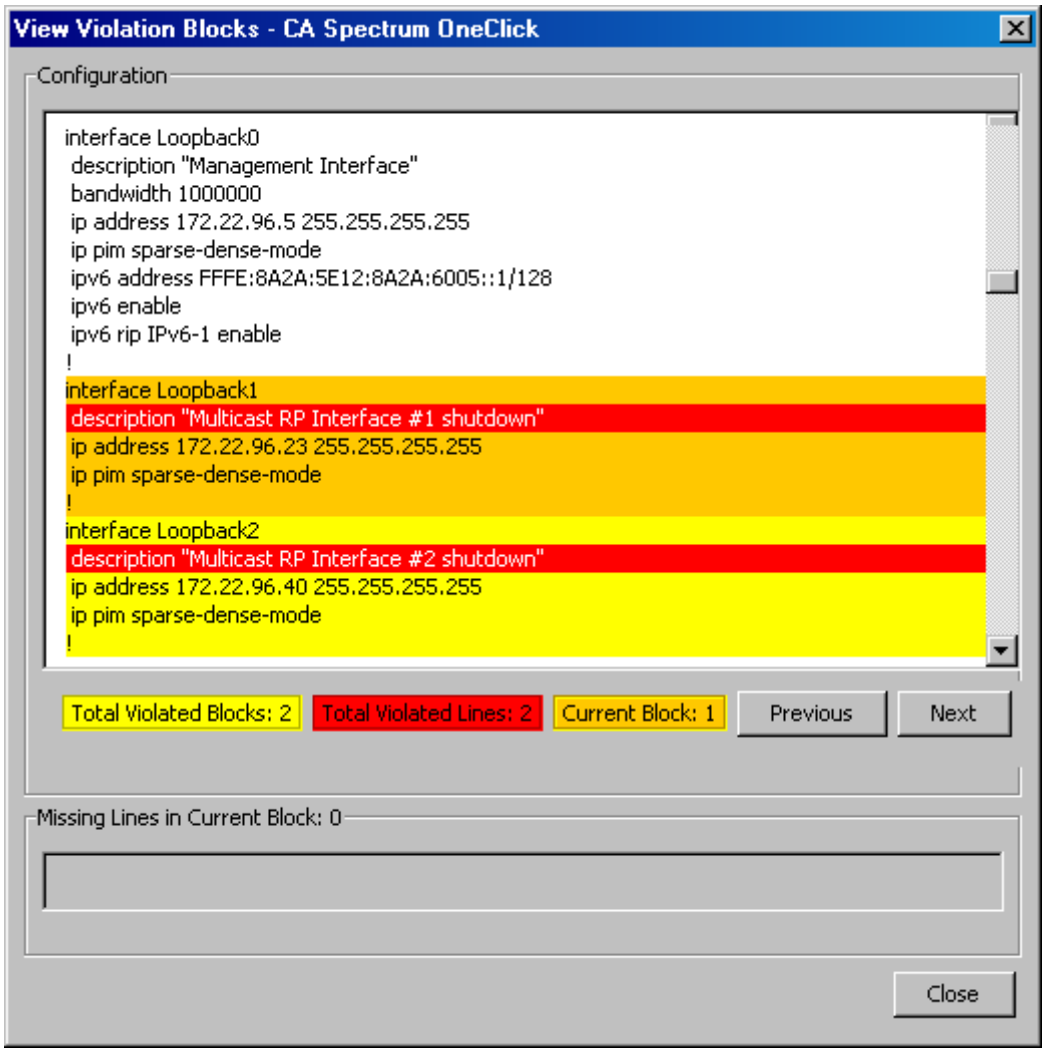
When testing of the policy is complete, the policy results are displayed, as follows:



When non-compliancy is detected, as in this example, the number of devices affected is reported in the Policy Status section, and, if it has been defined, corrective action is displayed as well. Notice that the <extracted_text> tag has been replaced with block-specific content.

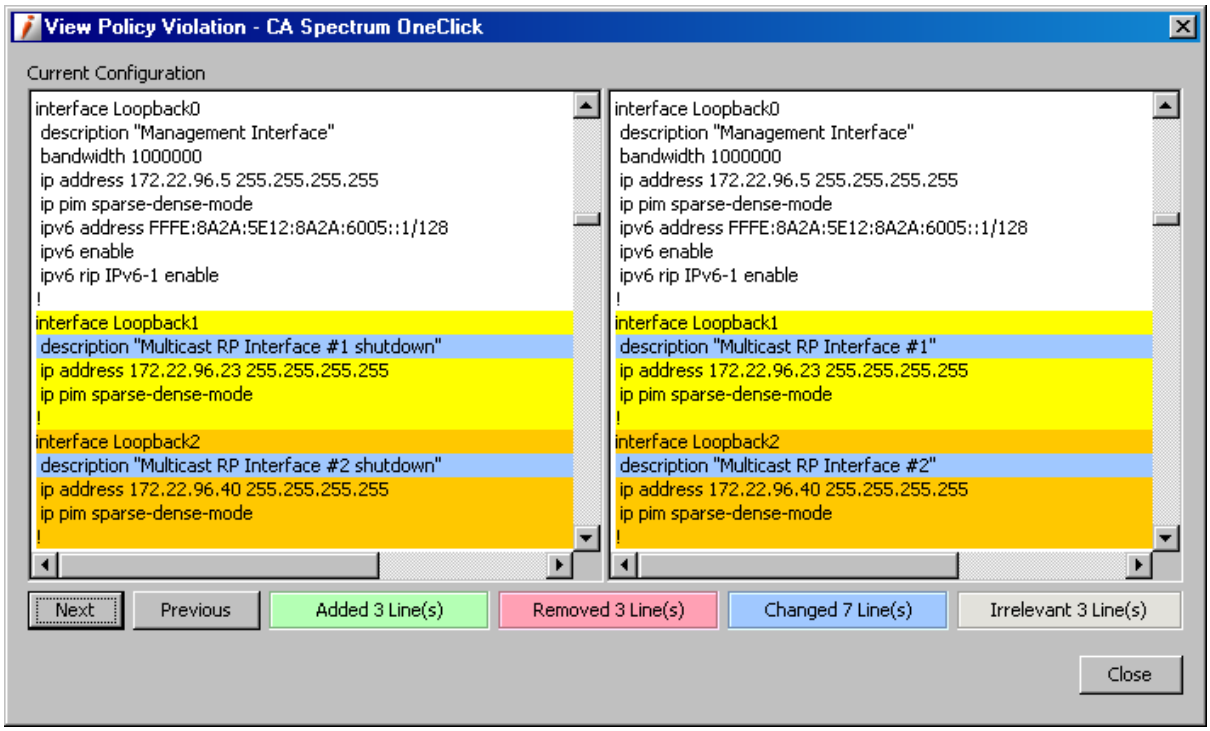
After the test is complete, you can do the following from the test dialog:

- To view the policy violations, click View Violation. A dialog appears that shows the violations.
  - If you used specified contents for comparison criteria, the View Violation Blocks dialog appears, as in the following image. Each block is distinguished by color and the violated lines are highlighted. In this example, the lines beginning with "description" and containing "shutdown" are identified as violations. You can scroll through the violations using the Next and Previous buttons.



– If you used another configuration for comparison criteria, the View Policy Violation dialog appears, as in the following image. Each block is distinguished by color and the differences are highlighted. In this example, the description content for two of the interfaces does not match what was defined as the reference. You can scroll through the violations using the Next and Previous buttons.

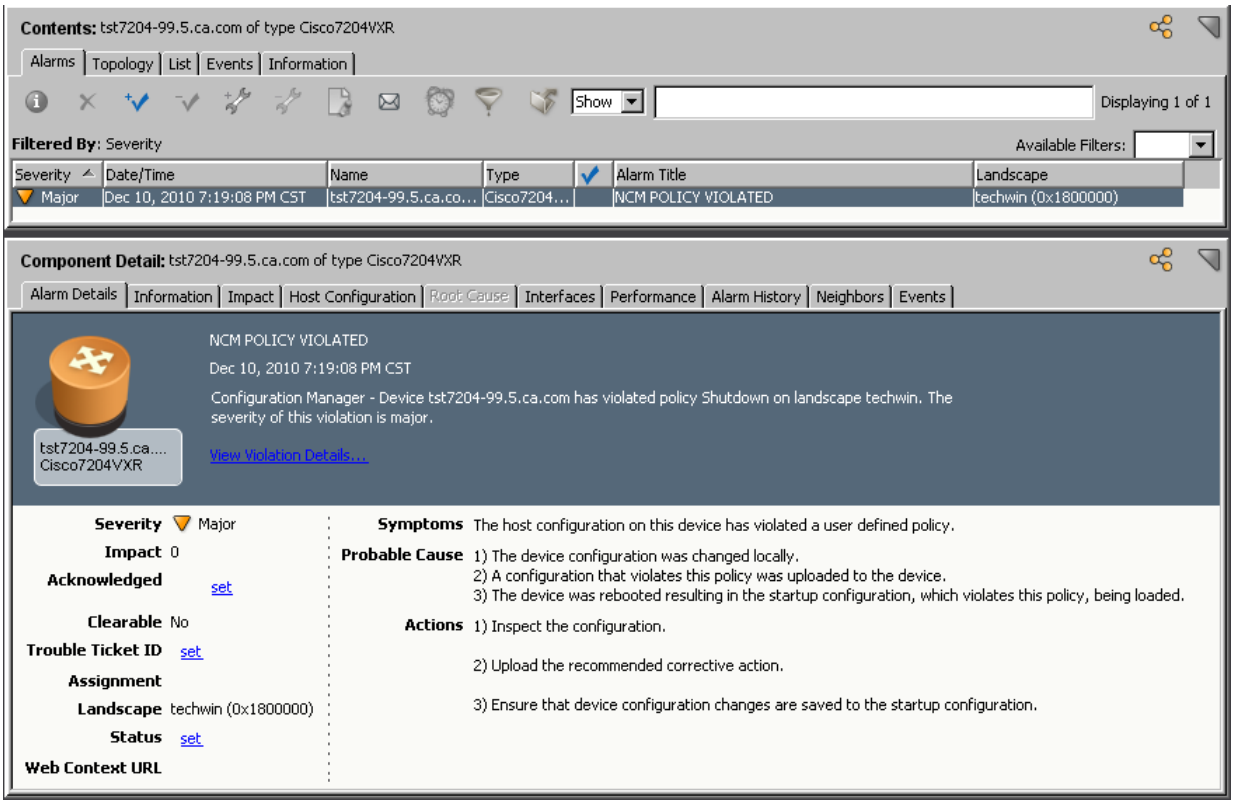
Important! When comparing against a reference configuration, be sure to review each of the differences found so that you do not inadvertently execute a corrective action where it does not apply.



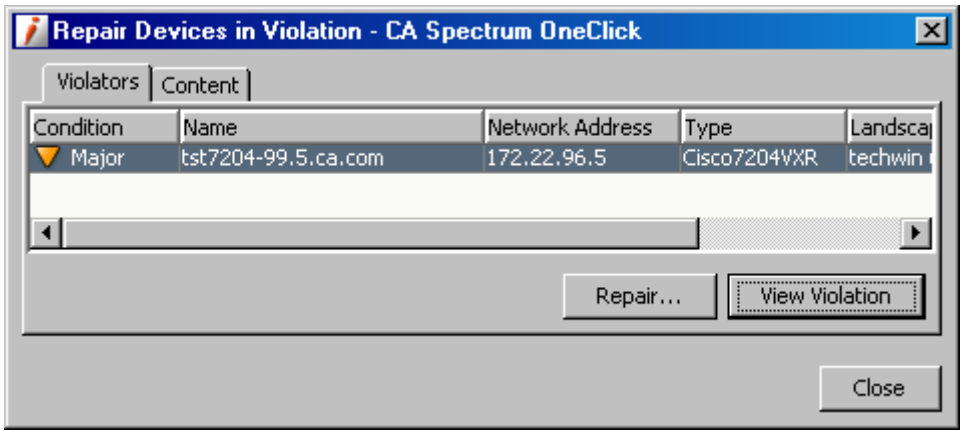
- To correct the policy violation and thereby make the device compliant, click Repair to upload the content as outlined in the 'Corrective Action for Repair' box. An Upload task is created and executed, with the results of the task displayed in the 'Upload Task Results' dialog.
- If you are satisfied with the results of the test, select the 'Enable policy' option to start automatic monitoring and alarm generation based on this policy; otherwise, you can click Back and modify the policy definition. If you click Finish, the policy will be saved but not enabled.

Monitoring Violations

After a policy has been enabled, it monitors configurations that are captured and will alert you to any violations based on the actions you have specified. An alarm generated by a policy violation has an alarm title of 'NCM Policy Violated.' The following image shows an alarm generated based on this example policy:



From the alarm details, you can click View Violation Details, which will open the Repair Devices in Violation dialog as follows:



From this dialog, you can use the available buttons to view violations or repair the non-compliant devices as described when testing the policy.

Note: You can also launch this dialog from the Network Configuration Policies table in the Contents panel for the non-compliant device. For more information, see Repair Non-Compliant Devices from the Policy Table (see page 137).

Appendix A: Supported Devices

This section contains the following topics:

Cisco Supported Devices

The CA Spectrum Network Configuration Manager supports the following Cisco devices. For a list of supported Catalyst devices, see Cisco Supported Catalyst Devices (see page 178). For a list of PIX firewall devices, see Cisco Supported PIX Firewall Devices (see page 185).

The table provides examples. For the most up-to-date information on device support, access the CA Device Certification database (see page 16).

When a Perl script is the only means of communication with the device, the script method is provided.

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
CiscoDSC9216K9	1.3.6.1.4.1.9.1.521	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco677i	1.3.6.1.4.1.9.1.363	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco741	1.3.6.1.4.1.9.1.94	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco742	1.3.6.1.4.1.9.1.95	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Cisco743	1.3.6.1.4.1.9.1.96	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco744	1.3.6.1.4.1.9.1.97	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco751	1.3.6.1.4.1.9.1.81	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco752	1.3.6.1.4.1.9.1.82	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco753	1.3.6.1.4.1.9.1.83	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco761	1.3.6.1.4.1.9.1.98	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco762	1.3.6.1.4.1.9.1.99	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco765	1.3.6.1.4.1.9.1.102	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco766	1.3.6.1.4.1.9.1.103	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco771	1.3.6.1.4.1.9.1.126	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco772	1.3.6.1.4.1.9.1.127	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco775	1.3.6.1.4.1.9.1.128	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco776	1.3.6.1.4.1.9.1.129	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco801	1.3.6.1.4.1.9.1.212	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco802	1.3.6.1.4.1.9.1.213	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco802J	1.3.6.1.4.1.9.1.295	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco803	1.3.6.1.4.1.9.1.214	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco804	1.3.6.1.4.1.9.1.215	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Cisco804J	1.3.6.1.4.1.9.1.296	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco805	1.3.6.1.4.1.9.1.245	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco806	1.3.6.1.4.1.9.1.384	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco811	1.3.6.1.4.1.9.1.395	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco813	1.3.6.1.4.1.9.1.396	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco826	1.3.6.1.4.1.9.1.322	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco826QuadV	1.3.6.1.4.1.9.1.321	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco827	1.3.6.1.4.1.9.1.284	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco827H	1.3.6.1.4.1.9.1.446	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco827QuadV	1.3.6.1.4.1.9.1.270	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco828	1.3.6.1.4.1.9.1.382	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco831	1.3.6.1.4.1.9.1.497	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco836	1.3.6.1.4.1.9.1.499	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco837	1.3.6.1.4.1.9.1.495	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco871	1.3.6.1.4.1.9.1.571	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco877	1.3.6.1.4.1.9.1.569	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco878	1.3.6.1.4.1.9.1.570	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1000	1.3.6.1.4.1.9.1.40	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Cisco1003	1.3.6.1.4.1.9.1.41	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1004	1.3.6.1.4.1.9.1.44	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1005	1.3.6.1.4.1.9.1.49	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1020	1.3.6.1.4.1.9.1.43	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1401	1.3.6.1.4.1.9.1.206	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1407	1.3.6.1.4.1.9.1.249	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1417	1.3.6.1.4.1.9.1.250	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1502	1.3.6.1.4.1.9.1.161	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1503	1.3.6.1.4.1.9.1.160	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1538M	1.3.6.1.4.1.9.1.224	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1548M	1.3.6.1.4.1.9.1.225	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1601	1.3.6.1.4.1.9.1.113	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1602	1.3.6.1.4.1.9.1.114	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1603	1.3.6.1.4.1.9.1.115	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1604	1.3.6.1.4.1.9.1.116	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1605	1.3.6.1.4.1.9.1.172	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1701ADSLBRI	1.3.6.1.4.1.9.1.550	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1710	1.3.6.1.4.1.9.1.200	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Cisco1711	1.3.6.1.4.1.9.1.538	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1712	1.3.6.1.4.1.9.1.539	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1720	1.3.6.1.4.1.9.1.201	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1721	1.3.6.1.4.1.9.1.444	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1750	1.3.6.1.4.1.9.1.216	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1751	1.3.6.1.4.1.9.1.326	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1760	1.3.6.1.4.1.9.1.416	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1801	1.3.6.1.4.1.9.1.638	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1811	1.3.6.1.4.1.9.1.641	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1812	1.3.6.1.4.1.9.1.642	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco1841	1.3.6.1.4.1.9.1.620	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2000	1.3.6.1.4.1.9.1.10	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2102	1.3.6.1.4.1.9.1.15	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2202	1.3.6.1.4.1.9.1.16	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2500	1.3.6.1.4.1.9.1.13	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2501	1.3.6.1.4.1.9.1.17	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2502	1.3.6.1.4.1.9.1.18	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2503	1.3.6.1.4.1.9.1.19	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Cisco2504	1.3.6.1.4.1.9.1.20	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2505	1.3.6.1.4.1.9.1.21	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2506	1.3.6.1.4.1.9.1.22	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2507	1.3.6.1.4.1.9.1.23	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2508	1.3.6.1.4.1.9.1.24	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2509	1.3.6.1.4.1.9.1.25	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2501FRADFX	1.3.6.1.4.1.9.1.165	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2501LANFRADFX	1.3.6.1.4.1.9.1.166	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2502LANFRADFX	1.3.6.1.4.1.9.1.167	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2510	1.3.6.1.4.1.9.1.26	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2511	1.3.6.1.4.1.9.1.27	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2512	1.3.6.1.4.1.9.1.28	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2513	1.3.6.1.4.1.9.1.29	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2514	1.3.6.1.4.1.9.1.30	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2515	1.3.6.1.4.1.9.1.31	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2516	1.3.6.1.4.1.9.1.42	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2517	1.3.6.1.4.1.9.1.67	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2518	1.3.6.1.4.1.9.1.68	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Cisco2519	1.3.6.1.4.1.9.1.69	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2520	1.3.6.1.4.1.9.1.70	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2521	1.3.6.1.4.1.9.1.71	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2522	1.3.6.1.4.1.9.1.72	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2523	1.3.6.1.4.1.9.1.73	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2524	1.3.6.1.4.1.9.1.74	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2525	1.3.6.1.4.1.9.1.75	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2610	1.3.6.1.4.1.9.1.185	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2610M	1.3.6.1.4.1.9.1.418	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2610XM	1.3.6.1.4.1.9.1.466	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2611	1.3.6.1.4.1.9.1.186	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2611M	1.3.6.1.4.1.9.1.419	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2611XM	1.3.6.1.4.1.9.1.467	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2612	1.3.6.1.4.1.9.1.187	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2613	1.3.6.1.4.1.9.1.195	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2620	1.3.6.1.4.1.9.1.208	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2620XM	1.3.6.1.4.1.9.1.468	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2621	1.3.6.1.4.1.9.1.209	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Cisco2621XM	1.3.6.1.4.1.9.1.469	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2650	1.3.6.1.4.1.9.1.319	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2650XM	1.3.6.1.4.1.9.1.470	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2651	1.3.6.1.4.1.9.1.320	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2651XM	1.3.6.1.4.1.9.1.471	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2691	1.3.6.1.4.1.9.1.413	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2801	1.3.6.1.4.1.9.1.619	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2811	1.3.6.1.4.1.9.1.576	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2821	1.3.6.1.4.1.9.1.577	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco2851	1.3.6.1.4.1.9.1.578	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco3000	1.3.6.1.4.1.9.1.6	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco3101	1.3.6.1.4.1.9.1.32	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco3102	1.3.6.1.4.1.9.1.33	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco3103	1.3.6.1.4.1.9.1.34	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco3104	1.3.6.1.4.1.9.1.35	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco3202	1.3.6.1.4.1.9.1.36	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco3204	1.3.6.1.4.1.9.1.37	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco3220	1.3.6.1.4.1.9.1.553	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Cisco3250	1.3.6.1.4.1.9.1.479	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco3620	1.3.6.1.4.1.9.1.122	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco3640	1.3.6.1.4.1.9.1.110	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco3660	1.3.6.1.4.1.9.1.205	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco3661Ac	1.3.6.1.4.1.9.1.338	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco3661Dc	1.3.6.1.4.1.9.1.339	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco3662Ac	1.3.6.1.4.1.9.1.340	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco3662AcCo	1.3.6.1.4.1.9.1.342	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco3662Dc	1.3.6.1.4.1.9.1.341	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco3662DcCo	1.3.6.1.4.1.9.1.343	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco371098-HP001	1.3.6.1.4.1.9.1.625	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco371098-HP001	1.3.6.1.4.1.11.2.3.7.11.33.3.1.1	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco3725	1.3.6.1.4.1.9.1.414	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco3745	1.3.6.1.4.1.9.1.436	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco3825	1.3.6.1.4.1.9.1.543	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco3845	1.3.6.1.4.1.9.1.544	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco4000	1.3.6.1.4.1.9.1.7	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco4224	1.3.6.1.4.1.9.1.399	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Cisco4500	1.3.6.1.4.1.9.1.14	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco4700	1.3.6.1.4.1.9.1.50	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco6015	1.3.6.1.4.1.9.1.299	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco6100	1.3.6.1.4.1.9.1.251	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco6130	1.3.6.1.4.1.9.1.252	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco6160	1.3.6.1.4.1.9.1.297	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco6200	1.3.6.1.4.1.9.1.192	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco6260	1.3.6.1.4.1.9.1.253	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco6400	1.3.6.1.4.1.9.1.180	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco6400Nrp	1.3.6.1.4.1.9.1.211	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco6400UAC	1.3.6.1.4.1.9.1.464	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7000	1.3.6.1.4.1.9.1.8	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7010	1.3.6.1.4.1.9.1.12	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7120Ae3	1.3.6.1.4.1.9.1.263	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7120At3	1.3.6.1.4.1.9.1.262	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7120E3	1.3.6.1.4.1.9.1.261	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7120Quadt1	1.3.6.1.4.1.9.1.259	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7120Smi3	1.3.6.1.4.1.9.1.264	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Cisco7120T3	1.3.6.1.4.1.9.1.260	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7140Dualae3	1.3.6.1.4.1.9.1.268	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7140Dualat3	1.3.6.1.4.1.9.1.267	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7140Duale3	1.3.6.1.4.1.9.1.266	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7140Dualfe	1.3.6.1.4.1.9.1.277	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7140Dualmm3	1.3.6.1.4.1.9.1.269	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7140Dualt3	1.3.6.1.4.1.9.1.265	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7140Octt1	1.3.6.1.4.1.9.1.276	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7150Dualfe	1.3.6.1.4.1.9.1.355	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7150Dualt3	1.3.6.1.4.1.9.1.357	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7150Octt1	1.3.6.1.4.1.9.1.356	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7202	1.3.6.1.4.1.9.1.194	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7204	1.3.6.1.4.1.9.1.125	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7204VXR	1.3.6.1.4.1.9.1.223	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7206	1.3.6.1.4.1.9.1.108	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7206VXR	1.3.6.1.4.1.9.1.222	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
UBR_7246	1.3.6.1.4.1.9.1.179	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7301	1.3.6.1.4.1.9.1.476	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Cisco7304	1.3.6.1.4.1.9.1.439	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7401ASR	1.3.6.1.4.1.9.1.403	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7401VXR	1.3.6.1.4.1.9.1.376	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7505	1.3.6.1.4.1.9.1.48	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7507z	1.3.6.1.4.1.9.1.288	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7506	1.3.6.1.4.1.9.1.47	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7507	1.3.6.1.4.1.9.1.45	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7507mx	1.3.6.1.4.1.9.1.290	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7513	1.3.6.1.4.1.9.1.46	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7513mx	1.3.6.1.4.1.9.1.291	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7513z	1.3.6.1.4.1.9.1.289	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7576	1.3.6.1.4.1.9.1.204	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7603	1.3.6.1.4.1.9.1.401	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7604	1.3.6.1.4.1.9.1.658	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7606	1.3.6.1.4.1.9.1.402	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7609	1.3.6.1.4.1.9.1.509	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco7613	1.3.6.1.4.1.9.1.528	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco9004	1.3.6.1.4.1.9.1.424	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Cisco10005	1.3.6.1.4.1.9.1.437	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco10008	1.3.6.1.4.1.9.1.438	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco10400	1.3.6.1.4.1.9.1.272	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco10720	1.3.6.1.4.1.9.1.397	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco12004	1.3.6.1.4.1.9.1.181	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco12006	1.3.6.1.4.1.9.1.590	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco12008	1.3.6.1.4.1.9.1.182	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco12010	1.3.6.1.4.1.9.1.348	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco12012	1.3.6.1.4.1.9.1.173	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco12016	1.3.6.1.4.1.9.1.273	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco12404	1.3.6.1.4.1.9.1.423	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco12406	1.3.6.1.4.1.9.1.388	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco12410	1.3.6.1.4.1.9.1.394	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco12416	1.3.6.1.4.1.9.1.385	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco3631Co	1.3.6.1.4.1.9.1.425	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoAGS+	1.3.6.1.4.1.9.1.11	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoAPEC	1.3.6.1.4.1.9.1.39	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoAPRC	1.3.6.1.4.1.9.1.38	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
CiscoAS5200	1.3.6.1.4.1.9.1.109	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoAS5300	1.3.6.1.4.1.9.1.162	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoAS5350	1.3.6.1.4.1.9.1.313	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoAS5350XM	1.3.6.1.4.1.9.1.679	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoAS5400	1.3.6.1.4.1.9.1.274	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoAS5400XM	1.3.6.1.4.1.9.1.668	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoAS5800	1.3.6.1.4.1.9.1.188	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoAS5850	1.3.6.1.4.1.9.1.308	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoCacheEngine	1.3.6.1.4.1.9.1.240	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoCrs1Fabric	1.3.6.1.4.1.9.1.739	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoCRS16S	1.3.6.1.4.1.9.1.613	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoCrs18LineCard	1.3.6.1.4.1.9.1.738	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoCRS8S	1.3.6.1.4.1.9.1.643	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoCS500	1.3.6.1.4.1.9.1.9	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoFastHubBMMFX	1.3.6.1.4.1.9.1.178	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoFastHubBMMTX	1.3.6.1.4.1.9.1.177	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoFastHub216T	1.3.6.1.4.1.9.1.169	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoGS	1.3.6.1.4.1.9.1.1	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
CiscoIGESM	1.3.6.1.4.1.9.1.592	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoIGS	1.3.6.1.4.1.9.1.5	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoLocalDirector	1.3.6.1.4.1.9.1.244	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco MC3810	1.3.6.1.4.1.9.1.286	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cisco MC3810	1.3.6.1.4.1.9.1.157	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoME6340ACA	1.3.6.1.4.1.9.1.713	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoME6340DCA	1.3.6.1.4.1.9.1.714	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoME6340DCB	1.3.6.1.4.1.9.1.715	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoMicroWebServer2	1.3.6.1.4.1.9.1.176	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoMWR1900	1.3.6.1.4.1.9.1.398	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoMWR1941DC	1.3.6.1.4.1.9.1.520	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoOlympus	1.3.6.1.4.1.9.1.358	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoOpticalRegenerator	1.3.6.1.4.1.9.1.254	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro316C	1.3.6.1.4.1.9.1.148	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro316T	1.3.6.1.4.1.9.1.147	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro741	1.3.6.1.4.1.9.1.84	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro742	1.3.6.1.4.1.9.1.85	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro743	1.3.6.1.4.1.9.1.86	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
CiscoPro744	1.3.6.1.4.1.9.1.87	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro751	1.3.6.1.4.1.9.1.76	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro752	1.3.6.1.4.1.9.1.77	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro753	1.3.6.1.4.1.9.1.78	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro761	1.3.6.1.4.1.9.1.88	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro762	1.3.6.1.4.1.9.1.89	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro765	1.3.6.1.4.1.9.1.92	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro766	1.3.6.1.4.1.9.1.93	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro1003	1.3.6.1.4.1.9.1.51	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro1004	1.3.6.1.4.1.9.1.52	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro1005	1.3.6.1.4.1.9.1.53	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro1020	1.3.6.1.4.1.9.1.54	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro1601	1.3.6.1.4.1.9.1.117	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro1602	1.3.6.1.4.1.9.1.118	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro1603	1.3.6.1.4.1.9.1.119	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro1604	1.3.6.1.4.1.9.1.120	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro2500PCE	1.3.6.1.4.1.9.1.55	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro2501	1.3.6.1.4.1.9.1.56	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
CiscoPro2502	1.3.6.1.4.1.9.1.130	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro2503	1.3.6.1.4.1.9.1.57	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro2504	1.3.6.1.4.1.9.1.131	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro2505	1.3.6.1.4.1.9.1.58	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro2506	1.3.6.1.4.1.9.1.132	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro2507	1.3.6.1.4.1.9.1.59	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro2508	1.3.6.1.4.1.9.1.133	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro2509	1.3.6.1.4.1.9.1.60	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro2510	1.3.6.1.4.1.9.1.134	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro2511	1.3.6.1.4.1.9.1.61	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro2512	1.3.6.1.4.1.9.1.135	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro2513	1.3.6.1.4.1.9.1.136	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro2514	1.3.6.1.4.1.9.1.62	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro2515	1.3.6.1.4.1.9.1.137	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro2516	1.3.6.1.4.1.9.1.63	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro2517	1.3.6.1.4.1.9.1.138	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro2518	1.3.6.1.4.1.9.1.139	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro2519	1.3.6.1.4.1.9.1.64	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
CiscoPro2520	1.3.6.1.4.1.9.1.104	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro2521	1.3.6.1.4.1.9.1.65	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro2522	1.3.6.1.4.1.9.1.105	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro2523	1.3.6.1.4.1.9.1.140	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro2524	1.3.6.1.4.1.9.1.106	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro2525	1.3.6.1.4.1.9.1.141	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro3116	1.3.6.1.4.1.9.1.149	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro3620	1.3.6.1.4.1.9.1.123	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro3640	1.3.6.1.4.1.9.1.124	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro4500	1.3.6.1.4.1.9.1.66	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoPro4700	1.3.6.1.4.1.9.1.142	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoProtocolTranslator	1.3.6.1.4.1.9.1.4	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoRPM	1.3.6.1.4.1.9.1.199	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoRPMPR	1.3.6.1.4.1.9.1.457	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoRpmXf	1.3.6.1.4.1.9.1.440	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoSC3640	1.3.6.1.4.1.9.1.189	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoSN5420	1.3.6.1.4.1.9.1.407	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoSN5428	1.3.6.1.4.1.9.1.475	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
CiscoSOHO76	1.3.6.1.4.1.9.1.354	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoSOHO91	1.3.6.1.4.1.9.1.498	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoSOHO97	1.3.6.1.4.1.9.1.496	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoSOHO77	1.3.6.1.4.1.9.1.353	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoSOHO96	1.3.6.1.4.1.9.1.500	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoTrouter	1.3.6.1.4.1.9.1.3	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoTS	1.3.6.1.4.1.9.1.2	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoWS3020Hpq	1.3.6.1.4.1.9.1.748	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoWS3030Del	1.3.6.1.4.1.9.1.749	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoWSC3750G-24PS	1.3.6.1.4.1.9.1.747	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoWSC6504E	1.3.6.1.4.1.9.1.657	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoWSC6509neba	1.3.6.1.4.1.9.1.534	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoWSX3011	1.3.6.1.4.1.9.1.112	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoWSX5302	1.3.6.1.4.1.9.1.168	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoWSX6302Msm	1.3.6.1.4.1.9.1.256	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoURM	1.3.6.1.4.1.9.1.373	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoURM2FE	1.3.6.1.4.1.9.1.374	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CiscoURM2FE2V	1.3.6.1.4.1.9.1.375	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
AP 1130	1.3.6.1.4.1.9.1.618	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
LS_1010	1.3.6.1.4.1.9.1.107	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
LS_1015	1.3.6.1.4.1.9.1.164	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
UBR_7223	1.3.6.1.4.1.9.1.210	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
UBR_7246VXR	1.3.6.1.4.1.9.1.271	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
UBR_904	1.3.6.1.4.1.9.1.191	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
UBR_924	1.3.6.1.4.1.9.1.255	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
UBR_912C	1.3.6.1.4.1.9.1.292	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
UBR_912S	1.3.6.1.4.1.9.1.293	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
UBR_914	1.3.6.1.4.1.9.1.294	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
UBR_925	1.3.6.1.4.1.9.1.316	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
UBR_10012	1.3.6.1.4.1.9.1.317	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
UBR_7111	1.3.6.1.4.1.9.1.344	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
UBR_7111E	1.3.6.1.4.1.9.1.345	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
UBR_7114	1.3.6.1.4.1.9.1.346	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
UBR_7114E	1.3.6.1.4.1.9.1.347	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
UBR_905	1.3.6.1.4.1.9.1.351	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
350 AP	1.3.6.1.4.1.9.1.552	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
1100 AP	1.3.6.1.4.1.9.1.507	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
1210/1230 AP	1.3.6.1.4.1.9.1.525	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
1240 AP	1.3.6.1.4.1.9.1.685	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
1400 AP	1.3.6.1.4.1.9.1.533	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
1300 AP	1.3.6.1.4.1.9.1.565	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
PIX Firewall	1.3.6.1.4.1.9.1.227	no	no	no	Telnet
PIX 506 Firewall	1.3.6.1.4.1.9.1.389	no	no	no	Telnet
PIX 515 Firewall	1.3.6.1.4.1.9.1.390	no	no	no	Telnet
PIX 520 Firewall	1.3.6.1.4.1.9.1.391	no	no	no	Telnet
PIX 525 Firewall	1.3.6.1.4.1.9.1.392	no	no	no	Telnet
PIX 535 Firewall	1.3.6.1.4.1.9.1.393	no	no	no	Telnet
PIX 501 Firewall	1.3.6.1.4.1.9.1.417	no	no	no	Telnet
PIX 515E Firewall	1.3.6.1.4.1.9.1.451	no	no	no	Telnet
PIX 506E Firewall	1.3.6.1.4.1.9.1.450	no	no	no	Telnet
cat6500FirewallSm	1.3.6.1.4.1.9.1.522	no	no	no	Telnet
PIX Firewall Security Module	1.3.6.1.4.1.9.1.674	no	no	no	Telnet
PIX 535sc Firewall	1.3.6.1.4.1.9.1.675	no	no	no	Telnet
PIX 525sc Firewall	1.3.6.1.4.1.9.1.676	no	no	no	Telnet
PIX 515Esc Firewall	1.3.6.1.4.1.9.1.677	no	no	no	Telnet
PIX 515sc Firewall	1.3.6.1.4.1.9.1.678	no	no	no	Telnet
PIX Firewall System Module	1.3.6.1.4.1.9.1.767	no	no	no	Telnet
PIX 515sy Firewall	1.3.6.1.4.1.9.1.768	no	no	no	Telnet
PIX 515Esy Firewall	1.3.6.1.4.1.9.1.769	no	no	no	Telnet

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
PIX 525sy Firewall	1.3.6.1.4.1.9.1.770	no	no	no	Telnet
PIX 535sy Firewall	1.3.6.1.4.1.9.1.771	no	no	no	Telnet

* IOS < 12.0 = OLD-CISCO-SYSTEM-MIB

** IOS > 12.2(18) with feature “K9”

Cisco Supported Devices

The CA Spectrum Network Configuration Manager supports the following Cisco Catalyst devices. For a list of other supported Cisco devices, see Cisco Supported Devices (see page 157). For a list of PIX Firewall devices, see Cisco Supported PIX Firewall Devices (see page 185).

The table provides examples. For the most up-to-date information on device support, access the CA Device Certification database (see page 16).

When a Perl script is the only means of communication with the device, the script method is provided.

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Cat116T	1.3.6.1.4.1.9.1.150	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat116C	1.3.6.1.4.1.9.1.151	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat1116	1.3.6.1.4.1.9.1.152	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat1912C	1.3.6.1.4.1.9.1.175	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat2924XL	1.3.6.1.4.1.9.1.183	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat2924CXL	1.3.6.1.4.1.9.1.184	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat2924XLv	1.3.6.1.4.1.9.1.217	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Cat2640-48TT	1.3.6.1.4.1.9.1.717	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat2948gL3	1.3.6.1.4.1.9.1.275	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat2948gL3Dc	1.3.6.1.4.1.9.1.386	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat2960-24TC	1.3.6.1.4.1.9.1.694	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat2960-24TT	1.3.6.1.4.1.9.1.716	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat2960G-24TC	1.3.6.1.4.1.9.1.696	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat2960-48TC	1.3.6.1.4.1.9.1.695	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat297024	1.3.6.1.4.1.9.1.527	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat297024TS	1.3.6.1.4.1.9.1.561	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat2908xl	1.3.6.1.4.1.9.1.170	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat2912LREXL	1.3.6.1.4.1.9.1.370	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat2912MfXL	1.3.6.1.4.1.9.1.221	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat2912XL	1.3.6.1.4.1.9.1.219	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat2916mxl	1.3.6.1.4.1.9.1.171	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat2924CXLv	1.3.6.1.4.1.9.1.218	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat2924MXL	1.3.6.1.4.1.9.1.220	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat295012	1.3.6.1.4.1.9.1.323	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat295024	1.3.6.1.4.1.9.1.324	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Cat295024C	1.3.6.1.4.1.9.1.325	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat2950t24	1.3.6.1.4.1.9.1.359	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat2924LREXL	1.3.6.1.4.1.9.1.369	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat295012G	1.3.6.1.4.1.9.1.427	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat295024G	1.3.6.1.4.1.9.1.428	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat295048G	1.3.6.1.4.1.9.1.429	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat_3500	1.3.6.1.4.1.9.1.111	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat_3508GXL	1.3.6.1.4.1.9.1.246	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat_3512XL	1.3.6.1.4.1.9.1.247	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat_3524XL	1.3.6.1.4.1.9.1.248	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat_3524tXLEn	1.3.6.1.4.1.9.1.287	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat_3548XL	1.3.6.1.4.1.9.1.278	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat355012G	1.3.6.1.4.1.9.1.431	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat355012T	1.3.6.1.4.1.9.1.368	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat355024	1.3.6.1.4.1.9.1.366	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat355048	1.3.6.1.4.1.9.1.367	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat355024Dc	1.3.6.1.4.1.9.1.452	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat355024Mmf	1.3.6.1.4.1.9.1.453	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Cat355024PWR	1.3.6.1.4.1.9.1.485	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat3560_24PS	1.3.6.1.4.1.9.1.563	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat3560G-24PS	1.3.6.1.4.1.9.1.614	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat3560-24TS	1.3.6.1.4.1.9.1.633	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat3560G-24TS	1.3.6.1.4.1.9.1.615	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat3560_48PS	1.3.6.1.4.1.9.1.564	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat3560G-48PS	1.3.6.1.4.1.9.1.616	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat3560-48TS	1.3.6.1.4.1.9.1.634	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat3560G-48TS	1.3.6.1.4.1.9.1.617	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat37xxStack	1.3.6.1.4.1.9.1.516	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat3750Ge12Sfp	1.3.6.1.4.1.9.1.530	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat3750_24ME	1.3.6.1.4.1.9.1.574	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat3750G16TD	1.3.6.1.4.1.9.1.591	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat375024	1.3.6.1.4.1.9.1.511	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat375024T	1.3.6.1.4.1.9.1.514	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat375024TS	1.3.6.1.4.1.9.1.513	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat375048	1.3.6.1.4.1.9.1.512	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat4kGateway	1.3.6.1.4.1.9.1.318	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Cat4000NAM	1.3.6.1.4.1.9.1.575	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat4006	1.3.6.1.4.1.9.1.448	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat4503	1.3.6.1.4.1.9.1.503	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat4510	1.3.6.1.4.1.9.1.537	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat4232L3	1.3.6.1.4.1.9.1.300	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat4506	1.3.6.1.4.1.9.1.502	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat4507	1.3.6.1.4.1.9.1.501	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat4840gL3	1.3.6.1.4.1.9.1.312	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat4908gL3	1.3.6.1.4.1.9.1.298	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat4908gL3Dc	1.3.6.1.4.1.9.1.387	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat4948	1.3.6.1.4.1.9.1.626	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat494810GE	1.3.6.1.4.1.9.1.659	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat5kRsfc	1.3.6.1.4.1.9.1.257	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat6kSup720	1.3.6.1.4.1.9.1.557	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat6kGateway	1.3.6.1.4.1.9.1.573	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat6503	1.3.6.1.4.1.9.1.449	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat6513	1.3.6.1.4.1.9.1.400	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat6000	1.3.6.1.4.1.9.1.241	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Cat6006	1.3.6.1.4.1.9.1.280	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat6009	1.3.6.1.4.1.9.1.281	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat6506	1.3.6.1.4.1.9.1.282	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat6509	1.3.6.1.4.1.9.1.283	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat6kMsfc	1.3.6.1.4.1.9.1.258	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat6kMsfc2	1.3.6.1.4.1.9.1.301	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat6509Sp	1.3.6.1.4.1.9.1.310	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat8510_CSR	1.3.6.1.4.1.9.1.190	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat8510_MSR	1.3.6.1.4.1.9.1.230	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat8515_CSR	1.3.6.1.4.1.9.1.196	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat8515_MSR	1.3.6.1.4.1.9.1.231	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat8540_CSR	1.3.6.1.4.1.9.1.203	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat8540_MSR	1.3.6.1.4.1.9.1.202	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat9006	1.3.6.1.4.1.9.1.197	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat9009	1.3.6.1.4.1.9.1.198	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat295024GDC	1.3.6.1.4.1.9.1.472	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat295024S	1.3.6.1.4.1.9.1.430	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat295024SX	1.3.6.1.4.1.9.1.480	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Cat295024LREG	1.3.6.1.4.1.9.1.484	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat295024LRESt	1.3.6.1.4.1.9.1.482	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat29508LRESt	1.3.6.1.4.1.9.1.483	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat2955C12	1.3.6.1.4.1.9.1.489	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat2955S12	1.3.6.1.4.1.9.1.508	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat2955T12	1.3.6.1.4.1.9.1.488	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat29408TF	1.3.6.1.4.1.9.1.542	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat29408TT	1.3.6.1.4.1.9.1.540	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat295048SX	1.3.6.1.4.1.9.1.560	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat295048T	1.3.6.1.4.1.9.1.559	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
Cat2950St24LRE997	1.3.6.1.4.1.9.1.551	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CatExpress500-24LC	1.3.6.1.4.1.9.1.725	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CatExpress500-12TC	1.3.6.1.4.1.9.1.727	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CatExpress500-24PC	1.3.6.1.4.1.9.1.726	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CatExpress500-24TT	1.3.6.1.4.1.9.1.724	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes
CatWsCBS3040FSC	1.3.6.1.4.1.9.1.784	*CISCO-CONFIG-COPY-MIB	yes	**yes	yes

* IOS < 12.0 = OLD-CISCO-SYSTEM-MIB

** IOS > 12.2(18) with feature “K9”

Cisco Supported Devices

The CA Spectrum Network Configuration Manager supports the following Cisco devices. For a list of supported Catalyst devices, see Cisco Supported Catalyst Devices.

The table provides examples. For the most up-to-date information on device support, access the CA Device Certification database (see page 16).

When a Perl script is the only means of communication with the device, the script method is provided.

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
PIX Firewall	1.3.6.1.4.1.9.1.227	no	no	no	Telnet
PIX 506 Firewall	1.3.6.1.4.1.9.1.389	no	no	no	Telnet
PIX 515 Firewall	1.3.6.1.4.1.9.1.390	no	no	no	Telnet
PIX 520 Firewall	1.3.6.1.4.1.9.1.391	no	no	no	Telnet
PIX 525 Firewall	1.3.6.1.4.1.9.1.392	no	no	no	Telnet
PIX 535 Firewall	1.3.6.1.4.1.9.1.393	no	no	no	Telnet
PIX 501 Firewall	1.3.6.1.4.1.9.1.417	no	no	no	Telnet
PIX 515E Firewall	1.3.6.1.4.1.9.1.451	no	no	no	Telnet
PIX 506E Firewall	1.3.6.1.4.1.9.1.450	no	no	no	Telnet
cat6500FirewallSm	1.3.6.1.4.1.9.1.522	no	no	no	Telnet
PIX Firewall Security Module	1.3.6.1.4.1.9.1.674	no	no	no	Telnet
PIX 535sc Firewall	1.3.6.1.4.1.9.1.675	no	no	no	Telnet
PIX 525sc Firewall	1.3.6.1.4.1.9.1.676	no	no	no	Telnet
PIX 515Esc Firewall	1.3.6.1.4.1.9.1.677	no	no	no	Telnet
PIX 515sc Firewall	1.3.6.1.4.1.9.1.678	no	no	no	Telnet
PIX Firewall System Module	1.3.6.1.4.1.9.1.767	no	no	no	Telnet
PIX 515sy Firewall	1.3.6.1.4.1.9.1.768	no	no	no	Telnet
PIX 515Esy Firewall	1.3.6.1.4.1.9.1.769	no	no	no	Telnet

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
PIX 525sy Firewall	1.3.6.1.4.1.9.1.770	no	no	no	Telnet
PIX 535sy Firewall	1.3.6.1.4.1.9.1.771	no	no	no	Telnet

* IOS < 12.0 = OLD-CISCO-SYSTEM-MIB

** IOS > 12.2(18) with feature “K9”

Cisco CAT Supported Devices

The following table lists Cisco CAT devices supported by CA Spectrum Network Configuration Manager. The table provides examples. For the most up-to-date information on device support, access the CA Device Certification database (see page 16).

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Cat2926	1.3.6.1.4.1.9.5.35	CISCO-CONFIG-COPY-MIB*	no	no	yes
Cat_2948G	1.3.6.1.4.1.9.5.42	CISCO-CONFIG-COPY-MIB*	no	no	yes
Cat2948ggetx	1.3.6.1.4.1.9.5.62	CISCO-CONFIG-COPY-MIB*	no	no	yes
Cat2980ga	1.3.6.1.4.1.9.5.51	CISCO-CONFIG-COPY-MIB*	no	no	yes
Cat_2980GSW	1.3.6.1.4.1.9.5.49	CISCO-CONFIG-COPY-MIB*	no	no	yes
Cat_4003	1.3.6.1.4.1.9.5.40	CISCO-CONFIG-COPY-MIB*	no	no	yes
Cat_4006	1.3.6.1.4.1.9.5.46	CISCO-CONFIG-COPY-MIB*	no	no	yes
Cat4503	1.3.6.1.4.1.9.5.58	CISCO-CONFIG-COPY-MIB*	no	no	yes
Cat_4506	1.3.6.1.4.1.9.5.59	CISCO-CONFIG-COPY-MIB*	no	no	yes
Cat4912	1.3.6.1.4.1.9.5.41	CISCO-CONFIG-COPY-MIB*	no	no	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Cat6knam	1.3.6.1.4.1.9.5.48	CISCO-CONFIG-COPY-MIB*	no	no	yes
Cat6503	1.3.6.1.4.1.9.5.56	CISCO-CONFIG-COPY-MIB*	no	no	yes
Cat6509neba	1.3.6.1.4.1.9.5.61	CISCO-CONFIG-COPY-MIB*	no	no	yes
Cat7603	1.3.6.1.4.1.9.5.53	CISCO-CONFIG-COPY-MIB*	no	no	yes
Cat7604	1.3.6.1.4.1.9.5.63	CISCO-CONFIG-COPY-MIB*	no	no	yes
Cat7606	1.3.6.1.4.1.9.5.54	CISCO-CONFIG-COPY-MIB*	no	no	yes
Cat7609	1.3.6.1.4.1.9.5.55	CISCO-CONFIG-COPY-MIB*	no	no	yes
Cat7613	1.3.6.1.4.1.9.5.60	CISCO-CONFIG-COPY-MIB*	no	no	yes
CiscoWSC6504E	1.3.6.1.4.1.9.5.64	CISCO-CONFIG-COPY-MIB*	no	no	yes
HubCat1400	1.3.6.1.4.1.9.5.6	CISCO-CONFIG-COPY-MIB*	no	no	yes
HubCat5000	1.3.6.1.4.1.9.5.7	CISCO-CONFIG-COPY-MIB*	no	no	yes
HubCat5002	1.3.6.1.4.1.9.5.29	CISCO-CONFIG-COPY-MIB*	no	no	yes
HubCat5500	1.3.6.1.4.1.9.5.17	CISCO-CONFIG-COPY-MIB*	no	no	yes
HubCat5505	1.3.6.1.4.1.9.5.34	CISCO-CONFIG-COPY-MIB*	no	no	yes
HubCat5509	1.3.6.1.4.1.9.5.36	CISCO-CONFIG-COPY-MIB*	no	no	yes
SwCat1200	1.3.6.1.4.1.9.5.5	CISCO-CONFIG-COPY-MIB*	no	no	yes
WS-C6006	1.3.6.1.4.1.9.5.38	CISCO-CONFIG-COPY-MIB*	no	no	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
WS-C6009	1.3.6.1.4.1.9.5.39	CISCO-CONFIG-COPY-MIB*	no	no	yes
WS-C6506	1.3.6.1.4.1.9.5.45	CISCO-CONFIG-COPY-MIB*	no	no	yes
WS-C6509	1.3.6.1.4.1.9.5.44	CISCO-CONFIG-COPY-MIB*	no	no	yes
WS-C6509neb	1.3.6.1.4.1.9.5.47	CISCO-CONFIG-COPY-MIB*	no	no	yes
WS-C6513	1.3.6.1.4.1.9.5.50	CISCO-CONFIG-COPY-MIB*	no	no	yes

* CATOS < 8.4 = CISCO-STACK-MIB

Cisco NX OS Supported Devices

The following table lists Cisco NX OS devices supported by CA Spectrum Network Configuration Manager.

Note: Cisco NX OS devices are supported through scripts that utilize the Net::SSH::Expect modules. The Perl area must be set up with these modules for out-of box support for Cisco NX OS devices.

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Cisco Nexus 1000V VSM	1.3.6.1.4.1.9.12.3.1.3.840	no	no	no	yes
Cisco Nexus 2000	1.3.6.1.4.1.9.12.3.1.3.820	no	no	no	yes
Cisco Nexus 5000	1.3.6.1.4.1.9.12.3.1.3.719	no	no	no	yes
Cisco Nexus 7000	1.3.6.1.4.1.9.12.3.1.3.612	no	no	no	yes

Enterasys Supported Devices

The following table lists Enterasys devices supported by CA Spectrum Network Configuration Manager. The table provides examples. For the most up-to-date information on device support, access the CA Device Certification database (see page 16).

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
1G582-09	1.3.6.1.4.1.5624.2.1.35	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
1G694-13	1.3.6.1.4.1.5624.2.1.36	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
1H582-25	1.3.6.1.4.1.5624.2.1.59	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
1H582-51	1.3.6.1.4.1.5624.2.1.34	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
1G587-09	1.3.6.1.4.1.5624.2.1.60	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
Matrix N	1.3.6.1.4.1.5624.2.1.51	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
Matrix N1	1.3.6.1.4.1.5624.2.1.83	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
Matrix N3	1.3.6.1.4.1.5624.2.1.53	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
Matrix N5	1.3.6.1.4.1.5624.2.1.79	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
Matrix N7	1.3.6.1.4.1.5624.2.1.52	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
Matrix N Router	1.3.6.1.4.1.5624.2.1.70	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
Matrix N Standalone	1.3.6.1.4.1.5624.2.1.77	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack A2H124-24	1.3.6.1.4.1.5624.2.1.87	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack A2H124-24FX	1.3.6.1.4.1.5624.2.1.91	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack A2H124-24P	1.3.6.1.4.1.5624.2.1.88	ENTERASYS-CONFIG-MAN-MIB	no	no	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
SecureStack A2H124-48	1.3.6.1.4.1.5624.2.1.89	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack A2H124-48P	1.3.6.1.4.1.5624.2.1.90	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack A2H254-16	1.3.6.1.4.1.5624.2.1.95	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack B2G124-24	1.3.6.1.4.1.5624.2.2.314	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack B2G124-48	1.3.6.1.4.1.5624.2.2.315	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack B2G124-48P	1.3.6.1.4.1.5624.2.2.316	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack B2H124-48	1.3.6.1.4.1.5624.2.2.317	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack B2H124-48P	1.3.6.1.4.1.5624.2.2.318	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack B3G124-24	1.3.6.1.4.1.5624.2.1.100	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack B3G124-24P	1.3.6.1.4.1.5624.2.1.101	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack B3G124-48	1.3.6.1.4.1.5624.2.1.102	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack B3G124-48P	1.3.6.1.4.1.5624.2.1.103	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack C2G124-24	1.3.6.1.4.1.5624.2.2.283	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack C2G124-48	1.3.6.1.4.1.5624.2.2.284	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack C2G124-48P	1.3.6.1.4.1.5624.2.2.287	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack C2G134-24P	1.3.6.1.4.1.5624.2.2.350	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack C2G170-24	1.3.6.1.4.1.5624.2.2.360	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack C2H124-48	1.3.6.1.4.1.5624.2.2.220	ENTERASYS-CONFIG-MAN-MIB	no	no	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
SecureStack C2H124-48P	1.3.6.1.4.1.5624.2.2.286	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack C2K122-24	1.3.6.1.4.1.5624.2.2.285	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack C3G124-24	1.3.6.1.4.1.5624.2.1.96	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack C3G124-24P	1.3.6.1.4.1.5624.2.1.97	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack C3G124-48	1.3.6.1.4.1.5624.2.1.98	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
SecureStack C3G124-48P	1.3.6.1.4.1.5624.2.1.99	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
XSR-1805	1.3.6.1.4.1.5624.2.1.32	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
XSR-1850	1.3.6.1.4.1.5624.2.1.45	ENTERASYS-CONFIG-MAN-MIB	no	no	yes
XSR-1800	1.3.6.1.4.1.5624.2.1	ENTERASYS-CONFIG-MAN-MIB	no	no	yes

Enterasys/Riverstone SSR Supported Devices

The following table lists Enterasys/Riverstone SSR devices supported by CA Spectrum Network Configuration Manager. The table provides examples. For the most up-to-date information on device support, access the CA Device Certification database (see page 16).

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
DEC 8000	1.3.6.1.4.1.36.2.15.30.1	CTRON-SSR-CONFIG-MIB	no	no	yes
DEC 8600	1.3.6.1.4.1.36.2.15.30.2	CTRON-SSR-CONFIG-MIB	no	no	yes
DEC 2000	1.3.6.1.4.1.36.2.15.30.3	CTRON-SSR-CONFIG-MIB	no	no	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
OLI-8000	1.3.6.1.4.1.285.9.25	CTRON-SSR-CONFIG-MIB	no	no	yes
OLI-8600	1.3.6.1.4.1.285.9.26	CTRON-SSR-CONFIG-MIB	no	no	yes
OLI-2000	1.3.6.1.4.1.285.9.27	CTRON-SSR-CONFIG-MIB	no	no	yes
CPQ-8000	1.3.6.1.4.1.232.134.1.1	CTRON-SSR-CONFIG-MIB	no	no	yes
CPQ-8600	1.3.6.1.4.1.232.134.1.2	CTRON-SSR-CONFIG-MIB	no	no	yes
CPQ-2000	1.3.6.1.4.1.232.134.1.3	CTRON-SSR-CONFIG-MIB	no	no	yes
6-SSRM-02	1.3.6.1.4.1.52.3.9.33.4.1	CTRON-SSR-CONFIG-MIB	no	no	yes
RS-8000	1.3.6.1.4.1.5567.1.1.1	CTRON-SSR-CONFIG-MIB	no	no	yes
RS-8600	1.3.6.1.4.1.5567.1.1.2	CTRON-SSR-CONFIG-MIB	no	no	yes
RS-2000	1.3.6.1.4.1.5567.1.1.3	CTRON-SSR-CONFIG-MIB	no	no	yes
RS-2100	1.3.6.1.4.1.5567.1.1.4	CTRON-SSR-CONFIG-MIB	no	no	yes
RS-3000	1.3.6.1.4.1.5567.1.1.5	CTRON-SSR-CONFIG-MIB	no	no	yes
IA-1100	1.3.6.1.4.1.5567.1.1.22	CTRON-SSR-CONFIG-MIB	no	no	yes
IA-1200	1.3.6.1.4.1.5567.1.1.23	CTRON-SSR-CONFIG-MIB	no	no	yes
RS-1000	1.3.6.1.4.1.5567.1.1.8	CTRON-SSR-CONFIG-MIB	no	no	yes
IA-1500	1.3.6.1.4.1.5567.1.1.27	CTRON-SSR-CONFIG-MIB	no	no	yes
SSR-8000	1.3.6.1.4.1.52.3.9.20.1.3	CTRON-SSR-CONFIG-MIB	no	no	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
SSR-8600	1.3.6.1.4.1.52.3.9.20.1.4	CTRON-SSR-CONFIG-MIB	no	no	yes
SSR-2000	1.3.6.1.4.1.52.3.9.33.1.1	CTRON-SSR-CONFIG-MIB	no	no	yes
SSR-2100	1.3.6.1.4.1.52.3.9.33.1.3	CTRON-SSR-CONFIG-MIB	no	no	yes
IA-1000	1.3.6.1.4.1.52.3.9.33.2.8	CTRON-SSR-CONFIG-MIB	no	no	yes
IA-2000	1.3.6.1.4.1.52.3.9.33.2.9	CTRON-SSR-CONFIG-MIB	no	no	yes
XP-2400	1.3.6.1.4.1.5624.2.1.42	CTRON-SSR-CONFIG-MIB	no	no	yes
RS-32000	1.3.6.1.4.1.5567.1.1.6	CTRON-SSR-CONFIG-MIB	no	no	yes
RS-38000	1.3.6.1.4.1.5567.1.1.9	CTRON-SSR-CONFIG-MIB	no	no	yes
SSR-32000	1.3.6.1.4.1.52.10.2	CTRON-SSR-CONFIG-MIB	no	no	yes
ER16	1.3.6.1.4.1.5624.2.1.23	CTRON-SSR-CONFIG-MIB	no	no	yes
BE2800	1.3.6.1.4.1.1456.3.2	CTRON-SSR-CONFIG-MIB	no	no	yes
Terayon Router	1.3.6.1.4.1.1456.3.3	CTRON-SSR-CONFIG-MIB	no	no	yes
5-SSRM-02	1.3.6.1.4.1.5624.2.1.24	CTRON-SSR-CONFIG-MIB	no	no	yes

Extreme Supported Devices

The following table lists Extreme devices supported by CA Spectrum Network Configuration Manager. The table provides examples. For the most up-to-date information on device support, access the CA Device Certification database (see page 16).

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Alpine 3802	1.3.6.1.4.1.1916.2.26	EXTREME-FILETRANSFER-MIB	no	no	yes
Alpine 3804	1.3.6.1.4.1.1916.2.20	EXTREME-FILETRANSFER-MIB	no	no	yes
Alpine 3808	1.3.6.1.4.1.1916.2.17	EXTREME-FILETRANSFER-MIB	no	no	yes
Altitude 300	1.3.6.1.4.1.1916.2.86	EXTREME-FILETRANSFER-MIB	no	no	yes
Altitude 350	1.3.6.1.4.1.1916.2.75	EXTREME-FILETRANSFER-MIB	no	no	yes
BlackDiamond 6800	1.3.6.1.4.1.1916.2.8	EXTREME-FILETRANSFER-MIB	no	no	yes
BlackDiamond 6804	1.3.6.1.4.1.1916.2.27	EXTREME-FILETRANSFER-MIB	no	no	yes
BlackDiamond 6808	1.3.6.1.4.1.1916.2.11	EXTREME-FILETRANSFER-MIB	no	no	yes
BlackDiamond 6816	1.3.6.1.4.1.1916.2.24	EXTREME-FILETRANSFER-MIB	no	no	yes
BlackDiamond 8806	1.3.6.1.4.1.1916.2.74	EXTREME-FILETRANSFER-MIB	no	no	yes
BlackDiamond 8810	1.3.6.1.4.1.1916.2.62	EXTREME-FILETRANSFER-MIB	no	no	yes
BlackDiamond 10808	1.3.6.1.4.1.1916.2.56	EXTREME-FILETRANSFER-MIB	no	no	yes
BlackDiamond 12802	1.3.6.1.4.1.1916.2.85	EXTREME-FILETRANSFER-MIB	no	no	yes
BlackDiamond 12804	1.3.6.1.4.1.1916.2.77	EXTREME-FILETRANSFER-MIB	no	no	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
EnetSwitch 24Port	1.3.6.1.4.1.1916.2.23	EXTREME-FILETRANSFER-MIB	no	no	yes
Sentriant CE150	1.3.6.1.4.1.1916.2.83	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 1	1.3.6.1.4.1.1916.2.1	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 1iSX	1.3.6.1.4.1.1916.2.19	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 1iTX	1.3.6.1.4.1.1916.2.14	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 2	1.3.6.1.4.1.1916.2.2	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 3	1.3.6.1.4.1.1916.2.3	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 4	1.3.6.1.4.1.1916.2.4	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 4FX	1.3.6.1.4.1.1916.2.5	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 5i	1.3.6.1.4.1.1916.2.15	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 5iLX	1.3.6.1.4.1.1916.2.21	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 5iTX	1.3.6.1.4.1.1916.2.22	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 7iSX	1.3.6.1.4.1.1916.2.12	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 7iTX	1.3.6.1.4.1.1916.2.13	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 24	1.3.6.1.4.1.1916.2.7	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 24e2SX	1.3.6.1.4.1.1916.2.41	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 24e2TX	1.3.6.1.4.1.1916.2.40	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 24e3	1.3.6.1.4.1.1916.2.25	EXTREME-FILETRANSFER-MIB	no	no	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Summit 48	1.3.6.1.4.1.1916.2.6	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 48i	1.3.6.1.4.1.1916.2.16	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 48i1u	1.3.6.1.4.1.1916.2.28	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 200-24	1.3.6.1.4.1.1916.2.53	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 200-24fx	1.3.6.1.4.1.1916.2.70	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 200-48	1.3.6.1.4.1.1916.2.54	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 300-24	1.3.6.1.4.1.1916.2.61	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 300-48	1.3.6.1.4.1.1916.2.55	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 400-24	1.3.6.1.4.1.1916.2.59	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 400-24p	1.3.6.1.4.1.1916.2.64	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 400-24t	1.3.6.1.4.1.1916.2.63	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit 400-48t	1.3.6.1.4.1.1916.2.58	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit Px1	1.3.6.1.4.1.1916.2.30	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit Ver2Stack	1.3.6.1.4.1.1916.2.93	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit X250-24p	1.3.6.1.4.1.1916.2.89	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit X250-24t	1.3.6.1.4.1.1916.2.88	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit X250-24x	1.3.6.1.4.1.1916.2.90	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit X250-48p	1.3.6.1.4.1.1916.2.92	EXTREME-FILETRANSFER-MIB	no	no	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Summit X250-48t	1.3.6.1.4.1.1916.2.91	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit X450-24t	1.3.6.1.4.1.1916.2.66	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit X450-24x	1.3.6.1.4.1.1916.2.65	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit X450a-24t	1.3.6.1.4.1.1916.2.71	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit X450a-24tDC	1.3.6.1.4.1.1916.2.80	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit X450a-24x	1.3.6.1.4.1.1916.2.84	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit X450a-24xDC	1.3.6.1.4.1.1916.2.82	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit X450a-48t	1.3.6.1.4.1.1916.2.76	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit X450a-48tDC	1.3.6.1.4.1.1916.2.87	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit X450e-24p	1.3.6.1.4.1.1916.2.72	EXTREME-FILETRANSFER-MIB	no	no	yes
Summit X450e-48p	1.3.6.1.4.1.1916.2.79	EXTREME-FILETRANSFER-MIB	no	no	yes
SummitStack	1.3.6.1.4.1.1916.2.67	EXTREME-FILETRANSFER-MIB	no	no	yes
SummitWM 100	1.3.6.1.4.1.1916.2.68	EXTREME-FILETRANSFER-MIB	no	no	yes
SummitWM 200	1.3.6.1.4.1.1916.2.94	EXTREME-FILETRANSFER-MIB	no	no	yes
SummitWM 1000	1.3.6.1.4.1.1916.2.69	EXTREME-FILETRANSFER-MIB	no	no	yes
SummitWM 2000	1.3.6.1.4.1.1916.2.95	EXTREME-FILETRANSFER-MIB	no	no	yes

Foundry Supported Devices

The following table lists Foundry devices supported by CA Spectrum Network Configuration Manager. The table provides examples. For the most up-to-date information on device support, access the CA Device Certification database (see page 16).

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
BigIronMG8Sw	1.3.6.1.4.1.1991.1.3.32.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
BigIronMG8Rt	1.3.6.1.4.1.1991.1.3.32.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
BigIronRX4Rt	1.3.6.1.4.1.1991.1.3.40.3.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
BigIronRX4Sw	1.3.6.1.4.1.1991.1.3.40.3.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
BigIronRX8Rt	1.3.6.1.4.1.1991.1.3.40.2.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
BigIronRX8Sw	1.3.6.1.4.1.1991.1.3.40.2.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
BigIronRX16Rt	1.3.6.1.4.1.1991.1.3.40.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
BigIronRX16Sw	1.3.6.1.4.1.1991.1.3.40.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
BigIronSXL3Sw	1.3.6.1.4.1.1991.1.3.37.1.3	FOUNDRY-SN-AGENT-MIB	no	no	yes
BigIronSXRt	1.3.6.1.4.1.1991.1.3.37.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
BigIronSXSw	1.3.6.1.4.1.1991.1.3.37.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
BIron4000Rt	1.3.6.1.4.1.1991.1.3.6.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
BIron4000SI	1.3.6.1.4.1.1991.1.3.6.3	FOUNDRY-SN-AGENT-MIB	no	no	yes
BIron4000Sw	1.3.6.1.4.1.1991.1.3.6.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
BIron8000Rt	1.3.6.1.4.1.1991.1.3.7.2	FOUNDRY-SN-AGENT-MIB	no	no	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
BIron8000SI	1.3.6.1.4.1.1991.1.3.7.3	FOUNDRY-SN-AGENT-MIB	no	no	yes
BIron15000Rt	1.3.6.1.4.1.1991.1.3.14.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
BIron15000SI	1.3.6.1.4.1.1991.1.3.14.3	FOUNDRY-SN-AGENT-MIB	no	no	yes
BIron8000Sw	1.3.6.1.4.1.1991.1.3.7.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
BIron15000Sw	1.3.6.1.4.1.1991.1.3.14.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FastIronBBSw	1.3.6.1.4.1.1991.1.3.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FastIron2Rt	1.3.6.1.4.1.1991.1.3.8.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FastIron2Sw	1.3.6.1.4.1.1991.1.3.8.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FastIron3Rt	1.3.6.1.4.1.1991.1.3.16.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FastIron3Sw	1.3.6.1.4.1.1991.1.3.16.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FastIronWGSw	1.3.6.1.4.1.1991.1.3.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FES2402Sw	1.3.6.1.4.1.1991.1.3.25.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FES2402Rt	1.3.6.1.4.1.1991.1.3.25.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FES4802Rt	1.3.6.1.4.1.1991.1.3.26.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FES4802Sw	1.3.6.1.4.1.1991.1.3.26.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FES9604Rt	1.3.6.1.4.1.1991.1.3.27.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FES9604Sw	1.3.6.1.4.1.1991.1.3.27.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FES12GCFRt	1.3.6.1.4.1.1991.1.3.28.2	FOUNDRY-SN-AGENT-MIB	no	no	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
FES12GCFSw	1.3.6.1.4.1.1991.1.3.28.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FES2402POERt	1.3.6.1.4.1.1991.1.3.29.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FES2402POESw	1.3.6.1.4.1.1991.1.3.29.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FES4802POERt	1.3.6.1.4.1.1991.1.3.30.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FES4802POESw	1.3.6.1.4.1.1991.1.3.30.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424Rt	1.3.6.1.4.1.1991.1.3.34.1.1.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424Sw	1.3.6.1.4.1.1991.1.3.34.1.1.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424PremRt	1.3.6.1.4.1.1991.1.3.34.1.1.2.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424PremSw	1.3.6.1.4.1.1991.1.3.34.1.1.2.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424P1XGPremSw	1.3.6.1.4.1.1991.1.3.34.1.2.2.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424P1XGRt	1.3.6.1.4.1.1991.1.3.34.1.2.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424P1XGSw	1.3.6.1.4.1.1991.1.3.34.1.2.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424P1XGPremRt	1.3.6.1.4.1.1991.1.3.34.1.2.2.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424P2XGRt	1.3.6.1.4.1.1991.1.3.34.1.3.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424P2XGSw	1.3.6.1.4.1.1991.1.3.34.1.3.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424P2XGPremRt	1.3.6.1.4.1.1991.1.3.34.1.3.2.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424P2XGPremSw	1.3.6.1.4.1.1991.1.3.34.1.3.2.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX448Rt	1.3.6.1.4.1.1991.1.3.34.2.1.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
FESX448Sw	1.3.6.1.4.1.1991.1.3.34.2.1.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX448PremRt	1.3.6.1.4.1.1991.1.3.34.2.1.2.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX448PremSw	1.3.6.1.4.1.1991.1.3.34.2.1.2.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX448P1XGSw	1.3.6.1.4.1.1991.1.3.34.2.2.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX448P1XGRt	1.3.6.1.4.1.1991.1.3.34.2.2.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX448P1XGPremRt	1.3.6.1.4.1.1991.1.3.34.2.2.2.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX448P1XGPremSw	1.3.6.1.4.1.1991.1.3.34.2.2.2.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX448P2XGRt	1.3.6.1.4.1.1991.1.3.34.2.3.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX448P2XGSw	1.3.6.1.4.1.1991.1.3.34.2.3.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX448P2XGPremRt	1.3.6.1.4.1.1991.1.3.34.2.3.2.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX448P2XGPremSw	1.3.6.1.4.1.1991.1.3.34.2.3.2.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424FiberRt	1.3.6.1.4.1.1991.1.3.34.3.1.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424FiberSw	1.3.6.1.4.1.1991.1.3.34.3.1.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424FiberPremRt	1.3.6.1.4.1.1991.1.3.34.3.1.2.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424FiberPremSw	1.3.6.1.4.1.1991.1.3.34.3.1.2.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424FiberP1XGRt	1.3.6.1.4.1.1991.1.3.34.3.2.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424FiberP1XGSw	1.3.6.1.4.1.1991.1.3.34.3.2.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424FiberP1XGPremRt	1.3.6.1.4.1.1991.1.3.34.3.2.2.2	FOUNDRY-SN-AGENT-MIB	no	no	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
FESX424FiberP1XGPremSw	1.3.6.1.4.1.1991.1.3.34.3.2.2.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424FiberP2XGRt	1.3.6.1.4.1.1991.1.3.34.3.3.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424FiberP2XGSw	1.3.6.1.4.1.1991.1.3.34.3.3.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424FiberP2XGPremRt	1.3.6.1.4.1.1991.1.3.34.3.3.2.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424FiberP2XGPremSw	1.3.6.1.4.1.1991.1.3.34.3.3.2.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX448FiberRt	1.3.6.1.4.1.1991.1.3.34.4.1.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX448FiberSw	1.3.6.1.4.1.1991.1.3.34.4.1.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX448FiberPremRt	1.3.6.1.4.1.1991.1.3.34.4.1.2.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX448FiberPremSw	1.3.6.1.4.1.1991.1.3.34.4.1.2.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX448FiberP1XGRt	1.3.6.1.4.1.1991.1.3.34.4.2.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX448FiberP1XGSw	1.3.6.1.4.1.1991.1.3.34.4.2.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX448FiberP1XGPremRt	1.3.6.1.4.1.1991.1.3.34.4.2.2.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX448FiberP1XGPremSw	1.3.6.1.4.1.1991.1.3.34.4.2.2.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX448FiberP2XGRt	1.3.6.1.4.1.1991.1.3.34.4.3.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX448FiberP2XGSw	1.3.6.1.4.1.1991.1.3.34.4.3.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX448FiberP2XGPremRt	1.3.6.1.4.1.1991.1.3.34.4.3.2.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX448FiberP2XGPremSw	1.3.6.1.4.1.1991.1.3.34.4.3.2.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424POERt	1.3.6.1.4.1.1991.1.3.34.5.1.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
FESX424POESw	1.3.6.1.4.1.1991.1.3.34.5.1.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424POEPremRt	1.3.6.1.4.1.1991.1.3.34.5.1.2.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424POEPremSw	1.3.6.1.4.1.1991.1.3.34.5.1.2.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424POEP1XGSw	1.3.6.1.4.1.1991.1.3.34.5.2.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424POEP1XGRt	1.3.6.1.4.1.1991.1.3.34.5.2.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424POEP1XGPremRt	1.3.6.1.4.1.1991.1.3.34.5.2.2.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424POEP1XGPremSw	1.3.6.1.4.1.1991.1.3.34.5.2.2.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424POEP2XGRt	1.3.6.1.4.1.1991.1.3.34.5.3.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424POEP2XGSw	1.3.6.1.4.1.1991.1.3.34.5.3.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424POEP2XGPremRt	1.3.6.1.4.1.1991.1.3.34.5.3.2.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FESX424POEP2XGPremSw	1.3.6.1.4.1.1991.1.3.34.5.3.2.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FWSX424Rt	1.3.6.1.4.1.1991.1.3.35.1.1.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FWSX424Sw	1.3.6.1.4.1.1991.1.3.35.1.1.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FWSX424P1XGRt	1.3.6.1.4.1.1991.1.3.35.1.2.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FWSX424P1XGSw	1.3.6.1.4.1.1991.1.3.35.1.2.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FWSX424P2XGRt	1.3.6.1.4.1.1991.1.3.35.1.3.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FWSX424P2XGSw	1.3.6.1.4.1.1991.1.3.35.1.3.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FWSX448Rt	1.3.6.1.4.1.1991.1.3.35.2.1.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
FWSX448Sw	1.3.6.1.4.1.1991.1.3.35.2.1.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FWSX448P1XGRt	1.3.6.1.4.1.1991.1.3.35.2.2.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FWSX448P1XGSw	1.3.6.1.4.1.1991.1.3.35.2.2.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FWSX448P2XGRt	1.3.6.1.4.1.1991.1.3.35.2.3.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FWSX448P2XGSw	1.3.6.1.4.1.1991.1.3.35.2.3.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FIron2GCRt	1.3.6.1.4.1.1991.1.3.12.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FIron2GCSw	1.3.6.1.4.1.1991.1.3.12.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FIron2PlusRt	1.3.6.1.4.1.1991.1.3.9.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FIron2PlusSw	1.3.6.1.4.1.1991.1.3.9.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FIron3GCRt	1.3.6.1.4.1.1991.1.3.17.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FIron3GCSw	1.3.6.1.4.1.1991.1.3.17.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FIron400Sw	1.3.6.1.4.1.1991.1.3.22.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FIron400Rt	1.3.6.1.4.1.1991.1.3.22.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FIron4802Rt	1.3.6.1.4.1.1991.1.3.21.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FIron4802SI	1.3.6.1.4.1.1991.1.3.21.3	FOUNDRY-SN-AGENT-MIB	no	no	yes
FIron4802Sw	1.3.6.1.4.1.1991.1.3.21.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FIron800Rt	1.3.6.1.4.1.1991.1.3.23.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FIron800Sw	1.3.6.1.4.1.1991.1.3.23.1	FOUNDRY-SN-AGENT-MIB	no	no	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
FIron1500Rt	1.3.6.1.4.1.1991.1.3.24.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FIron1500Sw	1.3.6.1.4.1.1991.1.3.24.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FIronSXRt	1.3.6.1.4.1.1991.1.3.36.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FIronSXSw	1.3.6.1.4.1.1991.1.3.36.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FIronSXL3Sw	1.3.6.1.4.1.1991.1.3.36.1.3	FOUNDRY-SN-AGENT-MIB	no	no	yes
FIronSXPremL3Sw	1.3.6.1.4.1.1991.1.3.36.2.3	FOUNDRY-SN-AGENT-MIB	no	no	yes
FIronSXPremRt	1.3.6.1.4.1.1991.1.3.36.2.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
FIronSXPremSw	1.3.6.1.4.1.1991.1.3.36.2.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FI2PlusGCSw	1.3.6.1.4.1.1991.1.3.13.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
FI2PlusGCRt	1.3.6.1.4.1.1991.1.3.13.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
NetIronRt	1.3.6.1.4.1.1991.1.3.2.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
NetIron40GRt	1.3.6.1.4.1.1991.1.3.33.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
NetIron400Rt	1.3.6.1.4.1.1991.1.3.10.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
NetIron800Rt	1.3.6.1.4.1.1991.1.3.11.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
NIron1500Rt	1.3.6.1.4.1.1991.1.3.15.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
NetIronMLX4Rt	1.3.6.1.4.1.1991.1.3.44.3.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
NetIronMLX16Rt	1.3.6.1.4.1.1991.1.3.44.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
NetIronMLX8Rt	1.3.6.1.4.1.1991.1.3.44.2.2	FOUNDRY-SN-AGENT-MIB	no	no	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
NetIronXMR16000Rt	1.3.6.1.4.1.1991.1.3.41.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
NetIronXMR8000Rt	1.3.6.1.4.1.1991.1.3.41.2.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
NetIronXMR4000Rt	1.3.6.1.4.1.1991.1.3.41.3.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
NetIronIMRRt	1.3.6.1.4.1.1991.1.3.39.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
NIron4802Rt	1.3.6.1.4.1.1991.1.3.31.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
NIron4802Sw	1.3.6.1.4.1.1991.1.3.31.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
ServerIron	1.3.6.1.4.1.1991.1.3.3.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
ServerIronXL	1.3.6.1.4.1.1991.1.3.3.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
SIron400Rt	1.3.6.1.4.1.1991.1.3.18.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
SIron400Sw	1.3.6.1.4.1.1991.1.3.18.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
SIron800Rt	1.3.6.1.4.1.1991.1.3.19.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
SIron800Sw	1.3.6.1.4.1.1991.1.3.19.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
SIron1500Rt	1.3.6.1.4.1.1991.1.3.20.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
SIron1500Sw	1.3.6.1.4.1.1991.1.3.20.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
SIronXLTCS	1.3.6.1.4.1.1991.1.3.3.3	FOUNDRY-SN-AGENT-MIB	no	no	yes
SIronLS100Rt	1.3.6.1.4.1.1991.1.3.42.9.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
SIronLS100Sw	1.3.6.1.4.1.1991.1.3.42.9.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
SIronLS300Rt	1.3.6.1.4.1.1991.1.3.42.9.2.2	FOUNDRY-SN-AGENT-MIB	no	no	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
SIronLS300Sw	1.3.6.1.4.1.1991.1.3.42.9.2.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
SIronTM100Sw	1.3.6.1.4.1.1991.1.3.42.10.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
SIronTM100Sw	1.3.6.1.4.1.1991.1.3.42.10.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
SIronTM300Sw	1.3.6.1.4.1.1991.1.3.42.10.2.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
SIronTM300Sw	1.3.6.1.4.1.1991.1.3.42.10.2.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
TurboIronSXSw	1.3.6.1.4.1.1991.1.3.38.1.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
TurboIronSXRt	1.3.6.1.4.1.1991.1.3.38.1.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
TurboIronSXL3Sw	1.3.6.1.4.1.1991.1.3.38.1.3	FOUNDRY-SN-AGENT-MIB	no	no	yes
TurboIronSxPremSw	1.3.6.1.4.1.1991.1.3.38.2.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
TurboIronSXPremRt	1.3.6.1.4.1.1991.1.3.38.2.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
TurboIronSXPremL3Sw	1.3.6.1.4.1.1991.1.3.38.2.3	FOUNDRY-SN-AGENT-MIB	no	no	yes
TIron8SIXLG	1.3.6.1.4.1.1991.1.3.5.4	FOUNDRY-SN-AGENT-MIB	no	no	yes
TurboIronRt	1.3.6.1.4.1.1991.1.3.4.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
TurboIronSw	1.3.6.1.4.1.1991.1.3.4.1	FOUNDRY-SN-AGENT-MIB	no	no	yes
TurboIron8Rt	1.3.6.1.4.1.1991.1.3.5.2	FOUNDRY-SN-AGENT-MIB	no	no	yes
TurboIron8SI	1.3.6.1.4.1.1991.1.3.5.3	FOUNDRY-SN-AGENT-MIB	no	no	yes
TurboIron8Sw	1.3.6.1.4.1.1991.1.3.5.1	FOUNDRY-SN-AGENT-MIB	no	no	yes

Juniper Supported Devices

The following table lists Juniper devices supported by CA Spectrum Network Configuration Manager. The table provides examples. For the most up-to-date information on device support, access the CA Device Certification database (see page 16).

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
EX3200	1.3.6.1.4.1.2636.1.1.1.2.30	no	no	yes	no
EX4200	1.3.6.1.4.1.2636.1.1.1.2.31	no	no	yes	no
EX8208	1.3.6.1.4.1.2636.1.1.1.2.32	no	no	yes	no
EX8216	1.3.6.1.4.1.2636.1.1.1.2.33	no	no	yes	no
IRM	1.3.6.1.4.1.2636.1.1.1.2.16	no	no	*yes	yes
J2300	1.3.6.1.4.1.2636.1.1.1.2.13	no	no	*yes	yes
J4300	1.3.6.1.4.1.2636.1.1.1.2.14	no	no	*yes	yes
J6300	1.3.6.1.4.1.2636.1.1.1.2.15	no	no	*yes	yes
M5	1.3.6.1.4.1.2636.1.1.1.2.5	no	no	*yes	yes
M7i	1.3.6.1.4.1.2636.1.1.1.2.10	no	no	*yes	yes
M10	1.3.6.1.4.1.2636.1.1.1.2.4	no	no	*yes	yes
M10i	1.3.6.1.4.1.2636.1.1.1.2.11	no	no	*yes	yes
M20	1.3.6.1.4.1.2636.1.1.1.2.2	no	no	*yes	yes
M40	1.3.6.1.4.1.2636.1.1.1.2.1	no	no	*yes	yes
M40e	1.3.6.1.4.1.2636.1.1.1.2.8	no	no	*yes	yes
M160	1.3.6.1.4.1.2636.1.1.1.2.3	no	no	*yes	yes
M320	1.3.6.1.4.1.2636.1.1.1.2.9	no	no	*yes	yes
T320	1.3.6.1.4.1.2636.1.1.1.2.7	no	no	*yes	yes
T640	1.3.6.1.4.1.2636.1.1.1.2.6	no	no	*yes	yes
TX	1.3.6.1.4.1.2636.1.1.1.2.17	no	no	*yes	yes

*Device must support SSH V2

Lancom Supported Devices

The following table lists Lancom devices supported by CA Spectrum Network Configuration Manager. Supported devices must be running firmware LCOS 7.58.0045 or above. The table provides examples. For the most up-to-date information on device support, access the CA Device Certification database (see page 16).

When a Perl script is the only means of communication with the device, the script method is provided.

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
LANCOM 1721 VPN	1.3.6.1.4.1.2356.500.4.1721	no	no	no	Telnet/ TFTP
LANCOM 1751	1.3.6.1.4.1.2356.1000.1.1751	no	no	no	Telnet/ TFTP
LANCOM 7111	1.3.6.1.4.1.2356.500.2.7111	no	no	no	Telnet/ TFTP
LANCOM 8011	1.3.6.1.4.1.2356.500.2.8011	no	no	no	Telnet/ TFTP

Nortel Baystack Supported Devices

The following table lists Nortel Baystack devices supported by CA Spectrum Network Configuration Manager. The table provides examples. For the most up-to-date information on device support, access the CA Device Certification database (see page 16).

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
BayStack450-24T	1.3.6.1.4.1.45.3.35.1	no	no	*yes	yes
BayStack380-24T	1.3.6.1.4.1.45.3.45.1	no	no	*yes	yes
BayStack420	1.3.6.1.4.1.45.3.43.1	no	no	*yes	yes
BayStack460-24T	1.3.6.1.4.1.45.3.49.1	no	no	*yes	yes
BayStack470-48T	1.3.6.1.4.1.45.3.46.1	no	no	*yes	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
BayStack425-24T	1.3.6.1.4.1.45.3.57.2	no	no	*yes	yes
BayStack470-24T	1.3.6.1.4.1.45.3.54.1	no	no	*yes	yes
BayStack5510-24T	1.3.6.1.4.1.45.3.52.1	no	no	*yes	yes
BayStack5510-48T	1.3.6.1.4.1.45.3.53.1	no	no	*yes	yes
BayStack5520-24T-PWR	1.3.6.1.4.1.45.3.59.1	no	no	*yes	yes
BayStack5520-48T-PWR	1.3.6.1.4.1.45.3.59.2	no	no	*yes	yes
Nortel ERS 5530-24TFD	1.3.6.1.4.1.45.3.65	no	no	*yes	yes

* Device must support SSH V2

Nortel Passport Supported Devices

The following table lists Nortel Passport devices supported by CA Spectrum Network Configuration Manager. The table provides examples. For the most up-to-date information on device support, access the CA Device Certification database (see page 16).

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Passport1424T	1.3.6.1.4.1.2272.42	SWL2MGMT-MIB	no	no	yes
Passport1648	1.3.6.1.4.1.2272.43	SWL2MGMT-MIB	no	no	yes
Passport1612	1.3.6.1.4.1.2272.44	SWL2MGMT-MIB	no	no	yes
Passport1624	1.3.6.1.4.1.2272.45	SWL2MGMT-MIB	no	no	yes
Passport8610	1.3.6.1.4.1.2272.30	RAPID-CITY MIB	no	no	yes
Passport8606	1.3.6.1.4.1.2272.31	RAPID-CITY MIB	no	no	yes
Passport8110	1.3.6.1.4.1.2272.32	RAPID-CITY MIB	no	no	yes
Passport8106	1.3.6.1.4.1.2272.33	RAPID-CITY MIB	no	no	yes

Device Name	Sys OID	SNMP/TFTP Support	Telnet Support	SSH Support	Perl Support
Passport8610	1.3.6.1.4.1.2272.37	RAPID-CITY MIB	no	no	yes
IntrWanPE100	1.3.6.1.4.1.2272.40	RAPID-CITY MIB	no	no	yes
Passport8006	1.3.6.1.4.1.2272.280887558	RAPID-CITY MIB	no	no	yes
Passport8010	1.3.6.1.4.1.2272.280887562	RAPID-CITY MIB	no	no	yes

Appendix B: Network Configuration Manager Events

This section contains the following topics:

About Network Configuration Manager Events

Events are generated when a configuration change occurs on a device. All events for a particular device during a specified Correlation Event Period, which is set in Configuration Manager General Configuration, are combined. See Configure General Configuration (see page 27) for more information.

Information is correlated based on device traps, Syslog traps and events, Network Configuration Manager internals and any other trap that is mapped to the generic change event. This information varies by device family. Out-of-box support is provided for Cisco CatOS, Cisco IOS, Cisco IOS - SSH Capable, and Juniper JUNOS device families. See Configure Notification Trap Settings (see page 45) for more information on customizing traps for your installation.

Events Generated on the Device

Configuration Change

Event0082101b:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Configuration change detected on device {m} of type {t} on landscape {S 3}. (event [{e}])

Event00821029:{d "%w- %d %m-, %Y - %T"} Configuration Manager - A configuration change notification was received from device {m}. (event [{e}])

Event0082105e:{d "%w- %d %m-, %Y - %T"} Configuration Manager - The running configuration of device {m} on landscape {S 2} is changed. (event [{e}])

Event0082105f:{d "%w- %d %m-, %Y - %T"} Configuration Manager - The running configuration of device {m} on landscape {S 2} is changed. An alarm will be generated on this model. (event [{e}])

Correlation of Configuration Change Events

Event0082105a:{d "%w- %d %m-, %Y - %T"} Configuration Manager - A configuration change notification was received from device {m} of type {t} on landscape {S 1}.

Device trap(s) provided:

Device User: {S 2}

From: {S 3}

On: {S 4}

The following information was provided by SPECTRUM:

Device User: {S 2}

Spectrum User: {S 5}

NCM Communication Mode: {S 6}

Capture Succeeded: {S 7}

Capture Error Message: {S 8}

Total Number of Line Changes: {I 9}

Relevant Number of Line Changes: {I 10}

Violated Policies: {S 11}

Compliant Policies: {S 12}

Model handle of current configuration model: {H 13}

Model handle of previous configuration model: {H 14}

Startup and Running Configurations Same/Differ

Event00821024:{d "%w- %d %m-, %Y - %T"} Configuration Manager - The startup configuration of device {m} on landscape {S 3} differs from its running configuration. (event [{e}])

Event00821025:{d "%w- %d %m-, %Y - %T"} Configuration Manager - The startup configuration of device {m} on landscape {S 3} differs from its running configuration. A minor alarm will be generated on this model. (event [{e}])

Event00821026:{d "%w- %d %m-, %Y - %T"} Configuration Manager - The startup configuration of device {m} on landscape {S 3} differs from its running configuration. A major alarm will be generated on this model. (event [{e}])

Event00821027:{d "%w- %d %m-, %Y - %T"} Configuration Manager - The startup configuration of device {m} on landscape {S 3} differs from its running configuration. A critical alarm will be generated on this model. (event [{e}])

Event00821028:{d "%w- %d %m-, %Y - %T"} Configuration Manager - The startup configuration of device {m} on landscape {S 3} is equal to its running configuration. (event [{e}])

Reference and Running Configuration Same/Differ

Event0082105b:{d "%w- %d %m-, %Y - %T"} Configuration Manager - The reference running configuration of device {m} on landscape {S 2} differs from its current running configuration. (event [{e}])

Event0082105c:{d "%w- %d %m-, %Y - %T"} Configuration Manager - The reference running configuration of device {m} on landscape {S 2} differs from its current running configuration. An alarm will be generated on this model. (event [{e}])

Event0082105d:{d "%w- %d %m-, %Y - %T"} Configuration Manager - The reference running configuration of device {m} on landscape {S 2} is equal to its running configuration. (event [{e}])

Device Compliant/Noncompliant with Policy

Event00821016:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Device {m} of type {t} is compliant with policy {S 1} on landscape {S 3}. (event [{e}])

Event00821017:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Device {m} of type {t} is not compliant with policy {S 1} on landscape {S 3}. (event [{e}])

Event00821051:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Unable to verify policy compliance of host configuration on device {m} of type {t} on landscape {S 1}. Specific error: {S 2} (event [{e}])

Event00821055:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Device {m} of type {t} is no longer in violation of policy {S 1} because the device has been removed from global collection {S 2} on landscape {S 3}. (event [{e}])

Event00821056:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Device {m} of type {t} is no longer in violation of policy {S 1} because the device has been removed from device family {S 2} on landscape {S 3}. (event [{e}])

Event00821057:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Device {m} of type {t} on landscape {S 2} is no longer in violation of policy {S 1} because the policy has been deleted. (event [{e}])

Device Noncompliant with Policy Alarm Generating Events

Event00821020:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Device {m} has violated policy {S 1} on landscape {S 3}. The severity of this violation is minor. (event [{e}])

Event00821021:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Device {m} has violated policy {S 1} on landscape {S 3}. The severity of this violation is major. (event [{e}])

Event00821022:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Device {m} has violated policy {S 1} on landscape {S 3}. The severity of this violation is critical. (event [{e}])

Capture Succeeded/Failed

Event00821000:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Capture succeeded for host configuration file from device {m} of type {t} on landscape {S 1} initiated by user {S 2}. (event [{e}])

Event00821001:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Capture failed for host configuration file from device {m} of type {t} on landscape {S 1} initiated by user {S 2}.
Specific error: {S 3} (event [{e}])

Event00821049:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Capture succeeded for host startup configuration file from device {m} of type {t} on landscape {S 1} initiated by user {u}. (event [{e}])

Event00821050:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Capture failed for host startup configuration file from device {m} of type {t} on landscape {S 1} initiated by user {u}. Specific error: {S 3} (event [{e}])

Upload Succeeded/Failed

Event00821002:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Load succeeded for host configuration on device {m} of type {t} on landscape {S 1} initiated by user {S 2}. (event [{e}])

Event00821003:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Load failed for host configuration on device {m} of type {t} on landscape {S 1} initiated by user {S 2}. Specific error: {S 4} (event [{e}])

Upload Failed Alarm Generating Events

Event00821035:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Load failed for host configuration on device {m} of type {t} on landscape {S 1} initiated by user {S 2}. The severity of this failure is minor. (event [{e}])

Event00821036:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Load failed for host configuration on device {m} of type {t} on landscape {S 1} initiated by user {S 2}. The severity of this failure is major. (event [{e}])

Event00821037:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Load failed for host configuration on device {m} of type {t} on landscape {S 1} initiated by user {S 2}. The severity of this failure is critical. (event [{e}])

Write to Startup Succeeded/Failed

Event00821018:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Successfully wrote the running configuration to the startup configuration on device {m} of type {t} on landscape {S 1} initiated by {S 2}. (event [{e}])

Event00821019:{d "%w- %d %m-, %Y - %T"} Configuration Manager - The attempt to write the running configuration to the startup configuration on device {m} of type {t} failed on landscape {S 1}. This operation was initiated by {S 2}. Specific Error: {S 3}. (event [{e}])

NCM Enabled/Disabled on Device

Event0082102f:{d "%w- %d %m-, %Y - %T"} Configuration Manager - NCM has been disabled for device {m}. (event [{e}])

Event00821030:{d "%w- %d %m-, %Y - %T"} Configuration Manager - NCM has been enabled for device {m}. (event [{e}])

NCM Disabled, Operation Not Performed

Event00821032:{d "%w- %d %m-, %Y - %T"} Configuration Manager - The requested NCM operation was not performed on model {m} because NCM is disabled on the models device family. (event [{e}])

Event00821033:{d "%w- %d %m-, %Y - %T"} Configuration Manager - The requested NCM operation was not performed on model {m} because NCM is disabled on this model. (event [{e}])

Event00821034:{d "%w- %d %m-, %Y - %T"} Configuration Manager - The requested NCM operation was not performed on model {m} because this model is a proxy model. (event [{e}])

Device Firmware Load

Event00821053:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Firmware load completed successfully on device {m} of type {t} on landscape {S 1}. Firmware script was executed with command line parameters: {S 3} This operation was initiated by {u}. (event [{e}])

Event00821054:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Firmware load failed on device {m} of type {t} on landscape {S 1}. Specific error: {S 2} Firmware script was executed with command line parameters: {S 3} (event [{e}])

Device Added/Removed from Device Family

Event00821058:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Device {m} of type {t} has been added to device family {S 2} on landscape {S 1}. (event [{e}])

Event00821059:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Device {m} of type {t} has been removed from device family {S 2} on landscape {S 1}. (event [{e}])

Events Generated on Policies

Policy Enabled/Disabled

Event00821014:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Policy {m} been enabled by {u}. (event [{e}])

Event00821015:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Policy {m} been disabled by {u}. (event [{e}])

Event00821023:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Policy {S 1} has been disabled. Any alarms previously generated by violations of this policy have been cleared. (event [{e}])

Policy Modified

Event00821011:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Policy {m} has been modified by {u}. (event [{e}])

Policy has Violators

Event00821012:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Policy {m} has a violator on landscape {S 1}. (event [{e}])

Event00821013:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Policy {m} no longer has a violator on landscape {S 1}. (event [{e}])

Violated Policy, Alarm Generating Events

Event0082101d:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Policy {m} has a violator on landscape {S 1}. The severity of this violation is minor. (event [{e}])

Event0082101e:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Policy {m} has a violator on landscape {S 1}. The severity of this violation is major. (event [{e}])

Event0082101f:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Policy {m} has a violator on landscape {S 1}. The severity of this violation is critical. (event [{e}])

Events Generated on Tasks Global Sync, Capture, Upload and Write to Startup

Task Scheduled/Unscheduled

Event00821040:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Task Scheduled - Task {m} of type {t} has been scheduled for {S 1} on landscape {S 2}. (event [{e}])

Event00821041:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Task Unscheduled - Task {m} of type {t} has had the schedule removed on landscape {S 1}. (event [{e}])

Task Started, Stopped, Completed, Partially Completed

Event00821042:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Task Started - Task {m} of type {t} has been started by {S 1} on {I 2} devices on landscape {S 3}. (event [{e}])

Event00821043:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Task Stopping - Task {m} of type {t} was stopped by {S 1} on landscape {S 3}. (event[{e}])

Event00821045:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Task Completed - Task {m} of type {t} has completed with all devices processed on landscape {S 1}. Out of a total of {I 2} devices, {I 3} succeeded and {I 4} failed. (event [{e}])

Event00821044:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Task Partially Completed - Task {m} of type {t} completed with {I 5} unprocessed devices on landscape {S 1}. For a total of {I 2} deivces, {I 3} succeeded, {I 4} failed and {I 5} devices remained unprocessed. (event [{e}])

Task Partially Completed Alarm Generating Events

Event00821046:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Task Partially Completed - Task {m} of type {t} completed with {I 5} unprocessed devices on landscape {S 1}. For a total of {I 2} devices, {I 3} succeeded, {I 4} failed and {I 5} devices remained unprocessed. A minor alarm has been generated. (event [{e}])

Event00821047:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Task Partially Completed - Task {m} of type {t} completed with {I 5} unprocessed devices on landscape {S 1}. For a total of {I 2} devices, {I 3} succeeded, {I 4} failed and {I 5} devices remained unprocessed. A major alarm has been generated. (event [{e}])

Event00821048:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Task Partially Completed - Task {m} of type {t} completed with {I 5} unprocessed devices on landscape {S 1}. For a total of {I 2} devices, {I 3} succeeded, {I 4} failed and {I 5} devices remained unprocessed. A critical alarm has been generated. (event [{e}])

Events Generated on the Configuration Manager Application

Event0082101a:{d "%w- %d %m-, %Y - %T"} Cannot connect to Configuration Manager - Cannot connect to the NCM secure communication daemon on landscape {S 1}. (event [{e}])

Event0082101c:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Cannot create file in Archive Directory. Unable to archive a device configuration. Could not create a file in the archive directory {S 1} on landscape {S 2}. (event [{e}])

Event00821052:{d "%w- %d %m-, %Y - %T"} Configuration Manager - Connection to the ncmservice daemon has been restored. (event [{e}])

Global Unsolicited Notification

Event0082102b:{d "%w- %d %m-, %Y - %T"} Configuration Manager - The ability to respond to unsolicited notifications of configuration change has been globally disabled on all landscapes. (event [{e}])

Event0082102c:{d "%w- %d %m-, %Y - %T"} Configuration Manager - The ability to respond to unsolicited notifications of configuration change has been globally enabled on all landscapes. (event [{e}])

Events Generated on Device Families

Event0082102d:{d "%w- %d %m-, %Y - %T"} Configuration Manager - NCM enabled/disabled for device family {m}. (event [{e}])

Event0082102e:{d "%w- %d %m-, %Y - %T"} Configuration Manager - NCM has been enabled for device family {m}. (event [{e}])

Appendix C: Network Configuration Manager Privileges

This section lists Network Configuration Manager privileges for OneClick users. By default, each privilege is enabled.

Note: See the *Administrator Guide* for details about configuring privileges.

Network Configuration Manager

Allows the administrator to configure the Network Configuration Manager application. This includes configurations performed in the Information tab views from the Configuration Manager node, Device Family nodes, and Network Configuration Manager configuration performed at the individual device level. This also includes the ability to schedule a global synchronization task.

Capture Host Configuration

Allows the operator to create a bulk capture task or an on-demand capture from the Host Configuration tab.

Hide Configuration Changes from Approval Requests

Allows the user to decide whether to include configuration content in a workflow approval request.

Include Global Collection in NCM Task

Allows the user to associate Network Configuration Manager tasks with Global Collections. By having access to a collection, a user will implicitly have access to all members within the collection. With this access, the user can perform any of the tasks, including uploading configurations and loading firmware, on these devices.

Load device firmware

Allows the operator to upload firmware to devices.

Manage NCM Tasks

Grants access to the Network Configuration Manager Tasks folder. Access to this folder provides global access to all Network Configuration Manager tasks on all CA Spectrum landscapes and the ability to start, stop, edit and delete them all.

Reload Device

Allows operator to reload firmware configuration to a device.

Repair Device

Allows the operator to upload the specified repair content for a policy with non-compliant devices.

Save Host Configuration to Startup

Allows the operator to create bulk Save to Startup tasks.

Schedule a Reload

Allows operator to schedule reload firmware configuration to a device.

Schedule NCM Tasks

Allows the operator to schedule bulk tasks.

Task Approver

Controls approval authorization for approval workflow.

ServiceDesk

If Approval Workflow Mode is set to ServiceDesk and the user has this privilege, acquiring approval through Service Desk is optional.

OneClick

If Approval Workflow Mode is set to OneClick and the user has this privilege, the user can approve his own tasks or tasks that are initiated by others.

Upload Host Configuration

Allows the operator to create a bulk Upload task or an automatic Upload from the Host Configuration tab.

Use Cached Device Authentication

Allows the operator to use the username and password as specified in the device family and single device override configurations. The user does not have to enter a username and password each time a task is initiated if this privilege is enabled. When initiating a task (for example, Upload or Save to Startup), the user will be prompted for device authentication if this privilege is disabled.

Note: When performing a bulk task, such as an Upload or Save to Startup, without this privilege, the operator is prompted for device authentication once. This same authentication data is then used for all devices for which the bulk operation is performed.

View Host Configuration

Allows the operator access to host configurations.

View NCM Policies

Grants access to the Network Configuration Manager Policies folder. Access to this folder provides global access to all Network Configuration Manager policies on all CA Spectrum landscapes and the ability to edit, enable, disable and delete them all.

Create/Edit NCM Policies

Allows the operator ability to create a new policy or edit an existing policy. This privilege does not allow the user to enable a policy.

Enable/Disable NCM Policies

Allows the operator to enable, disable, and delete a Network Configuration Manager Policy.

View Unmasked Configurations

Allows the operator to view content that is blacked-out by the View Mask. The View Mask is on a Device Family and can be overridden at the local device.

Index

E

F

G

I

J

K

L

M

N

P

R

S

T

U

V

W