GETTING STARTED GUIDE

Network Configuration Manager

Version 2020.2

solarwinds

Last Updated: Wednesday, June 3, 2020

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Table of Contents

How do I get started with NCM?

Welcome to the SolarWinds Network Configuration Manager (NCM) Getting Started Guide.

Ensure your long term success with SolarWinds NCM by following the guidelines described in this guide. Depending on your workload, getting started with NCM should take you one week or less.

Prerequisites

This getting started guide assumes that you have:

- Purchased or are evaluating NPM and NCM.
- Installed NPM and are adding NCM to your SolarWinds Orion deployment.
- Completed the NPM Getting Started Guide. There are some very important principles and skills that you learn in the NPM Getting Started Guide, so SolarWinds highly encourages you to work through that content.

Get started with NCM

To get started with NCM, complete the following tasks.

□ **Install NCM.**

Use the SolarWinds Orion Installer to prepare the environment and install NCM.

□ **Populate NCM with devices.**

For NCM to manage your device configs, you need to discover those network devices and add them to Orion for monitoring.

□ **Manage network change.**

Understand options for editing configs. Learn how to manually back up a config, edit one or more configs with a script, run an inventory scan, and edit a config using a config change template.

□ **Troubleshoot a network problem caused by a config change.**

Get a walk-through of investigating and correcting a network outage caused by a config change, and learn what was configured to enable that type of monitoring and troubleshooting.

☐ **Configure real-time change detection.**

Get instant notification through email whenever a change occurs to any of your device configurations. Real-time change detection helps you troubleshoot the root cause of network performance issues and identify unauthorized changes.

☐ **Run and schedule inventory reports.**

Use NCM inventory reports to access up-to-date device information and to manage the inventory of your network infrastructure. Learn how to run and schedule device inventory reports.

☐ **Ensure compliance.**

Use the NCM compliance policy reports to verify and maintain compliance within your network. Learn how to use preconfigured reports to conduct a compliance audit.

Existing customers: Access your licensed software from the SolarWinds Customer Portal.

If you need implementation help, contact our Support reps. Read this SolarWinds Customer Support article to learn how to properly open a support case and get your case the right level of visibility.

Evaluators: If you are evaluating SolarWinds NCM, download a free 30-day evaluation. The evaluation version of SolarWinds NCM is a full version of the product, functional for 30 days. After the evaluation period, you can easily convert your evaluation license to a production license by obtaining and applying a license key. If you need assistance with your evaluation, contact sales@solarwinds.com.

Product terminology

Orion Platform: The common backend platform used by the SolarWinds Orion suite of products, including NPM, SAM, NCM, NTA, and more. The platform provides the backbone for navigation, settings, and common features like alerts and reports. It also provides a consistent look-and-feel across products, giving you a “single pane of glass” for your Orion monitoring tools.

Orion Web Console: The web interface that you use to access NCM and other products that run on the Orion Platform. This interface is used to view, configure, and manage all of your monitored objects.

Check out this video on navigating the Web Console.

Orion Application Server: A Windows server that runs the Orion Web Console and collects data from monitored objects. Also called the Orion Main Poller.

Orion Database Server: A Windows SQL server that should be hosted on a dedicated server in a production environment, separately from the Orion Application Server. It stores Orion configuration data and all collected performance and syslog data.

Polling Engine: A polling engine controls polling job scheduling, data processing, and queries your monitored devices for performance metrics such as CPU, memory, and up or down status. Additional Polling Engines can be licensed to provide additional scalability and capacity. By default, the Orion Server provides one polling engine (often referred to as the main polling engine).

Populate NCM with devices

This section includes the following topics:

- Discovery for SolarWinds NCM
- Add a device to NCM

Discovery for SolarWinds NCM

For NCM to manage your device configs, you need to discover those network devices and add them to Orion for monitoring.

- If you have other Orion Platform products, such as NPM, you have probably already discovered the routers, switches, and firewalls that you want to manage with NCM. If you have already discovered these devices and added them to the Orion Platform, you can proceed to the next step and add the devices to NCM.
- If you have **not** discovered the network devices you want to manage with NCM, see the NPM Getting Started Guide to learn how to discover your network and add discovered devices to Orion. Then return to the Network Configuration Manager Getting Started Guide so you can add those devices to NCM.

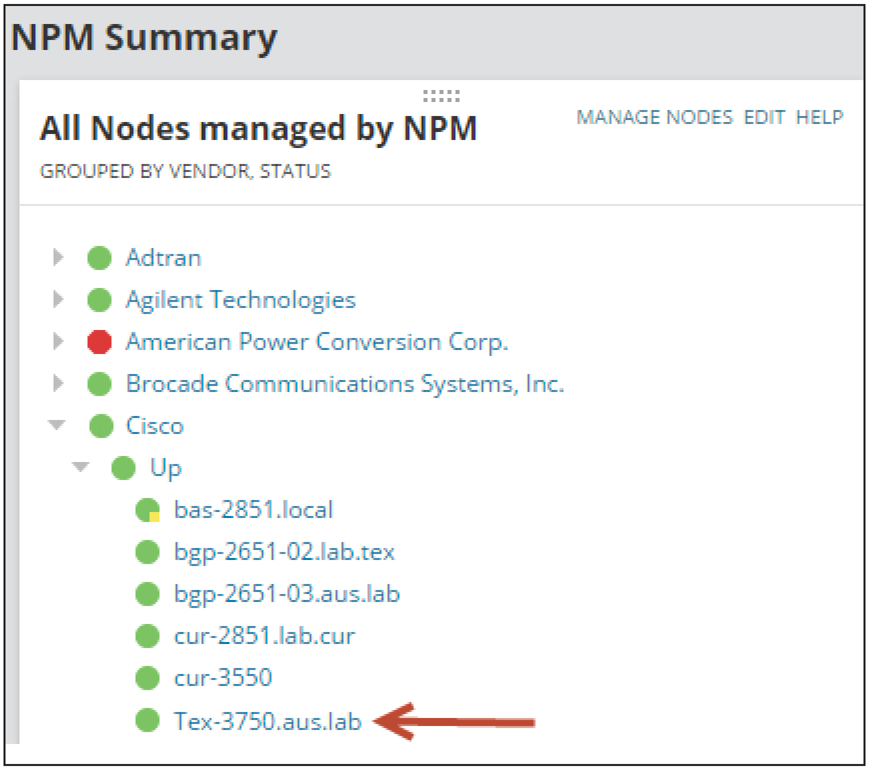
  ⓘ NPM and NCM use the **same** process for discovering network devices and adding them to the Orion Platform. There is no discovery specific to NCM.

SolarWinds recommends that you begin by discovering a limited number of core routers and switches so that you can learn how to manage them with NCM. Then you can add more devices to scale your deployment.

If you are unsure if you discovered any network devices, log in to the Orion Platform and click My Dashboards > Home > Summary. The All Nodes resource lists all network devices discovered and added to Orion for monitoring.

ⓘ After you discover and add devices to the Orion platform for monitoring, you also need to add the devices to NCM.

The examples in this guide use the Tex-3750.aus.lab Cisco router to illustrate how to back up and make changes to a config.



NPM Summary

All Nodes managed by NPM

GROUPED BY VENDOR, STATUS

- ● Adtran
- ● Agilent Technologies
- ● American Power Conversion Corp.
- ● Brocade Communications Systems, Inc.
- ● Cisco
  - ● Up
    - ● bas-2851.local
    - ● bgp-2651-02.lab.tex
    - ● bgp-2651-03.aus.lab
    - ● cur-2851.lab.cur
    - ● cur-3550
    - ● Tex-3750.aus.lab

Add a device to NCM

After you discover and add devices to the Orion platform for monitoring, you also need to add the devices to NCM. When you add a device to NCM, you configure a connection profile that establishes a line of communication between NCM and the node you want to manage. Communication is established by Telnet or SSH protocols.

Before you begin:

- Locate the login credentials for the node you want to add to NCM.
- Determine whether NCM communicates with the device by way of Telnet or SSH.
- Identify the Telnet or SSH ports used for communication.

The following example illustrates how to add the Tex-3750.lab.aus router to NCM for management. This router has already been added to, and is monitored by, the Orion platform and now needs to be added to NCM.

ⓘ For information about setting global variables, see Configure nodes to use device-level login credentials for NCM connections. For information about **other** connection options (such as connection profiles and user-level logins), see Options for specifying NCM connection information.

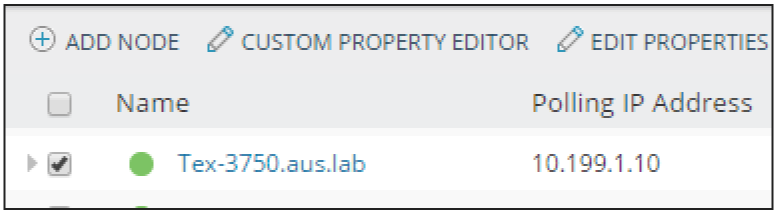
1. Click Settings > Manage Nodes.

   The Manage Nodes view lists all of the nodes that have been added to the Orion Web Console. Nodes that have been added to NCM have Yes in the NCM - Licensed column.

   > - If the Manage Entities view opens instead of the Manage Nodes view, click Commands > Switch Back to Legacy page.
   > - If the Manage Nodes view does not show the NCM - Licensed column, click the » icon at the far right of the table header and add the NCM - Licensed column.

2. Select all of the devices that you want to bring under NCM management, and click Edit Properties.

   This example adds the Tex-3750.aus.lab router under NCM management.

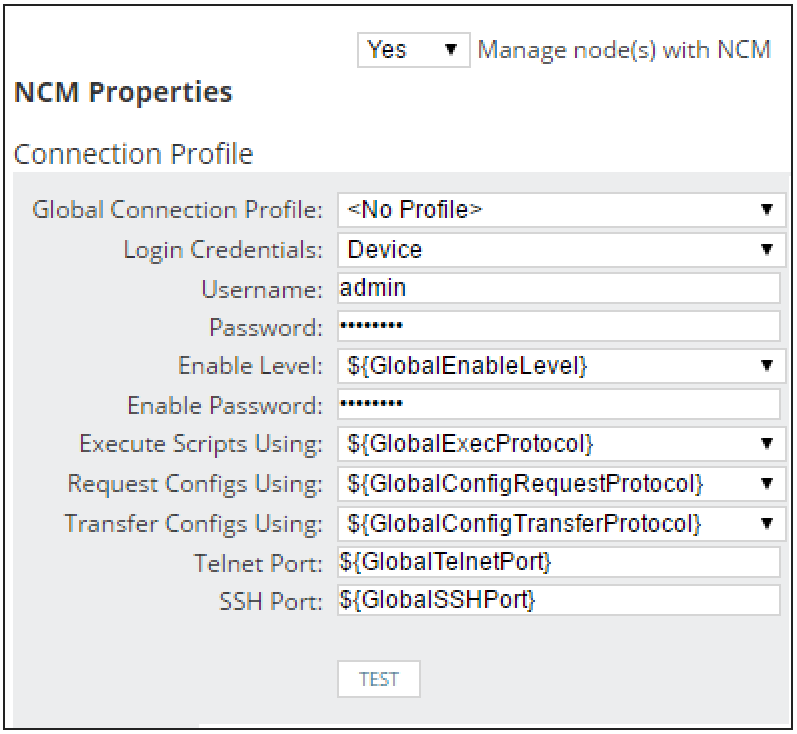


	Name	Polling IP Address
☑	● Tex-3750.aus.lab	10.199.1.10

3. In the Manage Node(s) with NCM field, select Yes.

   The NCM Properties are listed with their current values.

4. Enter the connection profile credentials and then click Test to make sure there is a valid connection between NCM and the router.



Yes ▼ Manage node(s) with NCM

NCM Properties

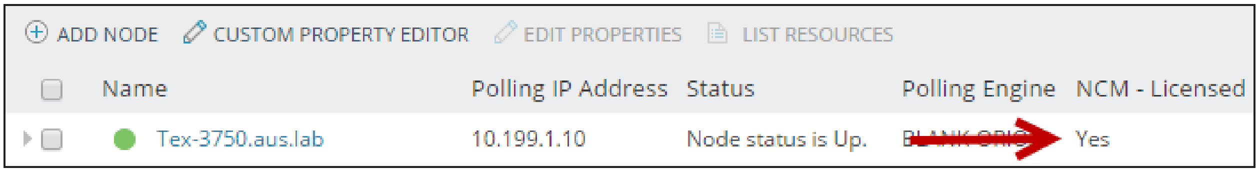
Connection Profile

Global Connection Profile: <No Profile> ▼
Login Credentials: Device ▼
Username: admin
Password: ••••••••
Enable Level: ${GlobalEnableLevel} ▼
Enable Password: ••••••••
Execute Scripts Using: ${GlobalExecProtocol} ▼
Request Configs Using: ${GlobalConfigRequestProtocol} ▼
Transfer Configs Using: ${GlobalConfigTransferProtocol} ▼
Telnet Port: ${GlobalTelnetPort}
SSH Port: ${GlobalSSHPort}

5. When a successful connection is made, click Submit.

   The results are displayed on the Managed Nodes page.

6. To verify the router was successfully added, view the NCM - Licensed column.



	Name	Polling IP Address	Status	Polling Engine	NCM - Licensed
□	● Tex-3750.aus.lab	10.199.1.10	Node status is Up.	BLANK-ORIG	Yes

Manage network change with NCM

This section includes the following topics:

- Ways to edit network configs
- Back up a network config manually
- Edit a network config using a script
- Run an NCM inventory scan on a node
- Edit a network config using a config change template

Ways to edit network configs

You can use NCM to streamline complex configuration changes and make bulk changes to the configs on multiple nodes. To edit a config, you can manually run a script against a node or use a config change template. Read below about the differences between using a script and a template to decide which method is right for your task. The troubleshooting and remediation section provides an example of a config change that had a major impact on a network and how a system administrator used tools to discover and remedy the problem.

Scripts

If you do not need the advanced logic available with config change templates, executing a command script is the most effective way to change configurations on multiple devices. Scripts can be executed manually or scheduled. Users who write scripts must know command line interface (CLI) commands required to make the config changes on a specific device type.

Several tasks can be automated with command scripts. For example, you can:

- Download configuration files
- Upload configuration files
- Upload IOS images
- Update login banners
- Update access control lists (ACLs)

Ready to create a script?

Config change templates

Config change templates are based on a programming language that enables you to create sophisticated config change routines using conditional logic, control flow, and string and value comparison. This method removes the chance of incorrect script syntax creating network errors.

Examples of tasks that can be completed using a template include:

- Change VLAN membership by device port
- Configure device interfaces based on description
- Enable IPSLA for VOIP implementations
- Manage a NetFlow collection at the source device

You can use the config change templates provided with NCM out-of-the-box, import templates from THWACK, or create your own.

> ⓘ The framework for creating config change templates depends on the SolarWinds Information Service (SWIS). SWIS is an API that is installed with NCM and interacts with inventory data in the Orion Platform database. Any device that is not inventoried in NCM cannot be targeted with a config change template. Each object in a device inventory is a SWIS entity that can be referenced in specific ways within scripts.

Ready to run a template?

Back up a network config manually

Before you make a change to a config, SolarWinds recommends that you back up the config in case the change is unsuccessful. If the change is unsuccessful, you can revert to the version you backed up. Configs monitored by NCM are scheduled to be automatically backed up each night. You can use the default backup job, or you can customize it to meet your needs.

> ⓘ To back up a config, you download a copy of the config from the device. The config backup is stored in the Orion database. If you specify a config archive location on the Orion server or on a network drive, the downloaded config files are also stored in that location.

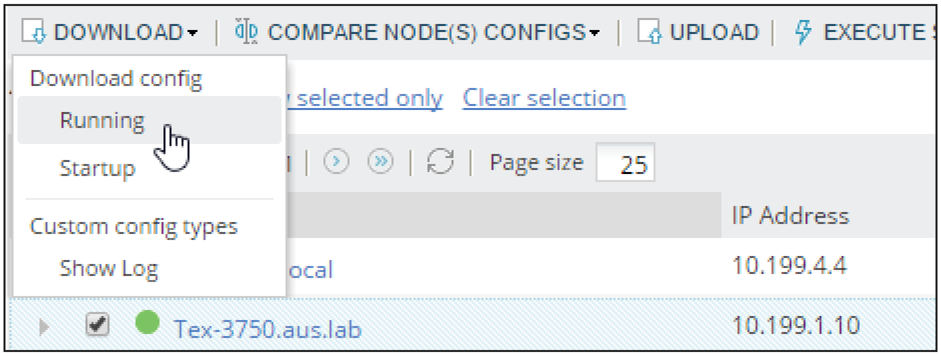
SolarWinds recommends the following best practices:

- For configurations that change daily, schedule a daily backup of the config.
- Use the real-time change detection feature to automatically be notified when a change is made.
- At a minimum, back up configs weekly.

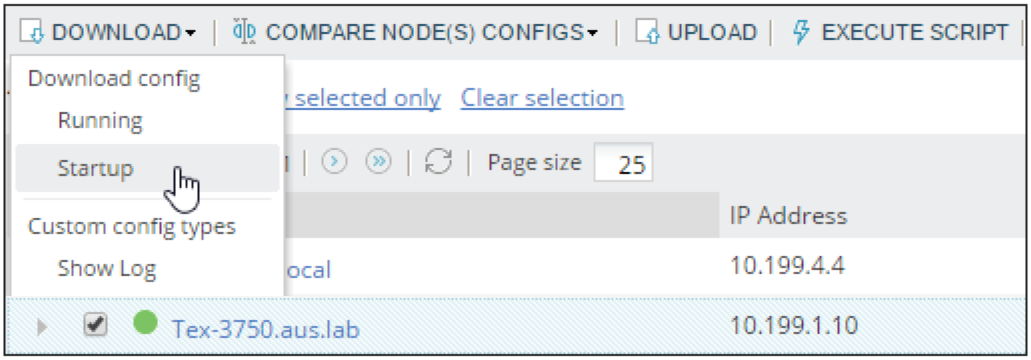
For the purposes of this guide, and so that you do not have to wait until the nightly backup job has run, you can manually back up a config.

The following example backs up the running and the startup config for the Tex-3750.aus.lab router.

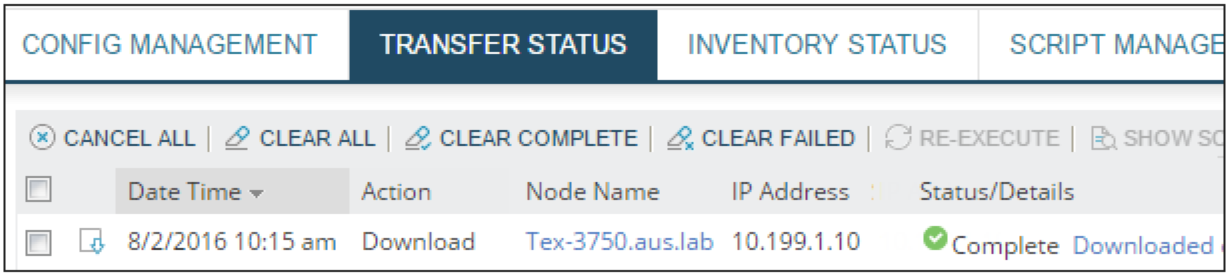
1. Click My Dashboards > Network Configuration > Configuration Management.
2. Select the device with the configs you want to back up.
3. Click Download > Running.



4. Click Download > Startup.



5. To verify the config was backed up, click the Transfer Status tab and view the Status column.



□		Date Time	Action	Node Name	IP Address	Status/Details
□		8/2/2016 10:15 am	Download	Tex-3750.aus.lab	10.199.1.10	✓ Complete Downloaded

Edit a network config using a script

Edit config change scripts to update access lists, modify community strings, or make other configuration changes. Before you write a script, be sure you know the commands required to make changes on the device and the basics of variables and logical structures. This guide does not address device-specific CLI commands.

Scripts are often used to make bulk changes to multiple devices. SolarWinds recommends running a script on one device to test your changes and, if you verify your changes and they are successful, then apply the script to multiple devices.

This topic provides steps on how to add, edit, and verify a config change script for one or more devices.

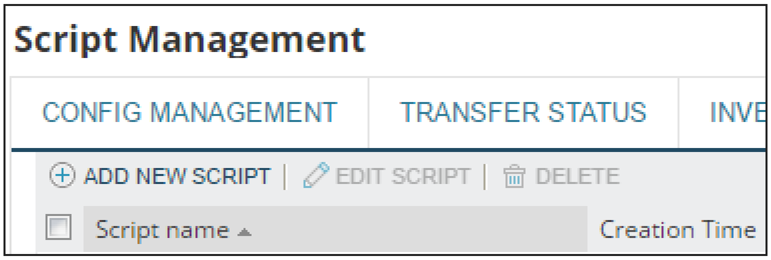
Before making changes to a config, make sure that the config has been backed up.

Add a config change script

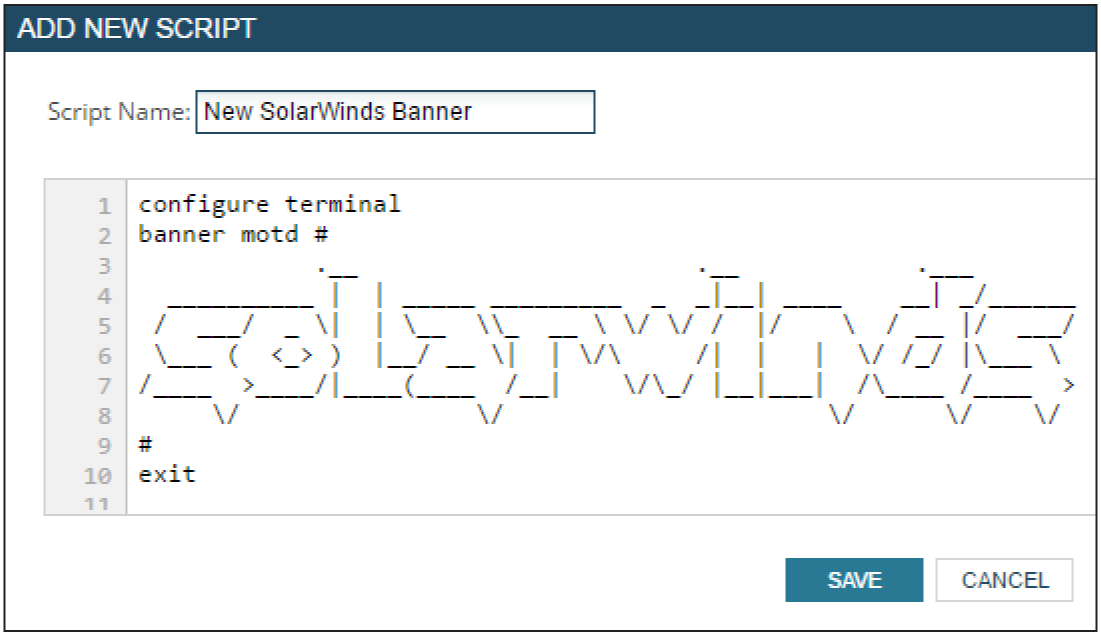
To edit a config using a script, you must first add a config change script.

The following example shows how to add a SolarWinds banner config change script. The commands in this script run on a Cisco device.

1. Click My Dashboards > Network Configuration > Configuration Management.
2. Click the Script Management tab.
3. Click Add New Script.



4. Enter the script information and click Save.

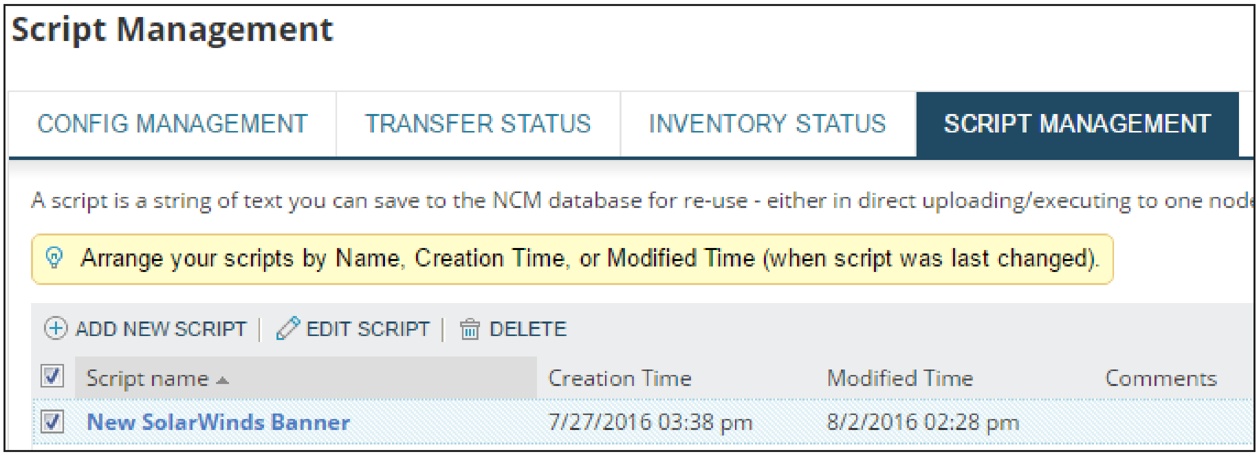


ADD NEW SCRIPT

Script Name: New SolarWinds Banner

```
configure terminal
banner motd #
             .__                       .__            .___      
  __________ |  | _____ ________  _  _|__| ____    __| _/______
 /  ___/  _ \|  | \__  \\_  __ \ \/ \/ /  |/    \  / __ |/  ___/
 \___ (  <_> )  |__/ __ \|  | \/\     /|  |   |  \/ /_/ |\___ \ 
/____  >____/|____(____  /__|    \/\_/ |__|___|  /\____ /____  >
     \/                \/                      \/      \/    \/ 
#
exit
```

The script is displayed in the Script Management tab.



Script Management

A script is a string of text you can save to the NCM database for re-use - either in direct uploading/executing to one node

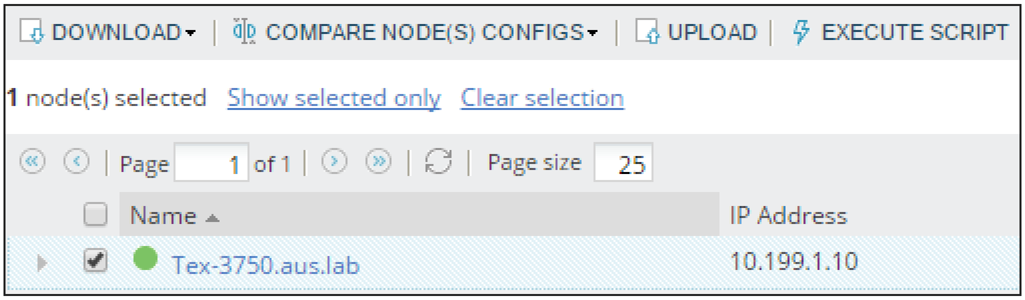
Arrange your scripts by Name, Creation Time, or Modified Time (when script was last changed).

☑	Script name ▲	Creation Time	Modified Time	Comments
☑	New SolarWinds Banner	7/27/2016 03:38 pm	8/2/2016 02:28 pm	

Edit a config using a script

The following example shows how to execute the SolarWinds banner script against a node managed in NCM.

1. Click My Dashboards > Network Configuration > Configuration Management.
2. Select the configuration item to edit and click Execute Script.



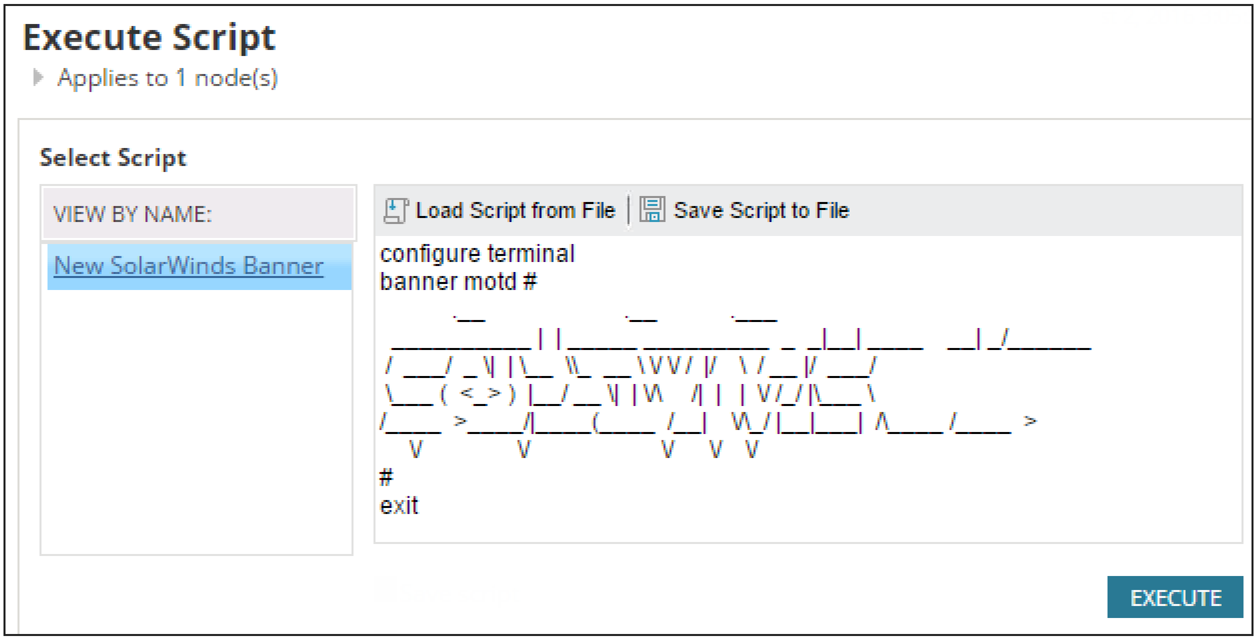
DOWNLOAD ▾ | COMPARE NODE(S) CONFIGS ▾ | UPLOAD | EXECUTE SCRIPT

1 node(s) selected Show selected only Clear selection

Page 1 of 1 | Page size 25

	Name ▴	IP Address
☑ ●	Tex-3750.aus.lab	10.199.1.10

3. Select a script and click Execute.



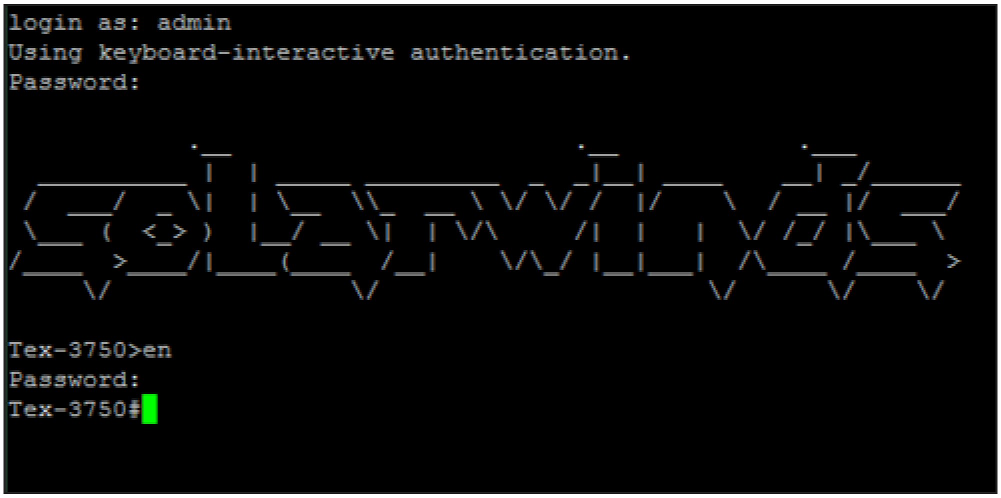
Execute Script

Applies to 1 node(s)

Select Script

```
configure terminal
banner motd #
            .__                        .__              .___
  __________|  | _____ ____________  _  _|__| ____    __| _/______
 /  ___/  _ \  | \__  \\_  __ \ \/ \/ /  |/    \  / __ |/  ___/
 \___ (  <_> )  |__/ __ \|  | \/\     /|  |   |  \/ /_/ |\___ \
/____  >____/|____(____  /__|    \/\_/ |__|___|  /\____ /____  >
     \/                \/                      \/      \/    \/
#
exit
```

4. To view the change you just made, log in to the device. This is an example of the script banner change for the Tex-3750.aus.lab router.



```
login as: admin
Using keyboard-interactive authentication.
Password:

            .__                        .__              .___
  __________|  | _____ ____________  _  _|__| ____    __| _/______
 /  ___/  _ \  | \__  \\_  __ \ \/ \/ /  |/    \  / __ |/  ___/
 \___ (  <_> )  |__/ __ \|  | \/\     /|  |   |  \/ /_/ |\___ \
/____  >____/|____(____  /__|    \/\_/ |__|___|  /\____ /____  >
     \/                \/                      \/      \/    \/

Tex-3750>en
Password:
Tex-3750#
```

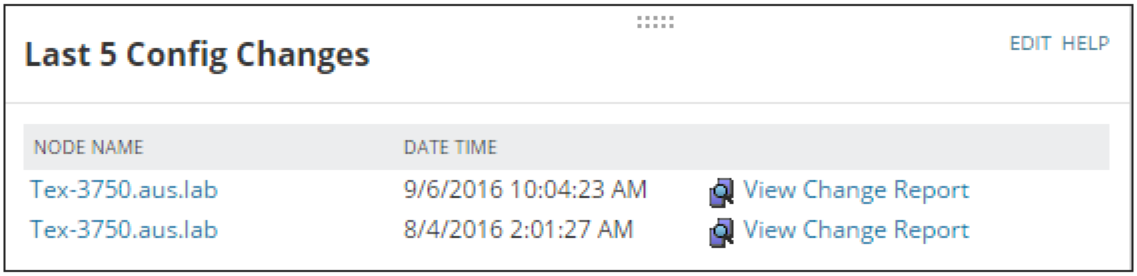
Verify config changes by comparing config versions

After you change a login banner, you can log in to the device to verify the change. For more complex changes, you can verify the change by viewing a report that compares the configs before and after the change. Because the config change report compares configs line by line, you can also use the report to troubleshoot issues.

The following example shows that the Tex-3750.aus.lab router config was updated on August 4, and the report highlights the differences between the config before and after the change.

1. Click My Dashboards > Network Configuration > Config Summary.
2. Navigate to the Last 5 Config Changes resource and note the date and time of the config change.

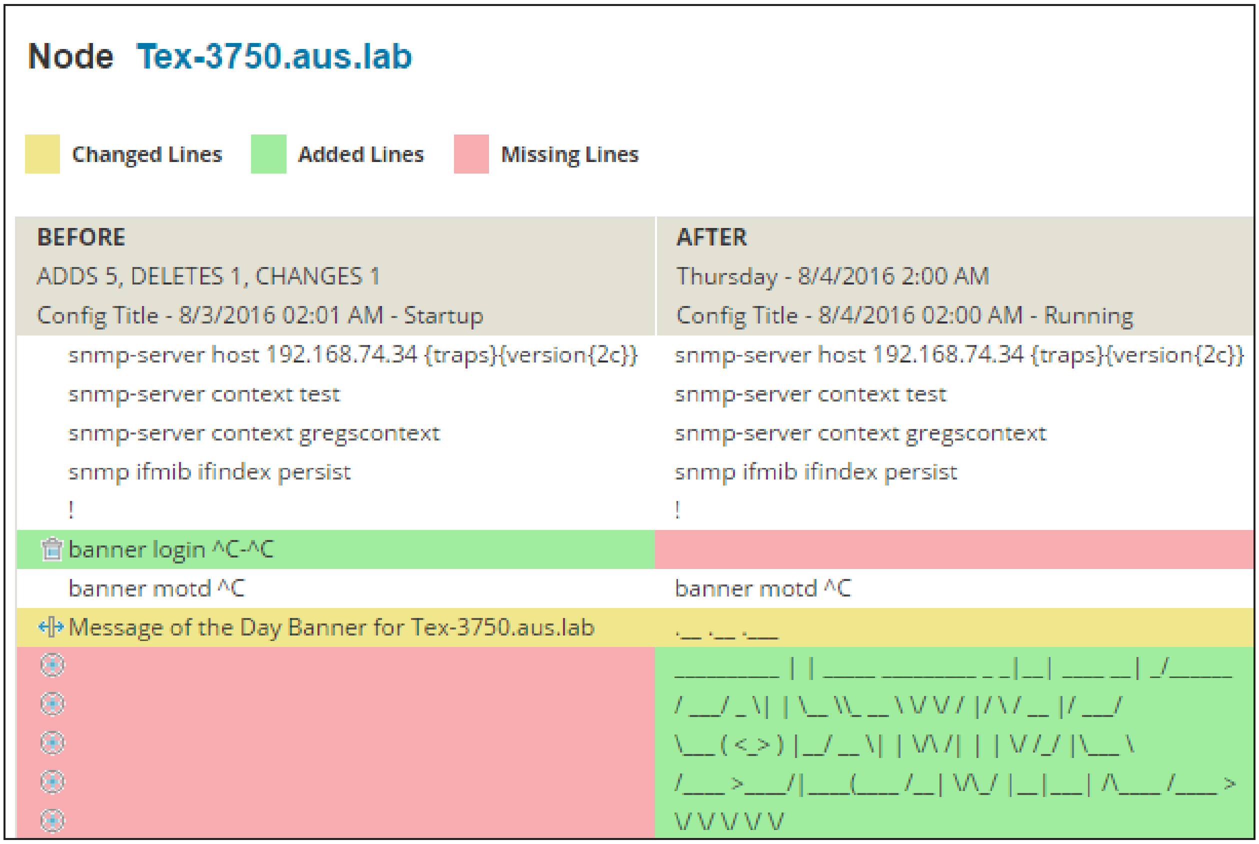
   ⓘ You can click Edit to change the number of configs listed in the resource.



Last 5 Config Changes

NODE NAME	DATE TIME	
Tex-3750.aus.lab	9/6/2016 10:04:23 AM	View Change Report
Tex-3750.aus.lab	8/4/2016 2:01:27 AM	View Change Report

3. To view changes, click the View Change Report link.



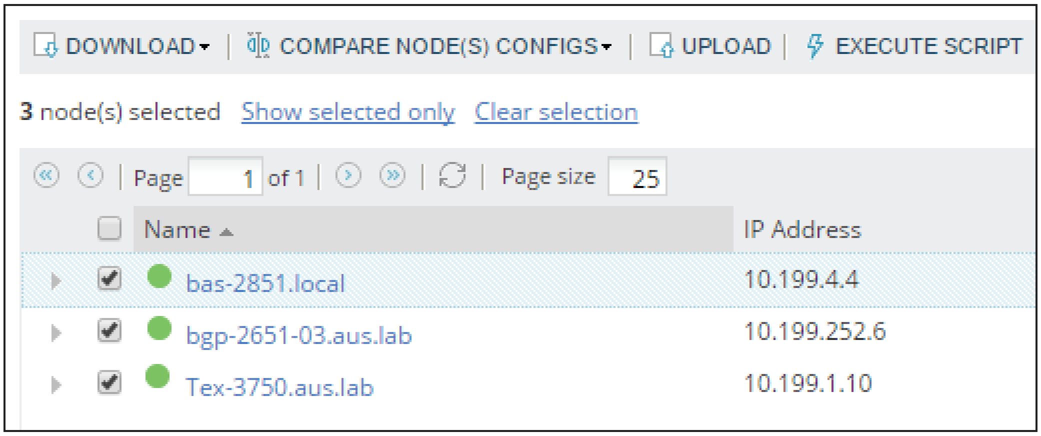
Node Tex-3750.aus.lab

🟨 Changed Lines 🟩 Added Lines 🟥 Missing Lines

<table>
<tr><th>BEFORE
ADDS 5, DELETES 1, CHANGES 1
Config Title - 8/3/2016 02:01 AM - Startup</th><th>AFTER
Thursday - 8/4/2016 2:00 AM
Config Title - 8/4/2016 02:00 AM - Running</th></tr>
<tr><td>snmp-server host 192.168.74.34 {traps}{version{2c}}</td><td>snmp-server host 192.168.74.34 {traps}{version{2c}}</td></tr>
<tr><td>snmp-server context test</td><td>snmp-server context test</td></tr>
<tr><td>snmp-server context gregscontext</td><td>snmp-server context gregscontext</td></tr>
<tr><td>snmp ifmib ifindex persist</td><td>snmp ifmib ifindex persist</td></tr>
<tr><td>!</td><td>!</td></tr>
<tr><td>banner login ^C-^C</td><td></td></tr>
<tr><td>banner motd ^C</td><td>banner motd ^C</td></tr>
<tr><td>Message of the Day Banner for Tex-3750.aus.lab</td><td>'__ '__ '___</td></tr>
<tr><td></td><td>_________ | | _____ _________ _ _|__| _____ __| _/_____</td></tr>
<tr><td></td><td>/ __/ _ \| | __ \__ __ \ V V / |/ \/ __ |/ __/</td></tr>
<tr><td></td><td>__ (<_>) |__/ __ \| | \W/| | | V /_/ |__ \</td></tr>
<tr><td></td><td>/___ >___/|___(___ /__| \W_/ |__|___| /___ /___ ></td></tr>
<tr><td></td><td>V V V V V</td></tr>
</table>

Edit multiple configs

To make changes to multiple devices, select multiple configs before you click Execute Script.



DOWNLOAD ▾ | COMPARE NODE(S) CONFIGS ▾ | UPLOAD | EXECUTE SCRIPT

3 node(s) selected Show selected only Clear selection

Page 1 of 1 | Page size 25

	□	Name ▲	IP Address
▸	☑	● bas-2851.local	10.199.4.4
▸	☑	● bgp-2651-03.aus.lab	10.199.252.6
▸	☑	● Tex-3750.aus.lab	10.199.1.10

Run an NCM inventory scan on a node

An inventory scan queries a node and gathers device information including the model and serial numbers, the operating system version, the number of NIC or interface cards, routing protocols, IP addresses, active ports, and much more. An inventory scan is a prerequisite for creating and running a config change template because the framework for creating config change templates depends on the SolarWinds Information Service (SWIS). SWIS is an API installed with NCM that interacts with inventory data in the Orion Platform database. Any device that is not inventoried in NCM cannot be targeted with a config change template.

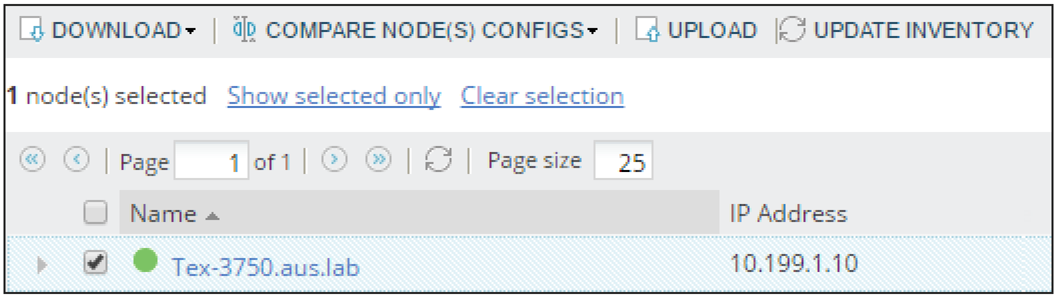
The information collected from an inventory scan can also be viewed in a number of inventory reports.

You can the choose the type of information collected by NCM for the inventory scan, as well as other settings that help you manage the inventory process. You can perform inventory scans on all of your nodes, node groups, or on a single node.

> As a best practice, the system automatically runs a daily inventory scan at midnight. If you have other jobs that run at the same time, you can change the time the inventory scan runs to avoid conflict. To have the latest available information, run an inventory scan before you generate NCM reports.

For the purpose of this guide, and to populate data now, the following example manually runs an inventory scan on the Tex-3750.aus.lab router.

1. Click My Dashboards > Network Configuration > Configuration Management.
2. Select the Tex-3750.aus.lab router and click Update Inventory.

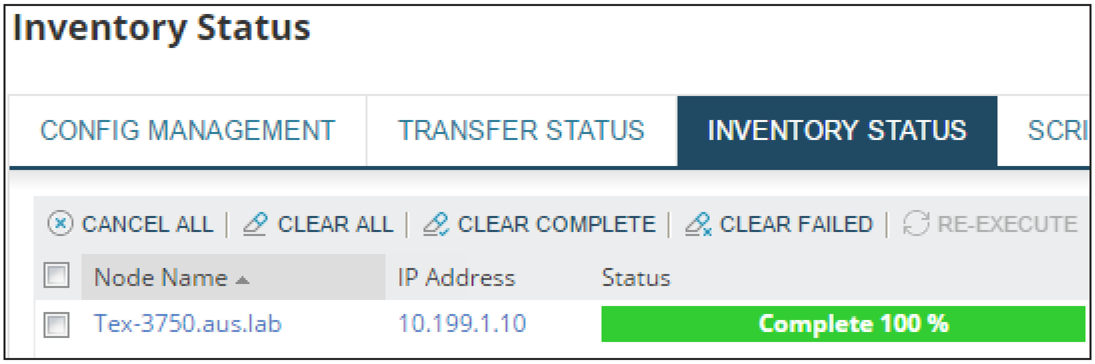


1 node(s) selected

	Name ▲	IP Address
☑	● Tex-3750.aus.lab	10.199.1.10

3. Click Yes at the confirmation prompt.

   When the inventory scan is complete, the progress bar reads Complete 100%.



□	Node Name ▲	IP Address	Status
□	Tex-3750.aus.lab	10.199.1.10	Complete 100 %

4. To view an inventory report, see Run an NCM inventory report.

Edit a network config using a config change template

Config change templates save time and ensure that changes are consistently applied to devices. You can use an out-of-the-box template or create a custom template.

> Templates are often used to make bulk changes to multiple devices. SolarWinds recommends running a template on one device to test your changes and, when you verify your changes are successful, then apply the template to multiple devices.

The example in this section shows how to apply the login banner template for a Cisco router. Other commonly used templates include:

- Change passwords
- Change SNMP settings
- Enable Netflow
- Define ACLs
- Define VLAN memberships

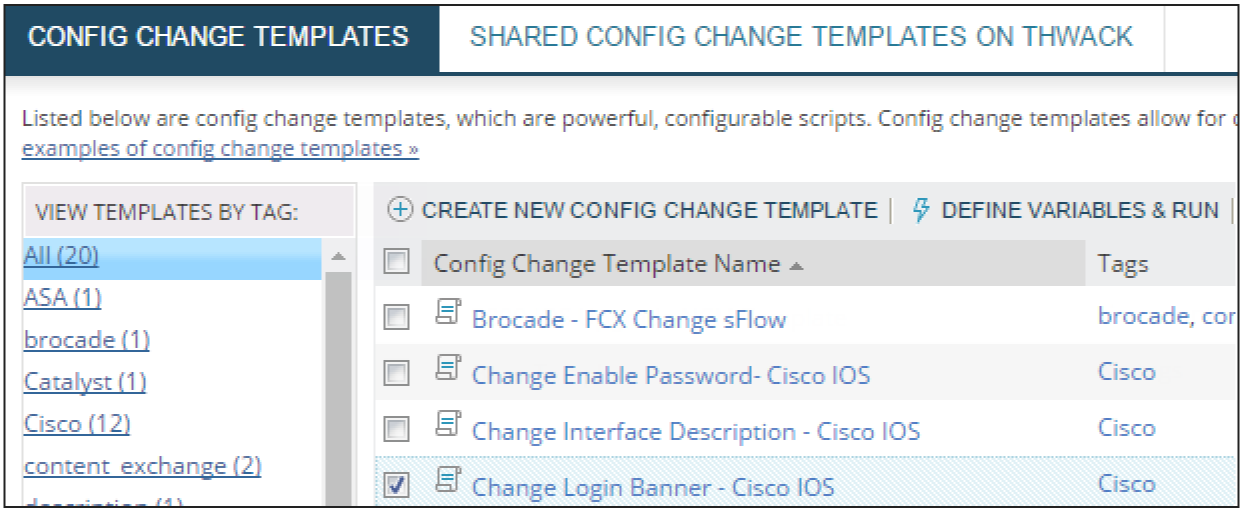
Before you begin:

- Run an NCM inventory scan on a node: if you have just added a device, you must perform an NCM device inventory scan and update device inventories before you can create and run a config change template.
- Be sure that the config is Back up a network config manually: SolarWinds recommends that you back up a config before you make a change so that you can revert to a previous version of the config if the change is not successful.

Execute the banner change template

This example uses a template to create a restricted access warning in the login banner.

1. Click My Dashboards > Network Configuration > Config Change Template.
2. Select the Change Login Banner template and click Define Variables & Run.



CONFIG CHANGE TEMPLATES | SHARED CONFIG CHANGE TEMPLATES ON THWACK

Listed below are config change templates, which are powerful, configurable scripts. Config change templates allow for

examples of config change templates »

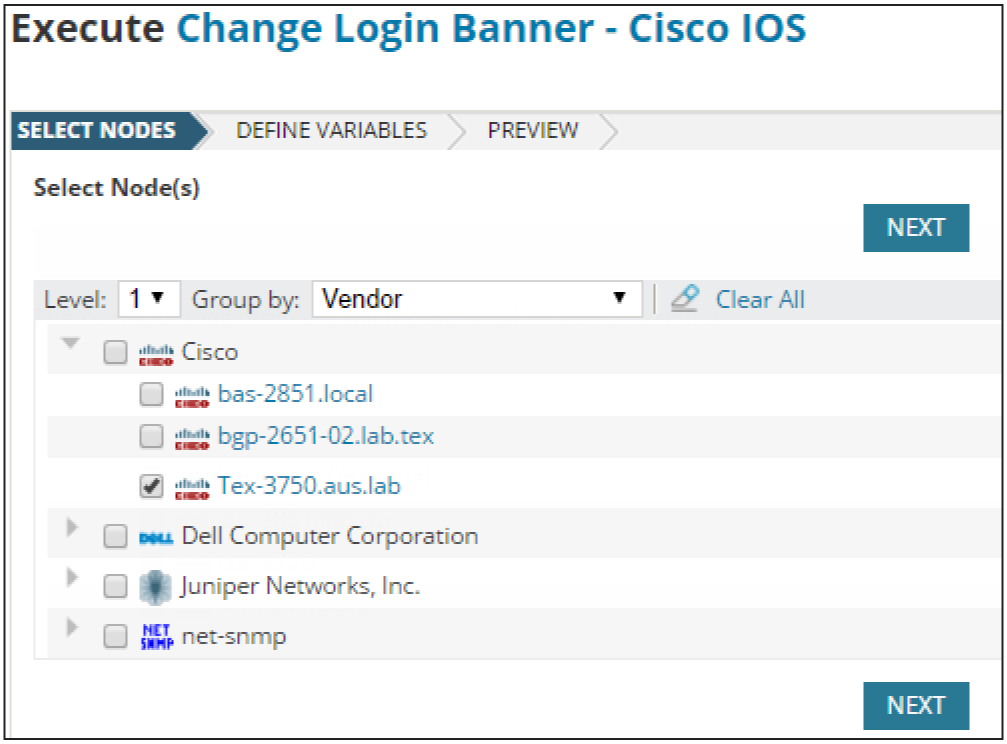
VIEW TEMPLATES BY TAG:

- All (20)
- ASA (1)
- brocade (1)
- Catalyst (1)
- Cisco (12)
- content_exchange (2)

⊕ CREATE NEW CONFIG CHANGE TEMPLATE | DEFINE VARIABLES & RUN

□	Config Change Template Name ▲	Tags
□	Brocade - FCX Change sFlow	brocade, cor
□	Change Enable Password- Cisco IOS	Cisco
□	Change Interface Description - Cisco IOS	Cisco
☑	Change Login Banner - Cisco IOS	Cisco

3. Select nodes and click Next.



Execute Change Login Banner - Cisco IOS

SELECT NODES > DEFINE VARIABLES > PREVIEW

Select Node(s)

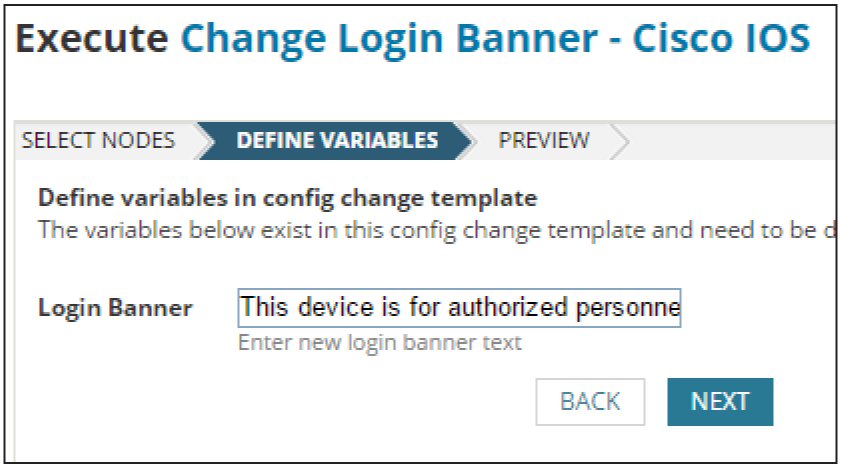
NEXT

Level: 1 ▼ Group by: Vendor ▼ | Clear All

- □ Cisco
  - □ bas-2851.local
  - □ bgp-2651-02.lab.tex
  - ☑ Tex-3750.aus.lab
- □ Dell Computer Corporation
- □ Juniper Networks, Inc.
- □ net-snmp

NEXT

4. In the Login Banner field, enter the banner text and click Next.



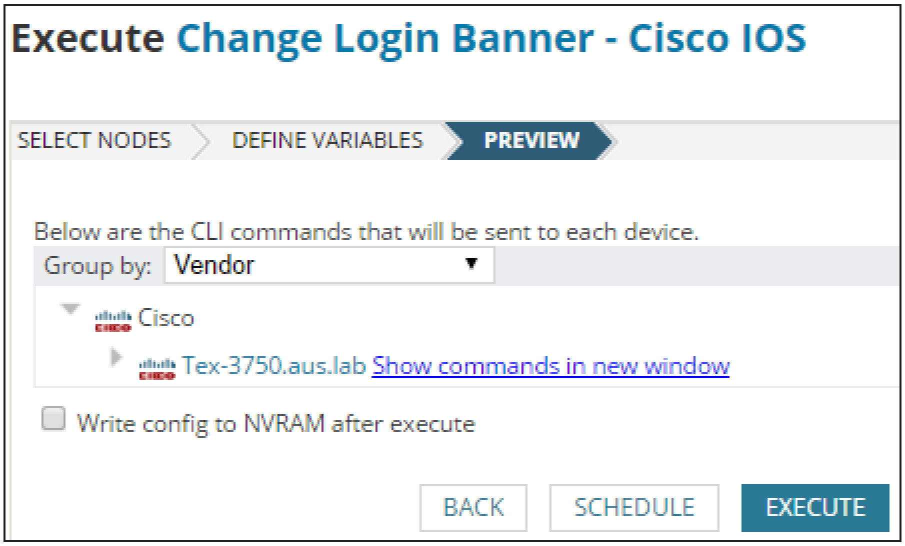
Define variables in config change template

The variables below exist in this config change template and need to be d

Login Banner: This device is for authorized personne

Enter new login banner text

5. To preview the script, click Show commands in new window.



Execute Change Login Banner - Cisco IOS
SELECT NODES
DEFINE VARIABLES
PREVIEW

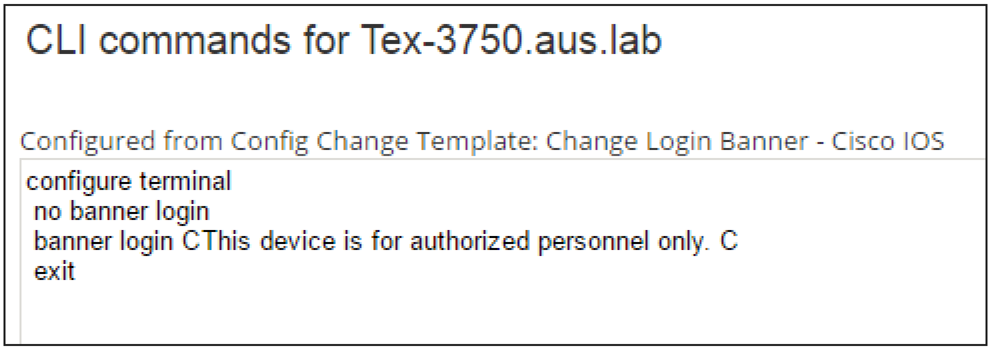
Below are the CLI commands that will be sent to each device.

Group by: Vendor

Cisco
Tex-3750.aus.lab Show commands in new window

□ Write config to NVRAM after execute

6. Verify the CLI commands and the banner text are correct in the script preview.

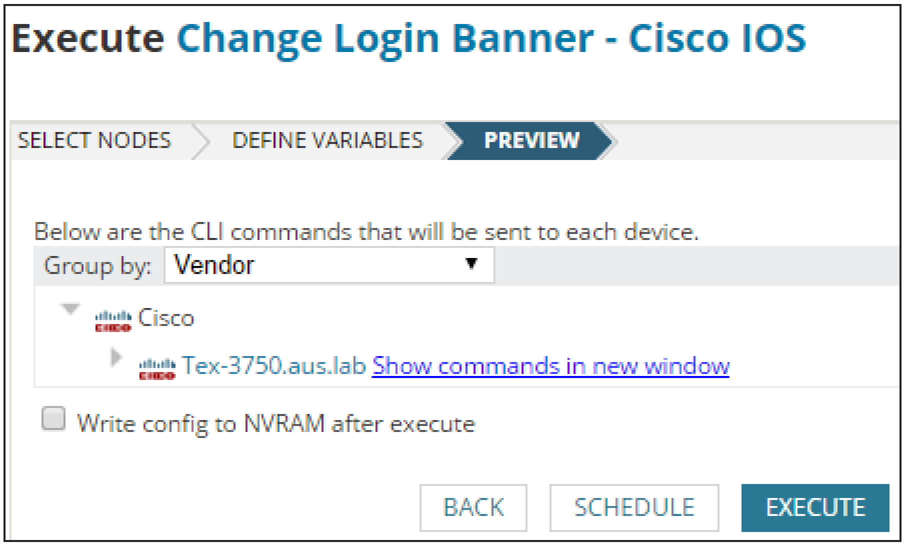


CLI commands for Tex-3750.aus.lab

Configured from Config Change Template: Change Login Banner - Cisco IOS

```
configure terminal
 no banner login
 banner login CThis device is for authorized personnel only. C
 exit
```

7. Click Execute.



Execute Change Login Banner - Cisco IOS

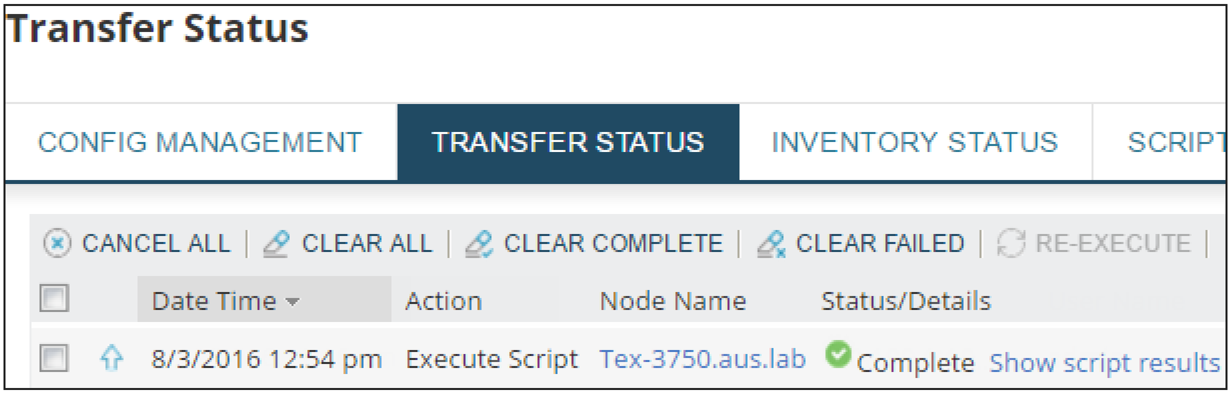
Below are the CLI commands that will be sent to each device.

Group by: Vendor

Cisco
Tex-3750.aus.lab Show commands in new window

□ Write config to NVRAM after execute

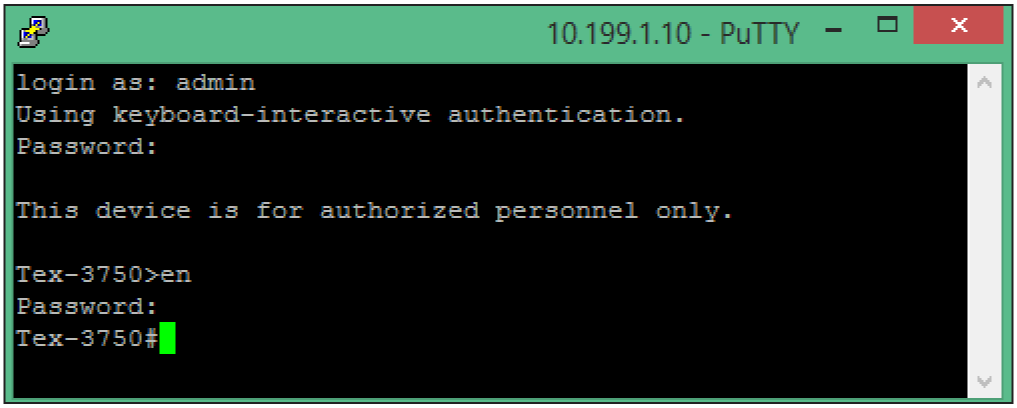
The Transfer Status tab shows the script execution status.



Transfer Status

□	Date Time	Action	Node Name	Status/Details
□	8/3/2016 12:54 pm	Execute Script	Tex-3750.aus.lab	✓ Complete Show script results

8. To view a change, log in to the device. This is an example of the login banner change for the Tex-3750.aus.lab router.



```
login as: admin
Using keyboard-interactive authentication.
Password:

This device is for authorized personnel only.

Tex-3750>en
Password:
Tex-3750#
```

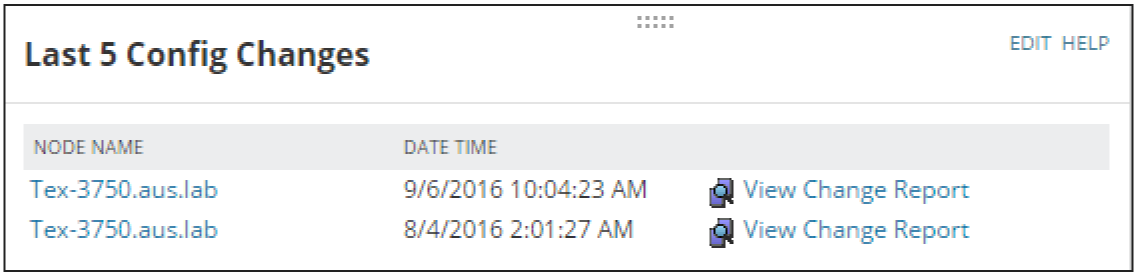
Verify config changes by comparing configs

After you change a login banner, you can log in to the device to verify the change. For more complex changes or changes across multiple configuration items, you can verify the change by viewing a report that compares the configs before and after the change. Because the config change report compares configs line by line, you can also use the report to troubleshoot issues.

The following example shows that the Tex-3750.aus.lab router config was updated on August 4, and the report highlights the differences between the config before and after the change.

1. Click My Dashboards > Network Configuration > Config Summary.
2. Navigate to the Last 5 Config Changes resource and note the date and time of the config change.

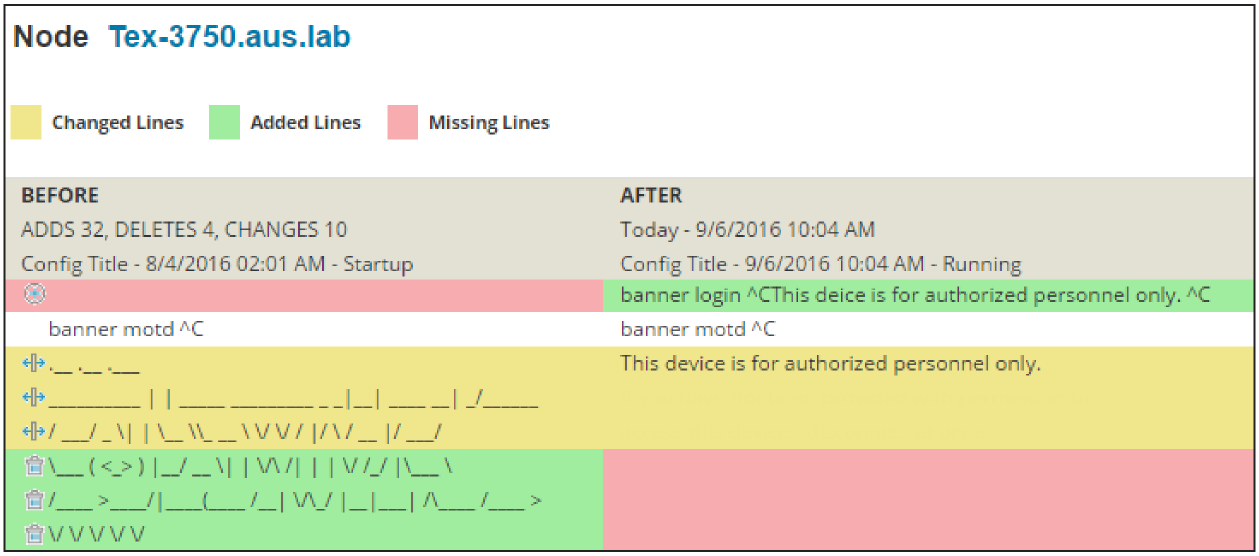
   ⓘ You can click Edit to change the number of configs listed in the resource.



Last 5 Config Changes

NODE NAME	DATE TIME	
Tex-3750.aus.lab	9/6/2016 10:04:23 AM	View Change Report
Tex-3750.aus.lab	8/4/2016 2:01:27 AM	View Change Report

3. To view changes, click the View Change Report link.



Node Tex-3750.aus.lab

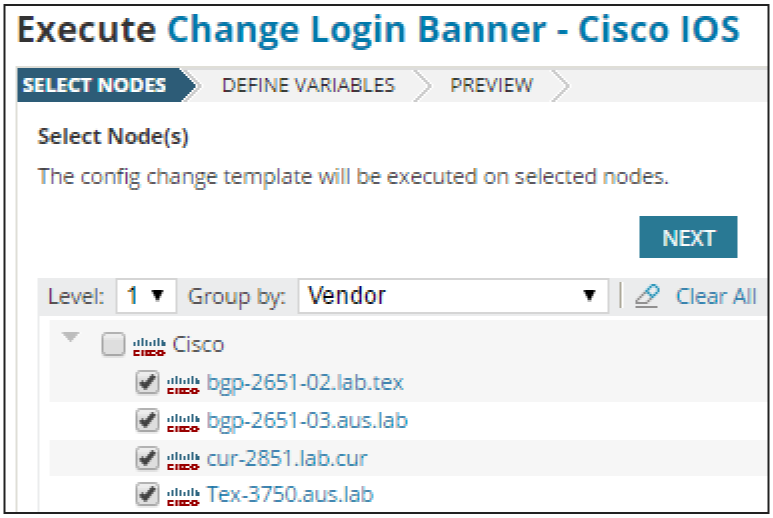
🟨 Changed Lines 🟩 Added Lines 🟥 Missing Lines

<table>
<tr><th>BEFORE</th><th>AFTER</th></tr>
<tr><td>ADDS 32, DELETES 4, CHANGES 10</td><td>Today - 9/6/2016 10:04 AM</td></tr>
<tr><td>Config Title - 8/4/2016 02:01 AM - Startup</td><td>Config Title - 9/6/2016 10:04 AM - Running</td></tr>
<tr><td></td><td>banner login ^CThis deice is for authorized personnel only. ^C</td></tr>
<tr><td>banner motd ^C</td><td>banner motd ^C</td></tr>
<tr><td>.__ .__ .___
_________ | | _____ ________ _ _|__| ____ __| _/_____
/ ___/ _\| | __ _ __ \ V V / |/ \ / __ |/ ___/</td><td>This device is for authorized personnel only.</td></tr>
<tr><td>___ (<_>) |__/ __\| | \/\ /| | | V /_/ |___ \
/____ >___/|___(____ /__| \/_/ |__|___| /____ /____ >
\/ \/ \/ \/ \/</td><td></td></tr>
</table>

Edit multiple nodes

To make changes to multiple devices, select multiple nodes before you click Execute Script.

If you want to verify changes to multiple devices, review the Status/Details of the Transfer Status tab.



Execute Change Login Banner - Cisco IOS

Select Node(s)

The config change template will be executed on selected nodes.

- □ Cisco
  - ☑ bgp-2651-02.lab.tex
  - ☑ bgp-2651-03.aus.lab
  - ☑ cur-2851.lab.cur
  - ☑ Tex-3750.aus.lab

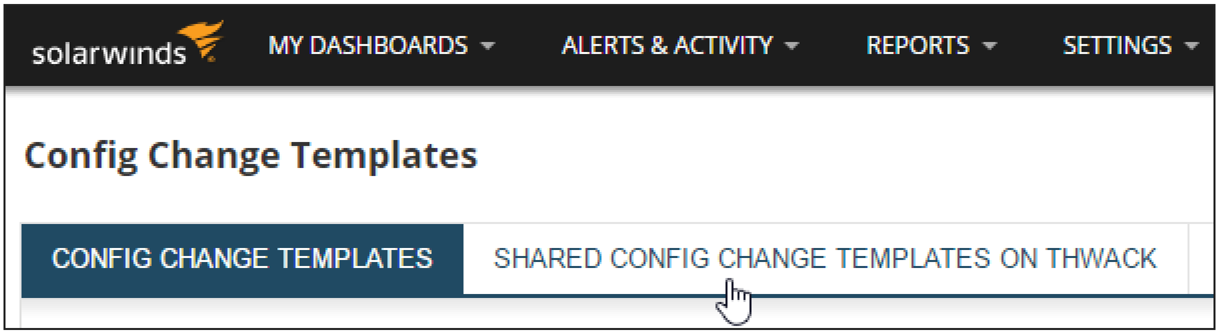
Import a config change template from THWACK

NCM ships with preconfigured templates you can use to make common changes to configs. You can also create your own change templates, or import change templates that other SolarWinds customers have created and posted to THWACK.

> ⓘ Creating a change template is not addressed in this guide. For information on creating a change template, see the SolarWinds Network Configuration Manager Administrator Guide.

Before you begin, create a THWACK account.

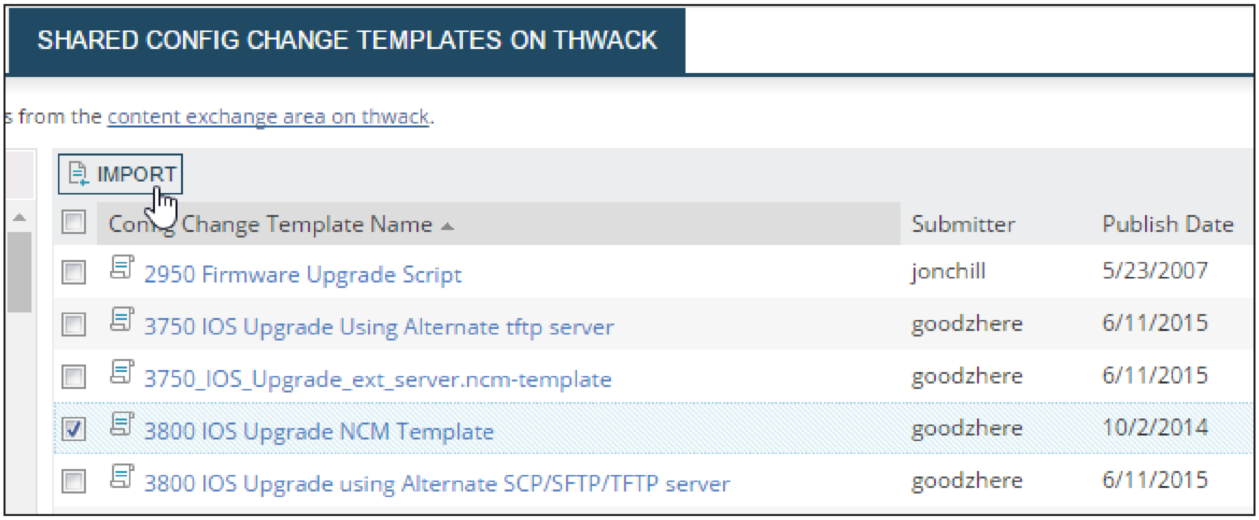
1. Click My Dashboards > Network Configuration > Config Change Templates.
2. On the Config Change Templates page, click Shared Config Change Templates on THWACK.



Config Change Templates

NCM automatically connects with THWACK and populates the list with shared config change templates.

3. Select a template and click Import.



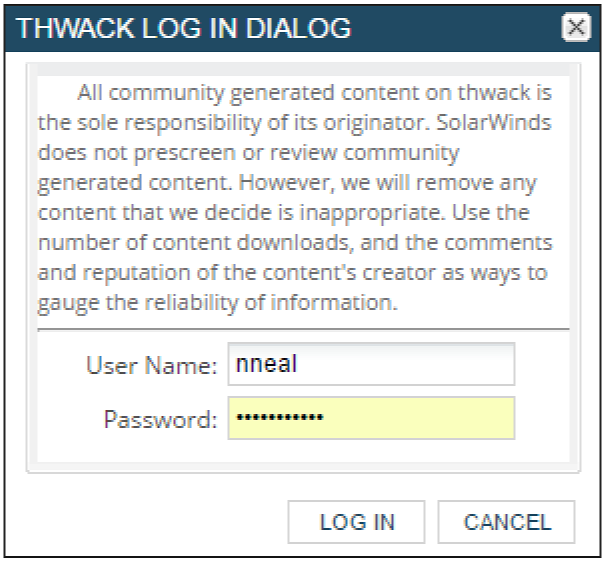
SHARED CONFIG CHANGE TEMPLATES ON THWACK

s from the content exchange area on thwack.

IMPORT

□	Config Change Template Name ▲	Submitter	Publish Date
□	2950 Firmware Upgrade Script	jonchill	5/23/2007
□	3750 IOS Upgrade Using Alternate tftp server	goodzhere	6/11/2015
□	3750_IOS_Upgrade_ext_server.ncm-template	goodzhere	6/11/2015
☑	3800 IOS Upgrade NCM Template	goodzhere	10/2/2014
□	3800 IOS Upgrade using Alternate SCP/SFTP/TFTP server	goodzhere	6/11/2015

4. Enter your user name and password, and click Log In.



THWACK LOG IN DIALOG

All community generated content on thwack is the sole responsibility of its originator. SolarWinds does not prescreen or review community generated content. However, we will remove any content that we decide is inappropriate. Use the number of content downloads, and the comments and reputation of the content's creator as ways to gauge the reliability of information.

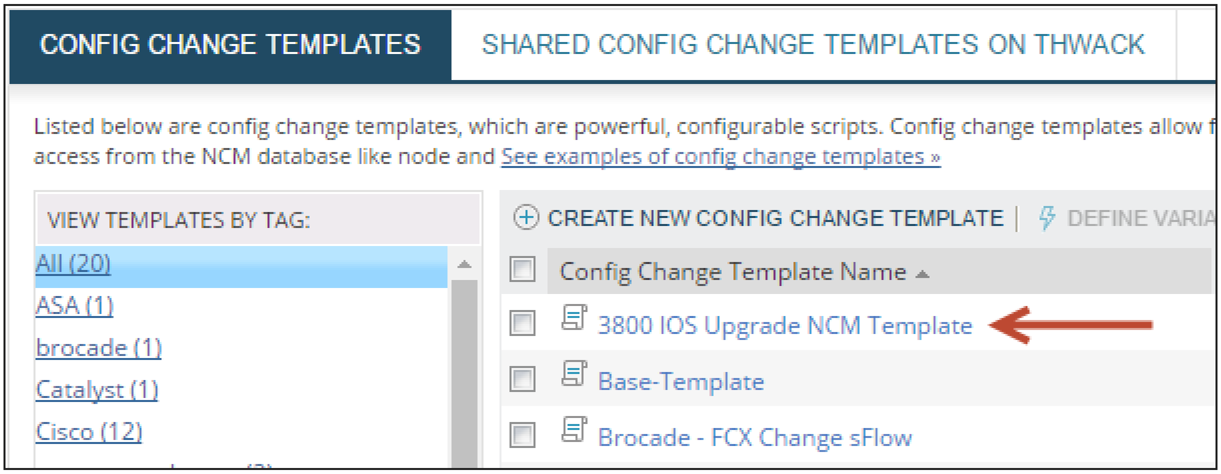
User Name: nneal

Password: ••••••••••••

LOG IN CANCEL

NCM imports the template and displays it in the list of config change templates. You can now execute the template against one or more nodes.

> SolarWinds recommends running a template on one device to test your changes and, when you verify your changes are successful, then apply the template to multiple devices.



Listed below are config change templates, which are powerful, configurable scripts. Config change templates allow f access from the NCM database like node and See examples of config change templates »

CONFIG CHANGE TEMPLATES
SHARED CONFIG CHANGE TEMPLATES ON THWACK
VIEW TEMPLATES BY TAG:
All (20)
ASA (1)
brocade (1)
Catalyst (1)
Cisco (12)
CREATE NEW CONFIG CHANGE TEMPLATE
DEFINE VARIA
Config Change Template Name
3800 IOS Upgrade NCM Template
Base-Template
Brocade - FCX Change sFlow

Network troubleshooting and remediation

This section includes the following topics:

- Troubleshoot a network issue caused by a network config change
- How was it done? Troubleshoot a network issue caused by a network config change

Troubleshoot a network issue caused by a network config change

Changes to configs can range from simple (using a template to create a login banner) to complex (using a script to change VLAN membership). Errors introduced in complex config changes can result in a network outage. By monitoring your network, you can learn about network problems before they affect your business critical applications. Instant notification of an error is essential to resolving a problem before business is disrupted and support calls are logged.

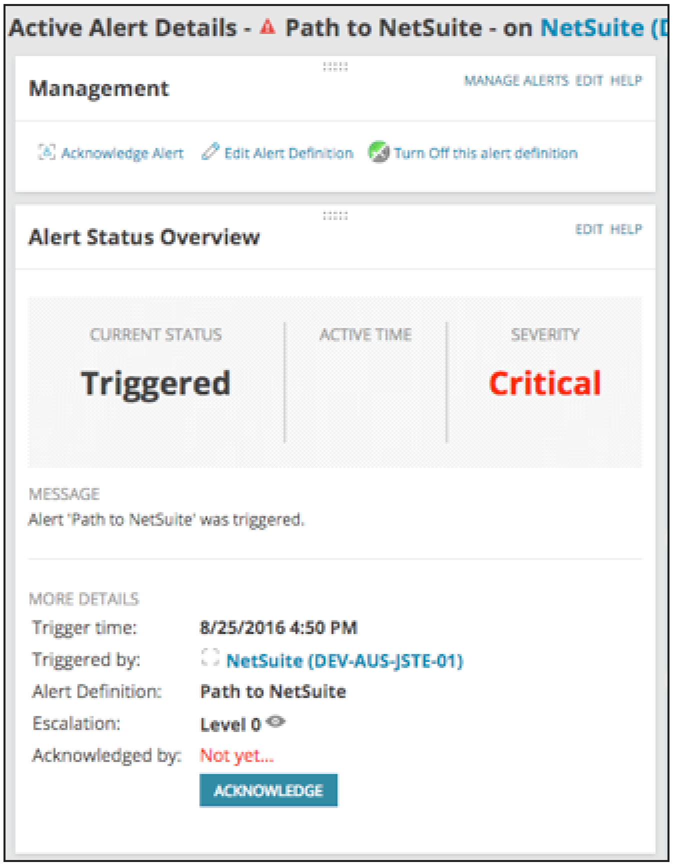
In the following scenario, a support organization uses NetSuite® as their customer relationship management system. The organization uses NetPath to monitor the path from the NetSuite service to the support organization. One day during business hours, a system administrator receives an alert notification email that the NetSuite service is unavailable and needs to investigate and resolve the problem immediately.

The system administrator begins by reviewing the details of the alert.

Review the Active Alert Details page

An alert is a notification that indicates a problem with a monitored element. There are different options for how to receive an alert. See How alerts work in NPM for more information on alerts in Orion Platform products.

In an alert notification email, click the provided link to open the Active Alert Details page. This alert is critical and needs to be addressed immediately. The system administrator clicks the link next to Triggered by to open NetPath and find if the problem is on an internal monitored device or caused by an external provider.



Active Alert Details - ⚠ Path to NetSuite - on NetSuite (D

Management

Alert Status Overview

CURRENT STATUS	ACTIVE TIME	SEVERITY
Triggered		Critical

MESSAGE
Alert 'Path to NetSuite' was triggered.

MORE DETAILS

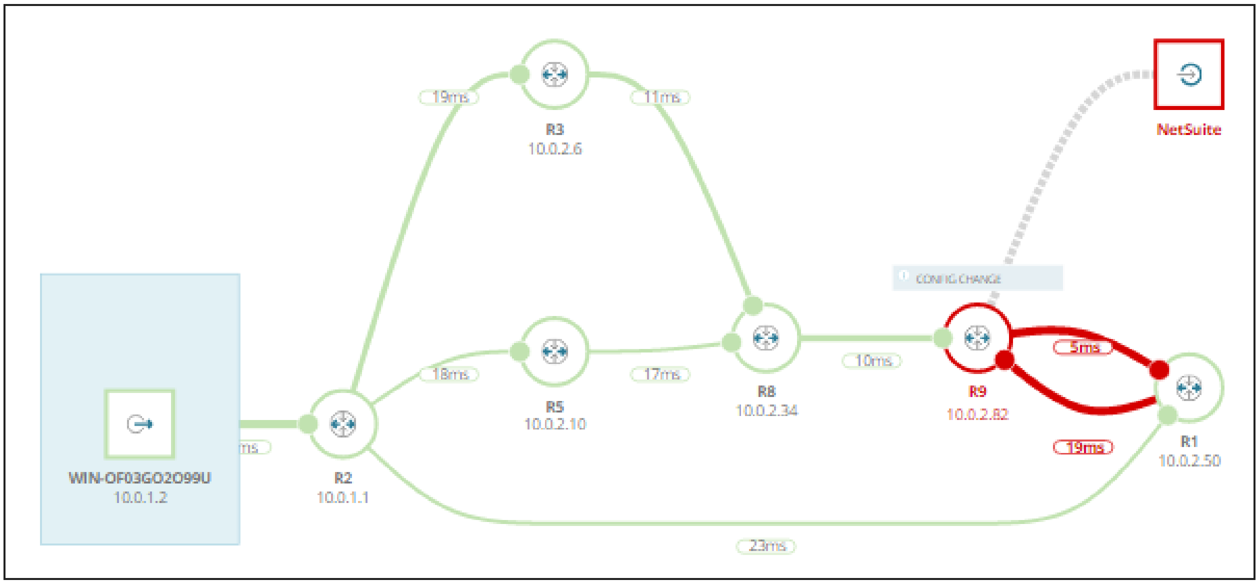
Trigger time:	8/25/2016 4:50 PM
Triggered by:	NetSuite (DEV-AUS-JSTE-01)
Alert Definition:	Path to NetSuite
Escalation:	Level 0
Acknowledged by:	Not yet...

Identify root cause of the problem

Check out this video on using NetPath

Use NetPath to discover and troubleshoot network paths, hop-by-hop, of the networks that you manage and the nodes and links of your providers. NetPath provides performance metrics and device details of the nodes, interfaces, and connectors it finds. Point to objects to see more details using the Object Inspector, or drill down on managed nodes.

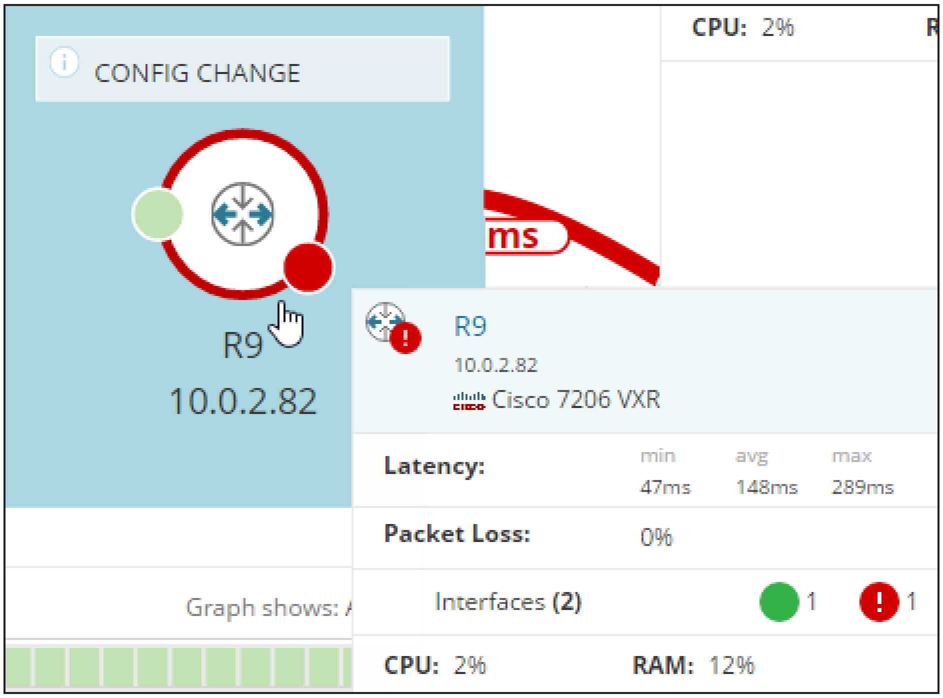
The color red indicates where on the path there is a problem.



The system administrator notices the node is:

- Part of the organization's internal network
- Experiencing high latency
- Showing a recent configuration change

To explore the configuration change, the system administrator clicks Config Change. The system compares the current config to last backed up config.



CPU: 2%

R9
10.0.2.82
Cisco 7206 VXR

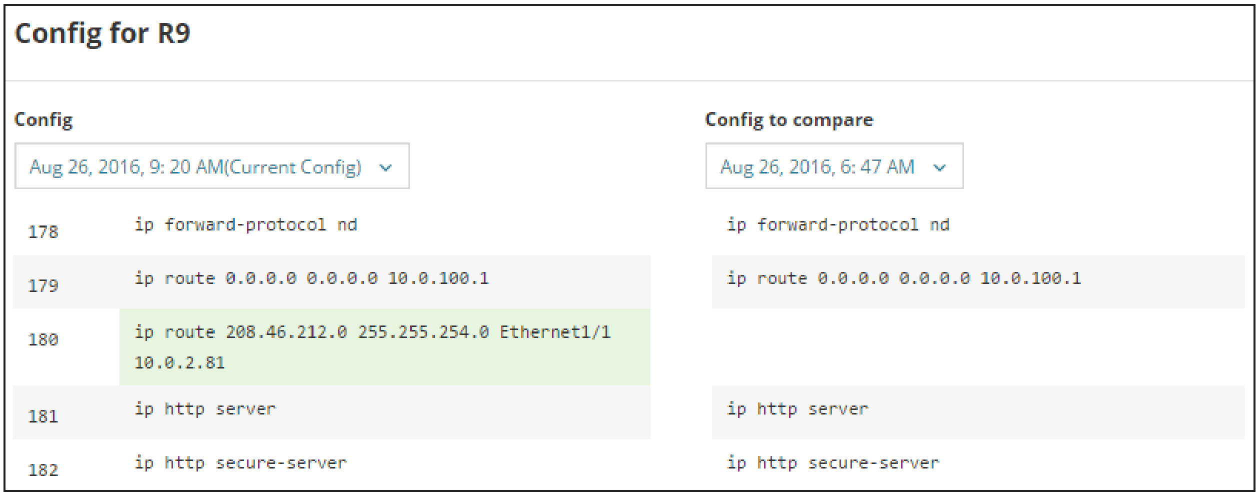
	min	avg	max
Latency:	47ms	148ms	289ms

Packet Loss: 0%

Interfaces (2) ● 1 ! 1

CPU: 2% RAM: 12%

The config comparison shows that in line 180, an IP address is added to the current config. This routing change prevents traffic from accessing its destination and creates network performance issues.



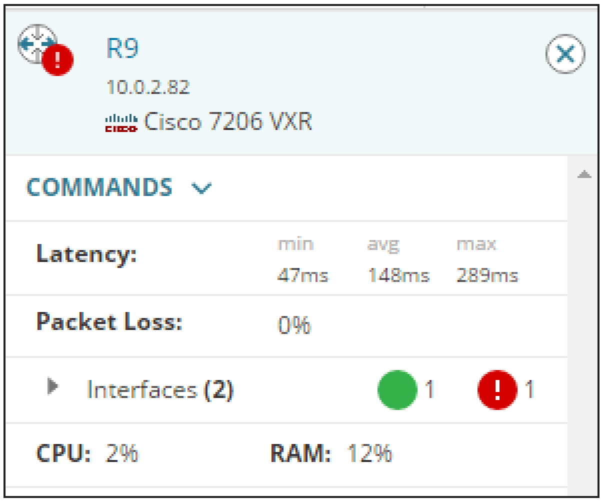
Config for R9

Config: Aug 26, 2016, 9: 20 AM(Current Config)	Config to compare: Aug 26, 2016, 6: 47 AM
`ip forward-protocol nd`	`ip forward-protocol nd`
`ip route 0.0.0.0 0.0.0.0 10.0.100.1`	`ip route 0.0.0.0 0.0.0.0 10.0.100.1`
`ip route 208.46.212.0 255.255.254.0 Ethernet1/1 10.0.2.81`	
`ip http server`	`ip http server`
`ip http secure-server`	`ip http secure-server`

The system administrator identified the root cause of the problem and knows that one solution is to revert to the last backed up config.

Revert a config

The system administrator clicks the name of the node (in this case, R9) on the right side of the NetPath page to open the Node Details page. This capability is also useful if someone makes an unauthorized or incorrect config change, and you want to revert to a prior version.



R9
10.0.2.82
Cisco 7206 VXR

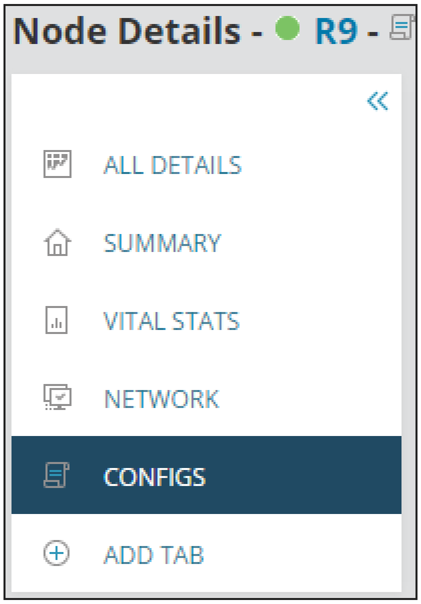
	min	avg	max
Latency:	47ms	148ms	289ms
Packet Loss:	0%		

Interfaces (2) ● 1 ❗ 1

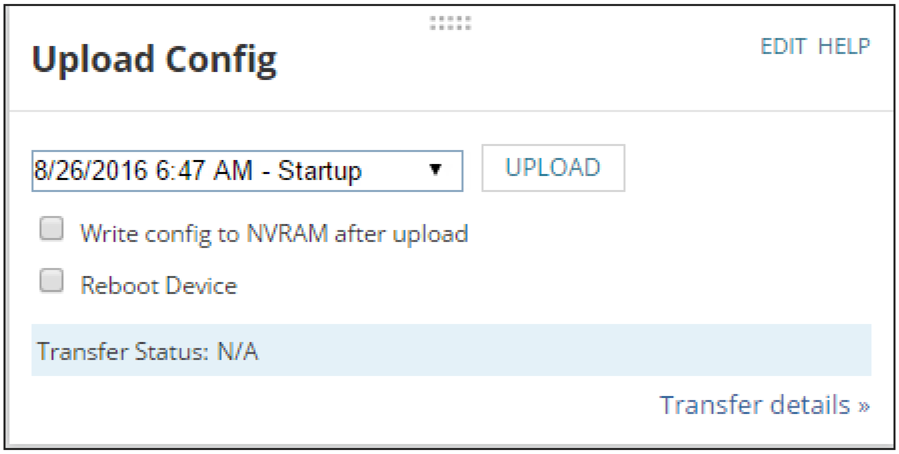
CPU: 2% **RAM:** 12%

There are two steps the system administrator needs to perform to revert the config:

1. Click the Configs tab.



2. Select the configuration item to revert back to and then click Upload.



Upload Config

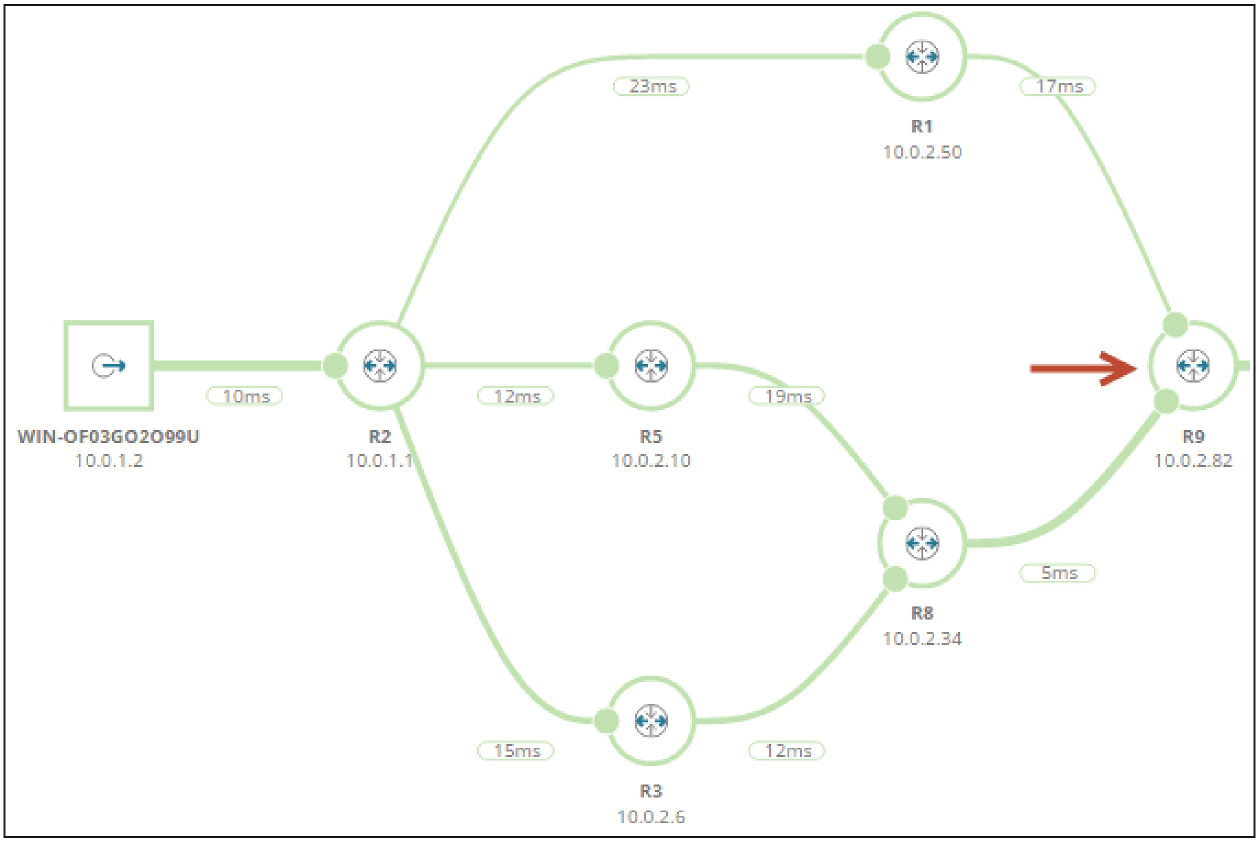
8/26/2016 6:47 AM - Startup

□ Write config to NVRAM after upload

□ Reboot Device

Transfer Status: N/A

NetPath refreshes a path during each polling interval. In this example, the polling interval is 10 minutes. The change to revert the node is made immediately and the service is restored, but NetPath does not show the updated path until the next polling interval completes.



Learn more

For more information on the setup necessary to replicate the troubleshooting and solution steps in this topic, see How was it done? Troubleshoot a network issue caused by a config change.

How was it done? Troubleshoot a network issue caused by a network config change

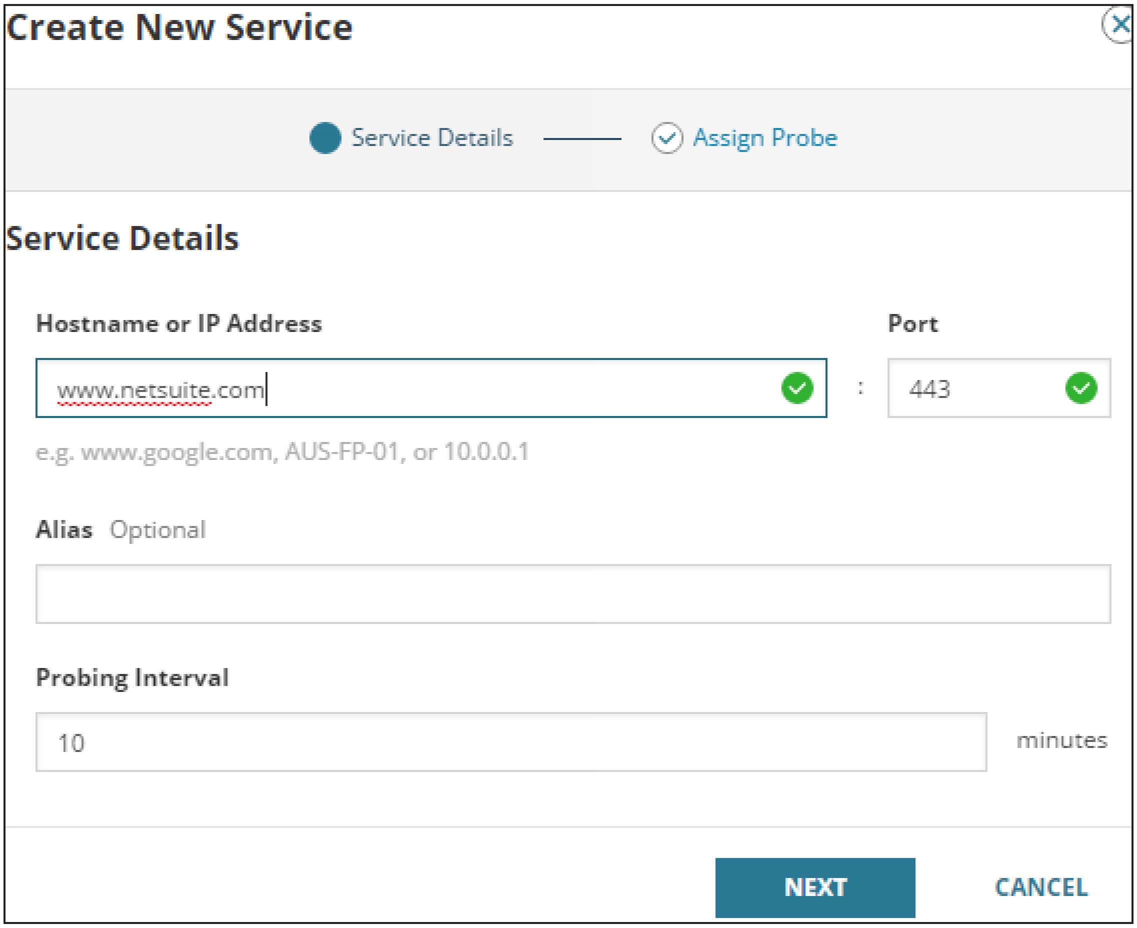
In the Troubleshoot a network issue caused by a network config change topic, a system administrator finds the root cause of a network problem and reverts a config to resolve the alert. This topic explains the setup necessary to replicate the troubleshooting and solution steps performed by the system administrator.

Create a path to NetSuite

Before you can monitor, you must first create a new service path. This example creates a path to NetSuite.

1. Navigate to My Dashboards > Network > NetPath Services.
2. Click Create New Service.

3. Enter the Service Details and click Next.



Create New Service

Service Details

Hostname or IP Address: www.netsuite.com

Port: 443

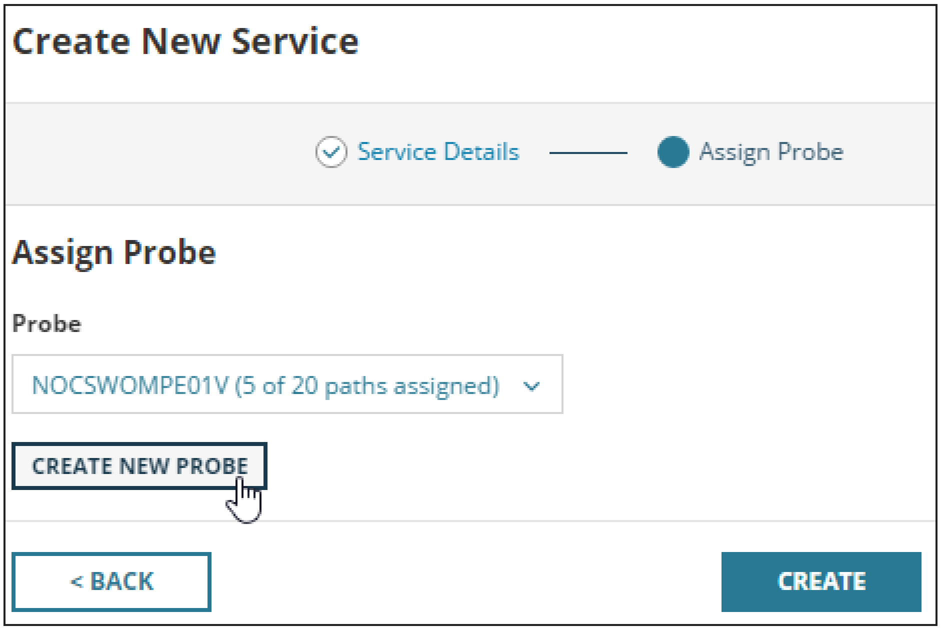
e.g. www.google.com, AUS-FP-01, or 10.0.0.1

Alias Optional

Probing Interval: 10 minutes

4. Assign a probe or create a probe.

5. Click Create.


Create New Service

Service Details — Assign Probe

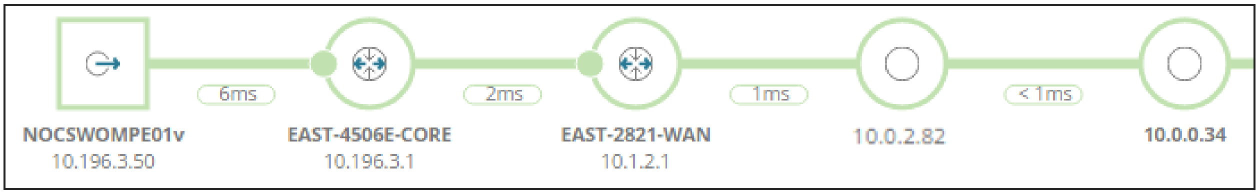
Assign Probe

Probe

NOCSWOMPE01V (5 of 20 paths assigned)

After the first polling interval, the network path from the probe to the NetSuite service is active. The system administrator knows that all nodes beginning with the number 10 are internal nodes.

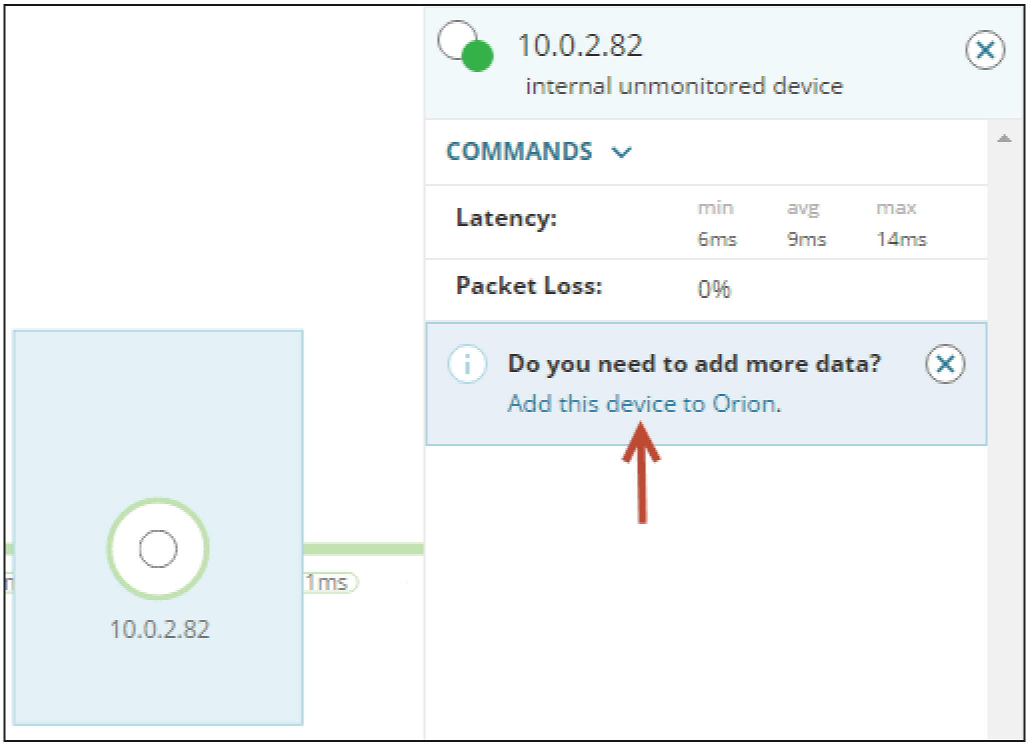
- If you are already monitoring internal nodes on the path, you see data about the nodes. In this example, nodes EAST-4506E-CORE and EAST-2821-WAN are monitored.
- If you are not monitoring internal nodes on the path, you can add them. See the Monitor nodes on a path section below. In this example, the system is not monitoring node 10.0.2.82.



Monitor nodes on a path

Before you begin, ensure that you know the credentials for the nodes you want to monitor.

1. Click any node on the path that you want to monitor.
2. Click Add this device to Orion.



10.0.2.82
internal unmonitored device

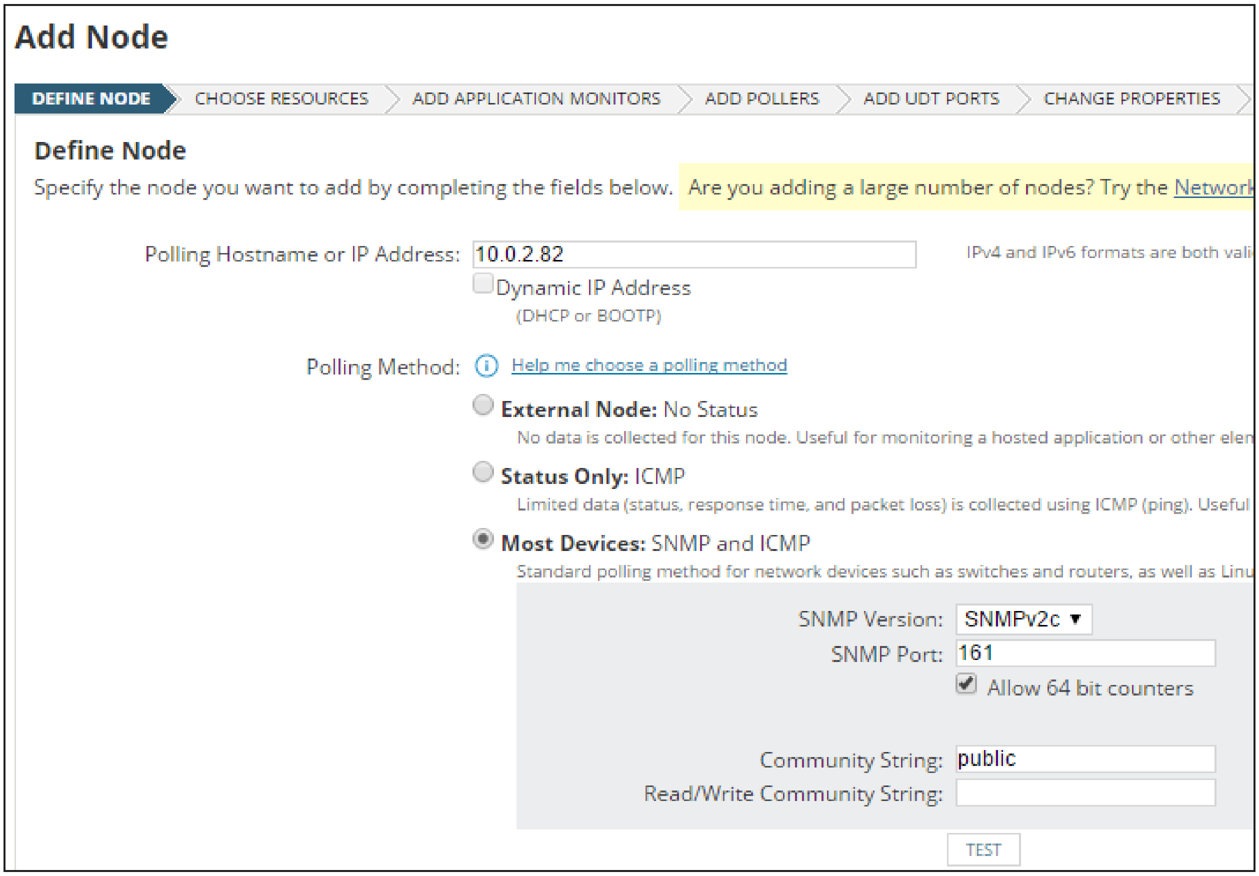
COMMANDS

	min	avg	max
Latency:	6ms	9ms	14ms
Packet Loss:	0%		

Do you need to add more data?
Add this device to Orion.

3. Enter the node credentials.

   To learn how to complete the remaining steps for adding a node, see Add a single node for monitoring to the Orion Platform.



Add Node

Define Node

Specify the node you want to add by completing the fields below. Are you adding a large number of nodes? Try the Network

Polling Hostname or IP Address: 10.0.2.82 IPv4 and IPv6 formats are both vali

□ Dynamic IP Address (DHCP or BOOTP)

Polling Method: Help me choose a polling method

○ **External Node:** No Status
No data is collected for this node. Useful for monitoring a hosted application or other elen

○ **Status Only:** ICMP
Limited data (status, response time, and packet loss) is collected using ICMP (ping). Useful

● **Most Devices:** SNMP and ICMP
Standard polling method for network devices such as switches and routers, as well as Linu

SNMP Version: SNMPv2c

SNMP Port: 161

☑ Allow 64 bit counters

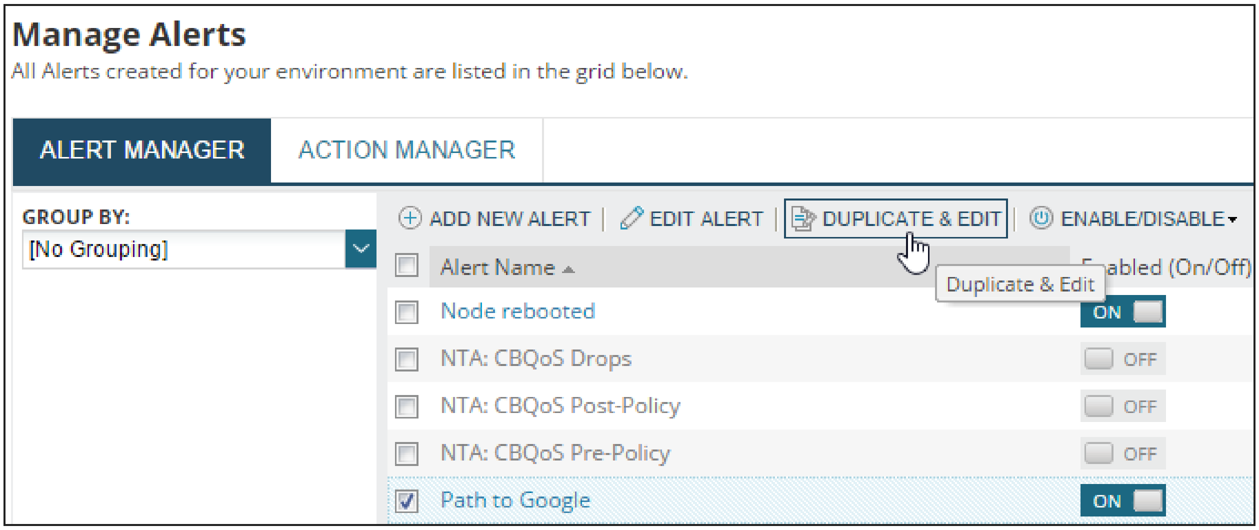
Community String: public

Read/Write Community String:

Create a NetPath alert for NetSuite

This example shows how to duplicate and edit the out-of-the-box alert Path to Google to create an alert for the new path to NetSuite. When the path to Netsuite breaks, an alert is triggered.

1. Navigate to the Manage Alert page.



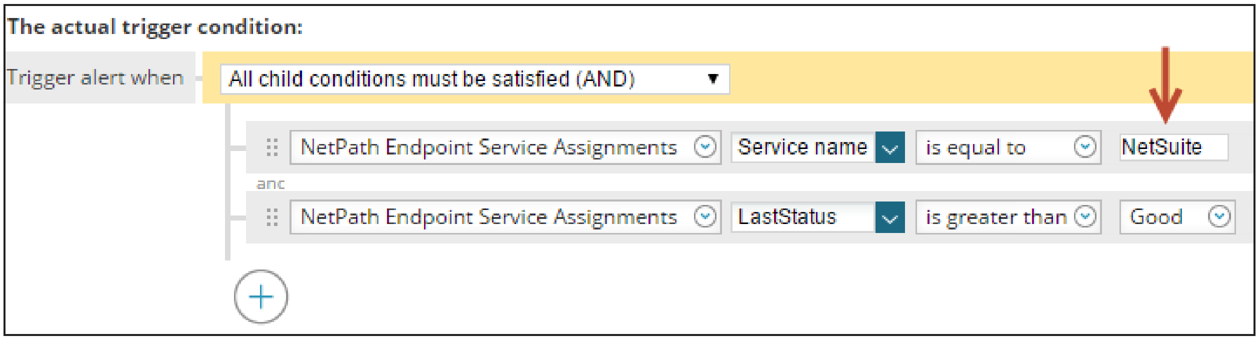
Manage Alerts

All Alerts created for your environment are listed in the grid below.

	Alert Name ▲	Enabled (On/Off)
□	Node rebooted	ON
□	NTA: CBQoS Drops	OFF
□	NTA: CBQoS Post-Policy	OFF
□	NTA: CBQoS Pre-Policy	OFF
☑	Path to Google	ON

2. On the Properties page, update the name and description of the alert. For example, you can enter `Path to NetSuite` for the name.

3. On the Trigger Condition page, change Google to NetSuite.



The actual trigger condition:

Trigger alert when All child conditions must be satisfied (AND)

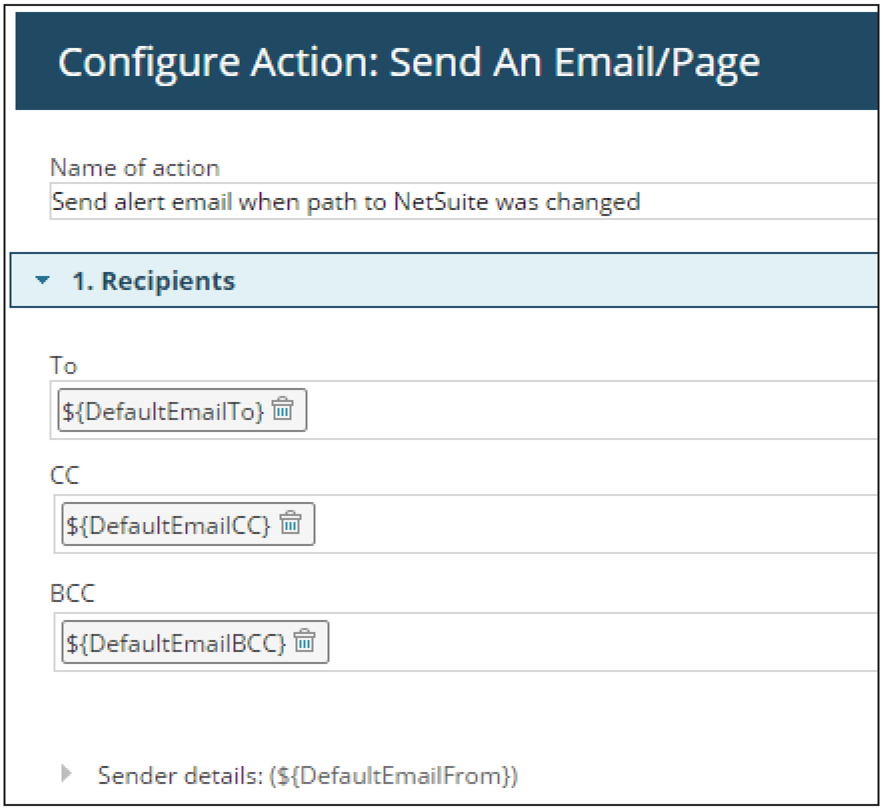
NetPath Endpoint Service Assignments | Service name | is equal to | NetSuite

and

NetPath Endpoint Service Assignments | LastStatus | is greater than | Good

4. Click Next until you reach the Trigger Action page.

5. Edit the email action so you (or other responsible party) receive a notification email when the alert is triggered.



Configure Action: Send An Email/Page

Name of action
Send alert email when path to NetSuite was changed

1. Recipients

To
${DefaultEmailTo}

CC
${DefaultEmailCC}

BCC
${DefaultEmailBCC}

Sender details: (${DefaultEmailFrom})

6. Complete the rest of the alert wizard steps, and then click Submit on the Summary page.

You can review possible errors made to configs before an alert is sent. Enable real-time change detection and receive an email notification whenever there is a change to a config. Real-time change detection also has an option to restrict access to users so you can prevent unauthorized changes to configs.

Configure real-time change detection: an example

The Troubleshoot a network issue caused by a network config change section provides an example scenario of a system administrator resolving an alert caused by a config change. If the system administrator had enabled real-time change detection (RTCD), the config change could have been viewed and resolved before the alert was sent. Real-time change detection provides instant notification through email whenever a change occurs to any of your device configurations.

The notification provides log information you can use to quickly determine if a configuration change is the cause of a network problem. This access to real-time visibility of your network helps you improve your network security, prevent unexpected downtime or delays, and resolve known errors faster.

ⓘ Unlike the Config Change Report, changes are detected only on the same configuration type. For example, if you download a startup configuration, make changes, and then upload it as a running configuration, the changes are compared against the previous running configuration. A comparison is not made between running and startup configuration types.

The following sections walk you through an example of setting up real-time change detection. This example provides configuration steps for:

- Cisco IOS devices
- Orion Log Viewer (OLV) as the syslog server

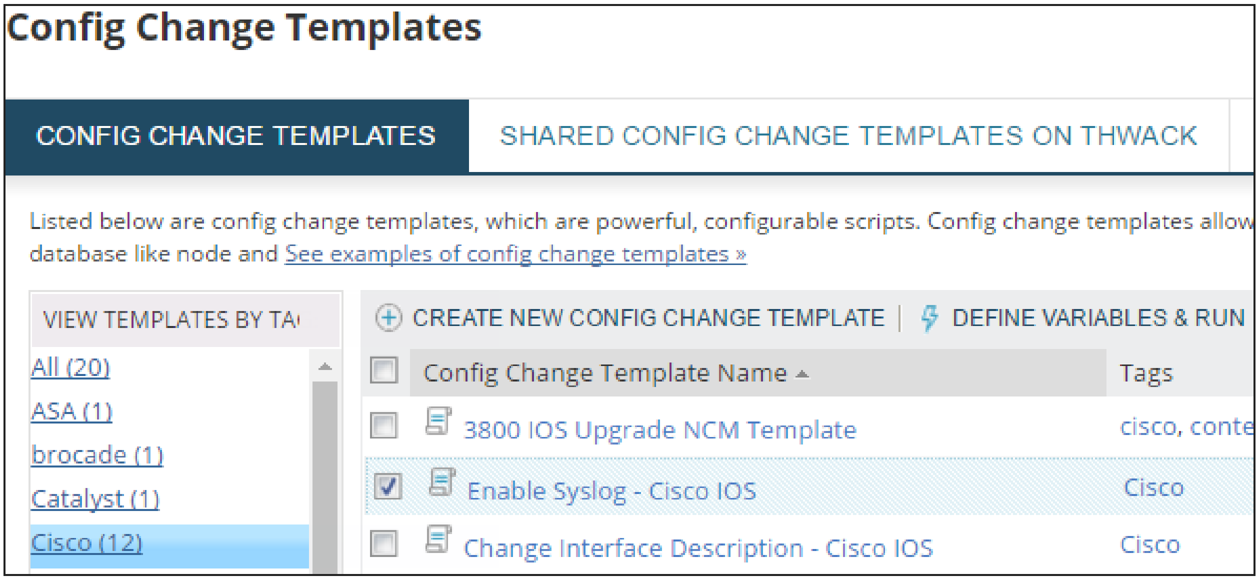
For information about setting up real-time change detection with **other** syslog servers or device types, see the NCM Administrator Guide topic Configure real-time change detection in NCM.

Task 1: Configure a Cisco device to send syslog messages

The following example shows how to use a config change template to enable Cisco IOS devices to send syslog messages to the Orion server.

For the purposes of RTCD, SolarWinds recommends configuring Cisco devices to send syslog messages, **not** trap messages. Cisco devices send trap messages when a user enters config mode, but not when the user exits. RTCD requires that a message be sent when the user exits config mode.

1. Click My Dashboards > Network Configuration > Config Change Templates.
2. Select Enable Syslog - Cisco IOS, and click Define Variables & Run.



Config Change Templates

CONFIG CHANGE TEMPLATES | SHARED CONFIG CHANGE TEMPLATES ON THWACK

Listed below are config change templates, which are powerful, configurable scripts. Config change templates allow
database like node and See examples of config change templates »

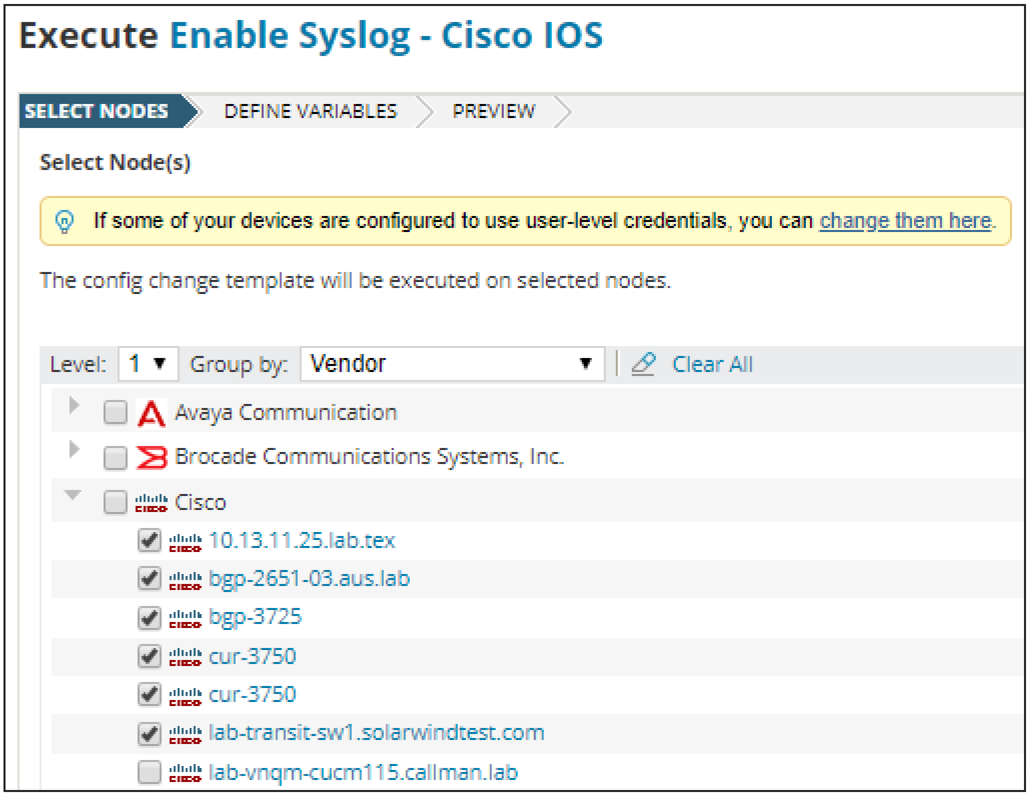
VIEW TEMPLATES BY TA

- All (20)
- ASA (1)
- brocade (1)
- Catalyst (1)
- Cisco (12)

CREATE NEW CONFIG CHANGE TEMPLATE | DEFINE VARIABLES & RUN

☐	Config Change Template Name ▲	Tags
☐	3800 IOS Upgrade NCM Template	cisco, conte
☑	Enable Syslog - Cisco IOS	Cisco
☐	Change Interface Description - Cisco IOS	Cisco

3. Select the device on which you want to enable syslog, and click Next.



Execute Enable Syslog - Cisco IOS

SELECT NODES > DEFINE VARIABLES > PREVIEW

Select Node(s)

If some of your devices are configured to use user-level credentials, you can change them here.

The config change template will be executed on selected nodes.

Level: 1 ▼ Group by: Vendor ▼ | Clear All

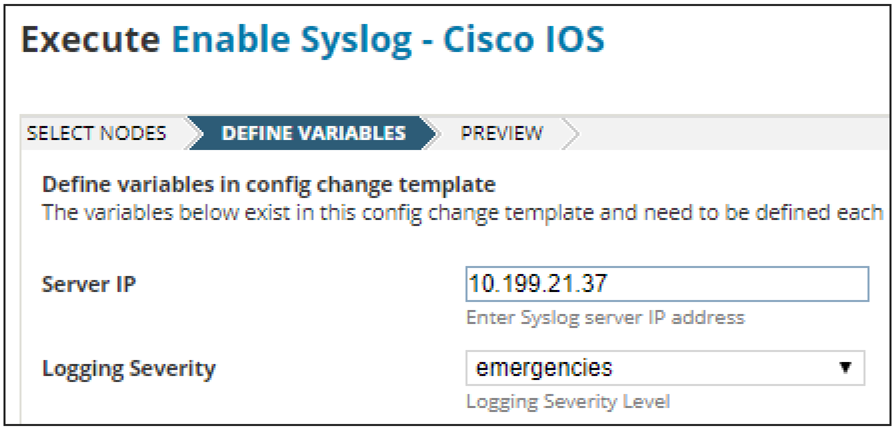
- ☐ Avaya Communication
- ☐ Brocade Communications Systems, Inc.
- ☐ Cisco
  - ☑ 10.13.11.25.lab.tex
  - ☑ bgp-2651-03.aus.lab
  - ☑ bgp-3725
  - ☑ cur-3750
  - ☑ cur-3750
  - ☑ lab-transit-sw1.solarwindtest.com
  - ☐ lab-vnqm-cucm115.callman.lab

10.

4. Enter the IP address of the Orion server, and select a Severity level.

   You can choose any logging severity value.

5. Click Next.



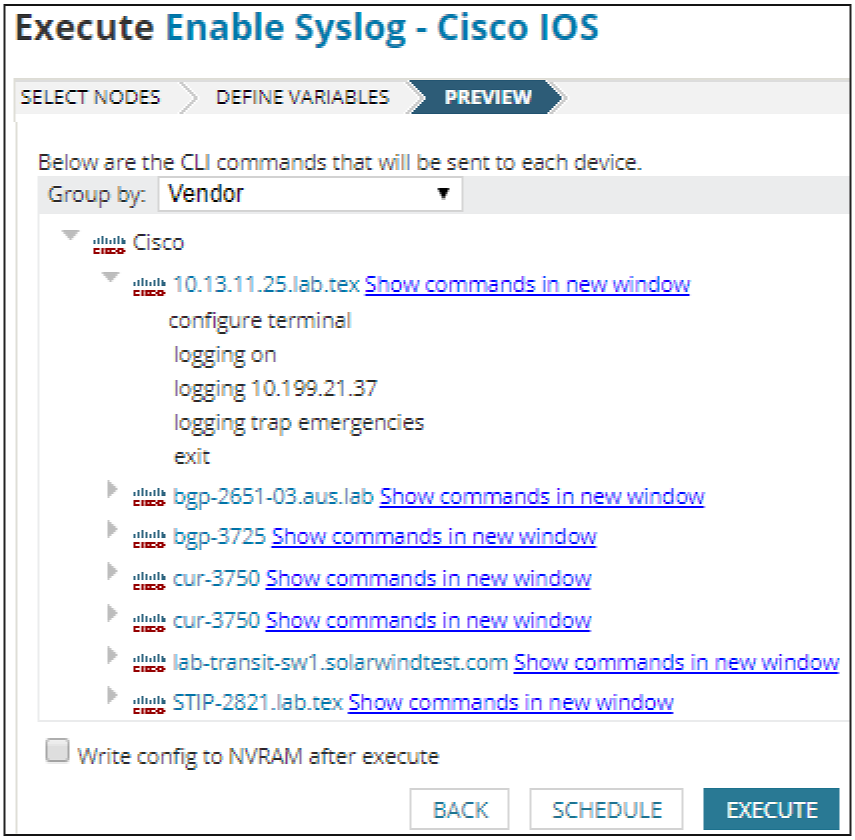
Execute Enable Syslog - Cisco IOS

Define variables in config change template
The variables below exist in this config change template and need to be defined each

Server IP: 10.199.21.37
Enter Syslog server IP address

Logging Severity: emergencies
Logging Severity Level

6. After the system generates the script, you can expand any node to examine the commands. Then click Execute.



Execute Enable Syslog - Cisco IOS

Below are the CLI commands that will be sent to each device.
Group by: Vendor

Cisco
10.13.11.25.lab.tex Show commands in new window

```
configure terminal
 logging on
 logging 10.199.21.37
 logging trap emergencies
 exit
```

bgp-2651-03.aus.lab Show commands in new window
bgp-3725 Show commands in new window
cur-3750 Show commands in new window
cur-3750 Show commands in new window
lab-transit-sw1.solarwindtest.com Show commands in new window
STIP-2821.lab.tex Show commands in new window

□ Write config to NVRAM after execute

Task 2: Enable the RTCD rule in the Orion Log Viewer

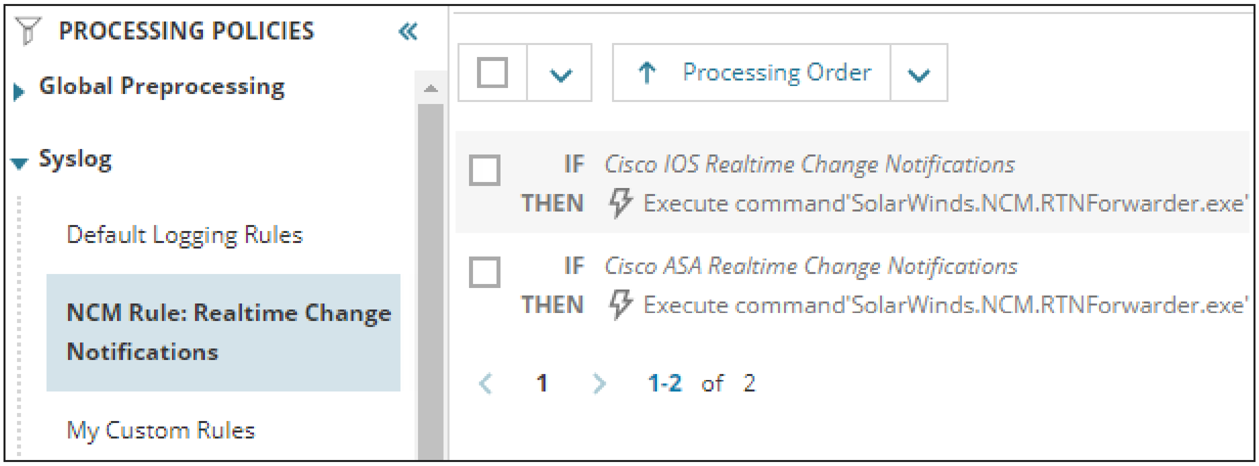
In this example, Orion Log Viewer (OLV) is used to listen for syslog messages. OLV includes default rules for Cisco ASA and Cisco IOS devices. When OLV receives a syslog message indicating that a config on a Cisco ASA or Cisco IOS device has changed, the rule runs a program to compare the device's current config with the previously backed-up config. Then it sends an email to notify you of the changes so that you can quickly identify unauthorized changes or misconfigurations.

By default, these rules are not enabled. Complete the following steps to enable them.

> ⓘ If you are using a different syslog server, or you need to configure rules for other device types, see Configure real-time change detection in NCM.

1. In the Orion Web Console, click My Dashboard > Logs > Log Viewer.
2. In the upper-right corner, click Configure Rules.
3. Under Processing Policies, expand Syslog. Then click NCM Rule: Realtime Change Notifications.

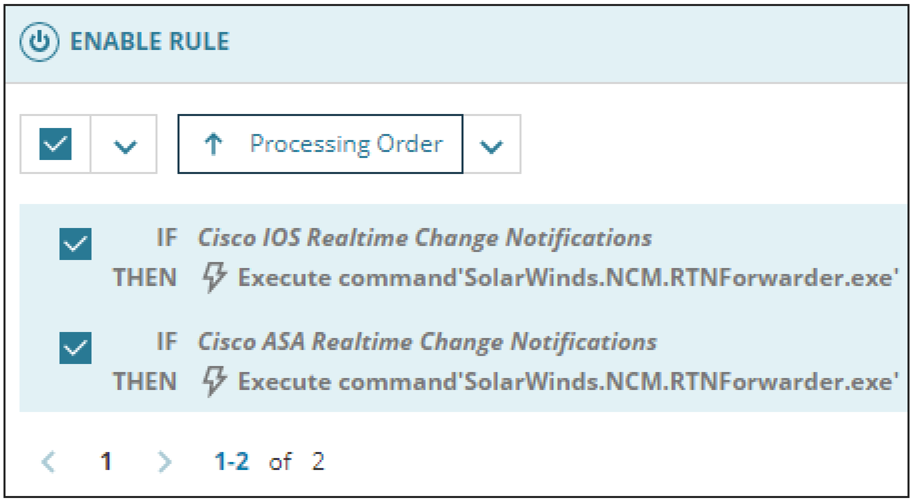
   Descriptions of the default RTCD rules are displayed.



□ IF *Cisco IOS Realtime Change Notifications*
THEN Execute command'SolarWinds.NCM.RTNForwarder.exe'

□ IF *Cisco ASA Realtime Change Notifications*
THEN Execute command'SolarWinds.NCM.RTNForwarder.exe'

4. To take action when configs are changed on Cisco IOS devices such as the Tex-3750.aus.lab router, select the Cisco IOS Realtime Change Notifications rule. Optionally, you can also select the Cisco ASA Realtime Change Notifications rule.



ENABLE RULE

☑ Processing Order

☑ IF *Cisco IOS Realtime Change Notifications*
THEN Execute command'SolarWinds.NCM.RTNForwarder.exe'

☑ IF *Cisco ASA Realtime Change Notifications*
THEN Execute command'SolarWinds.NCM.RTNForwarder.exe'

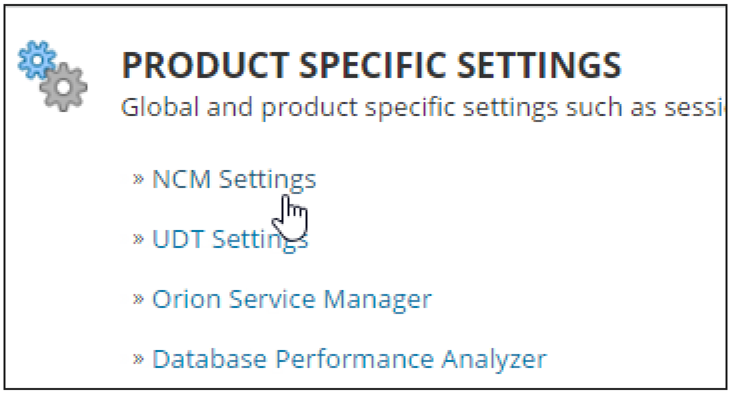
1 1-2 of 2

5. Click Enable Rule.

Task 3: Configure NCM for real-time change detection

After you configure a Cisco device to send syslog messages and enable the rule that is triggered when a config changes, configure SolarWinds NCM for real-time change detection.

1. Click Settings > All Settings.
2. Under Product Specific Settings, click NCM Settings.



PRODUCT SPECIFIC SETTINGS

Global and product specific settings such as sessi

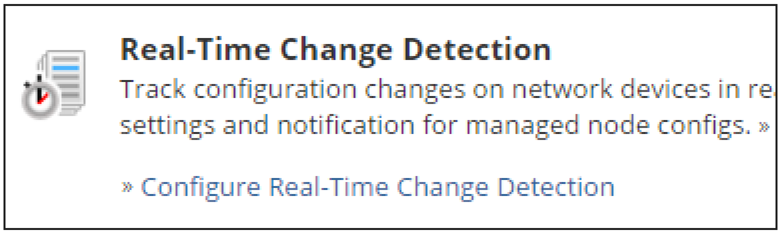
» NCM Settings

» UDT Settings

» Orion Service Manager

» Database Performance Analyzer

3. Under Real-Time Change Detection, click Configure Real-Time Change Detection.

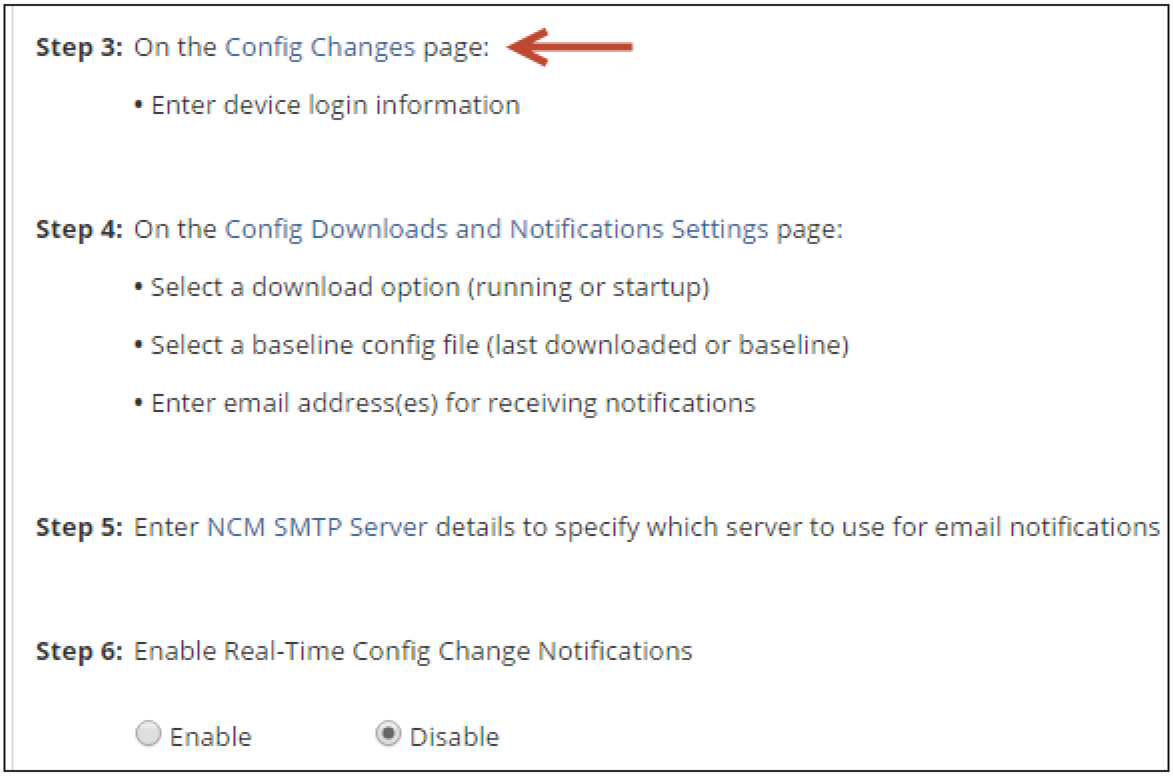


Real-Time Change Detection

Track configuration changes on network devices in re settings and notification for managed node configs. »

» Configure Real-Time Change Detection

The real-time change detection page lists the required steps to configure real-time change detection. We have already completed the first two steps, so you can begin at step 3.



Step 3: On the Config Changes page:

- Enter device login information

Step 4: On the Config Downloads and Notifications Settings page:

- Select a download option (running or startup)
- Select a baseline config file (last downloaded or baseline)
- Enter email address(es) for receiving notifications

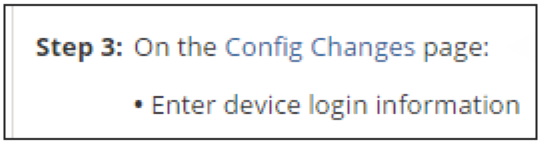
Step 5: Enter NCM SMTP Server details to specify which server to use for email notifications

Step 6: Enable Real-Time Config Change Notifications

○ Enable ● Disable

4. Enter the log in credentials that syslog will use to access devices:

    a. Click Config Changes.

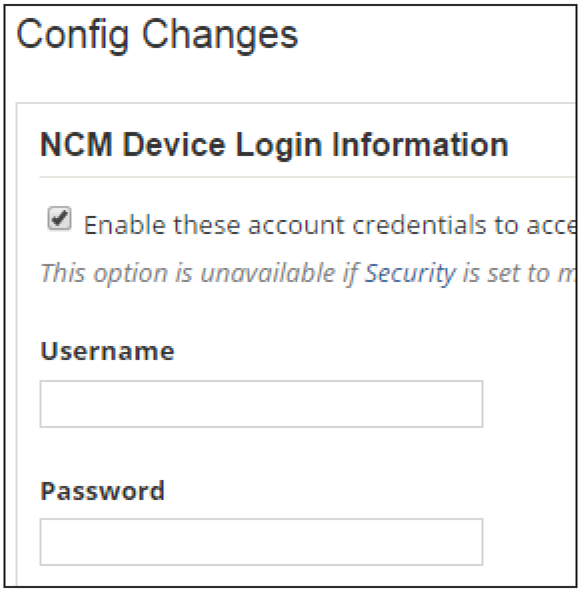


Step 3: On the Config Changes page:

- Enter device login information

    b. On the Config Change page, select Enable these account credentials.

c. Enter the account credentials for the devices on which you want to receive real-time change detection emails.



Config Changes

NCM Device Login Information

☑ Enable these account credentials to acce

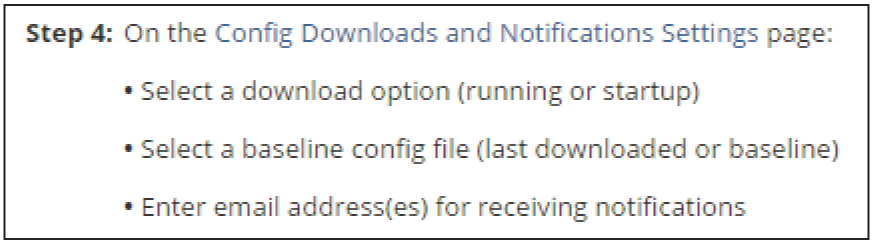
This option is unavailable if Security is set to m

Username

Password

5. Use the Config Download and Notifications page to select the config type to monitor for change, and specify who gets notified when a change is made:

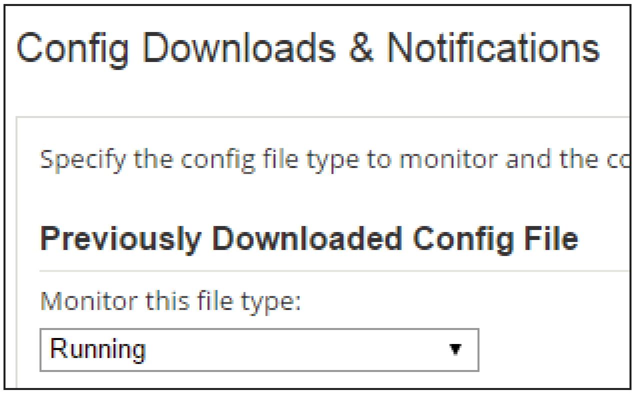
    a. On the Real-Time Change Detection page, click Config Downloads and Notifications Settings.

    Step 4: On the Config Downloads and Notifications Settings page:

    - Select a download option (running or startup)
    - Select a baseline config file (last downloaded or baseline)
    - Enter email address(es) for receiving notifications

    b. In the Monitor this file type field, select Running or Startup.

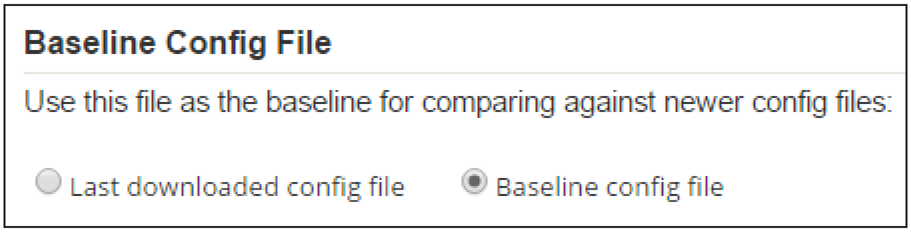
    Config Downloads & Notifications

    Specify the config file type to monitor and the co

    Previously Downloaded Config File

    Monitor this file type: Running ▼

    c. Under Baseline Config File, select whether you want to compare the changed config against the latest downloaded config or the baseline config.



Baseline Config File

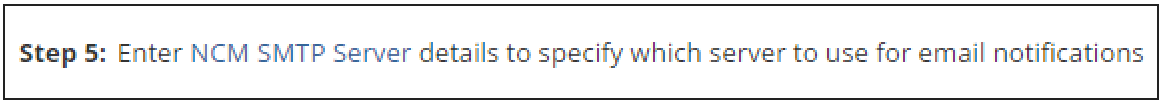
Use this file as the baseline for comparing against newer config files:

○ Last downloaded config file ● Baseline config file

d. Select email notification options, and click Submit.

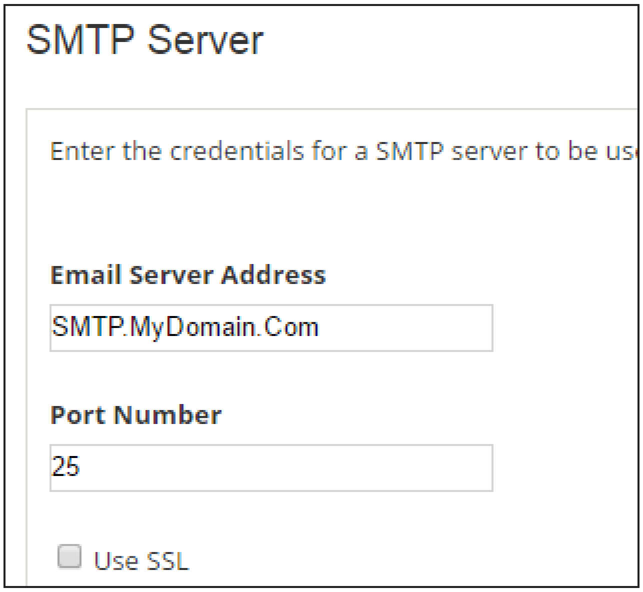
6. Use the SMTP Server page to enter the credentials for an SMTP server used for config change approvals, real-time change detection, and running jobs:

   a. On the Real-Time Change Detection page, click NCM SMTP Server.



Step 5: Enter NCM SMTP Server details to specify which server to use for email notifications

   b. Enter the email server address and credentials, and click Submit.



SMTP Server

Enter the credentials for a SMTP server to be us

Email Server Address

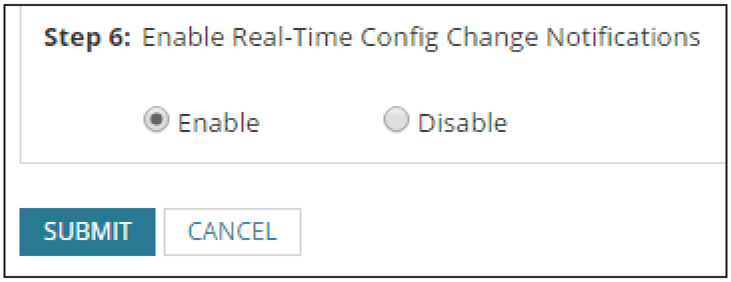
SMTP.MyDomain.Com

Port Number

25

□ Use SSL

7. On the Real-Time Change Detection page, click Enable and then click Submit.



Step 6: Enable Real-Time Config Change Notifications

● Enable ○ Disable

Reporting in NCM

This section includes the following topics:

Uses of NCM inventory reports

Use NCM inventory reports to access up-to-date device information and to manage the inventory of your network infrastructure. NCM automatically updates your device information when you import a device. Select and run an inventory report to collect specific information for devices. For example, you can run an inventory scan of all IP addresses inventoried on each device. A searchable list of IP addresses is valuable when trying to locate an address in a large network. You can also set regular inventory scans to gather device information.

Examples of device information collected by network inventory reports include:

- Serial numbers
- Port details
- IP addresses
- Vendors
- End-of-life dates
- End-of-support dates
- Maintenance providers

You can choose from several unique inventory reports, or create your own.

Popular out-of-the-box inventory reports include:

- Cisco 3750 Stack - Physical Entity: displays information about Physical Entities within each device.
- Cisco Chassis IDs: displays the Chassis IDs (and serial number if available) for Cisco devices.
- Cisco IOS Image Details: shows details about the running IOS in each Cisco device.
- Cisco VLANs: displays which VLAN IDs belong to which devices.

To learn more, see:

- Run an inventory report
- Schedule a report

Run an NCM inventory report

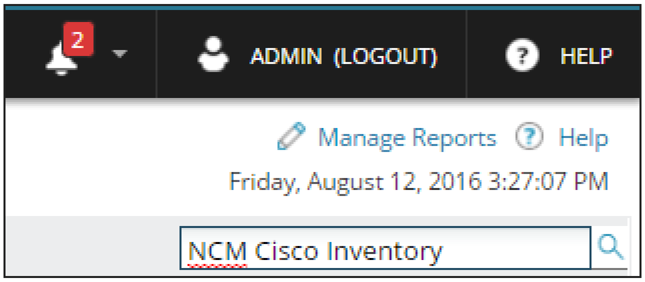
Generate a detailed report of a single node, all nodes, or groups of nodes. Inventory reports provide on-demand information for your devices, such as auditing, routing protocols, end-of-support, and much more.

The following example shows how to:

- Filter all reports in the system to include just the NCM Cisco Inventory reports.
- Run the Cisco 3750 Stack - Physical Entity report.

Complete the following steps.

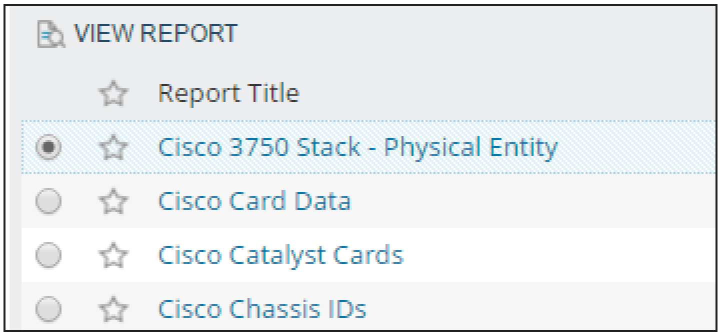
1. Click Reports > All Reports.
2. In the search field, type NCM Cisco Inventory and click Search.



Friday, August 12, 2016 3:27:07 PM

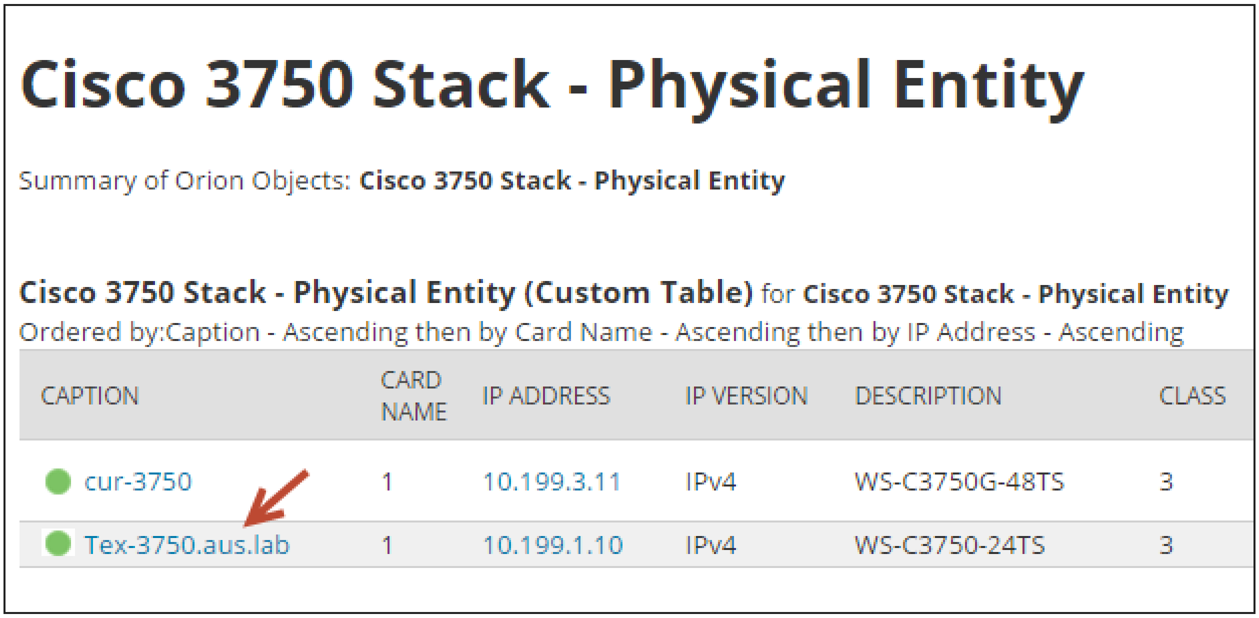
NCM Cisco Inventory

3. Select a report and click View Report.



	Report Title
●	Cisco 3750 Stack - Physical Entity
○	Cisco Card Data
○	Cisco Catalyst Cards
○	Cisco Chassis IDs

SolarWinds Orion reports are interactive. In this example, if you click the node name, the Node Details page opens.



Cisco 3750 Stack - Physical Entity

Summary of Orion Objects: **Cisco 3750 Stack - Physical Entity**

Cisco 3750 Stack - Physical Entity (Custom Table) for **Cisco 3750 Stack - Physical Entity**
Ordered by:Caption - Ascending then by Card Name - Ascending then by IP Address - Ascending

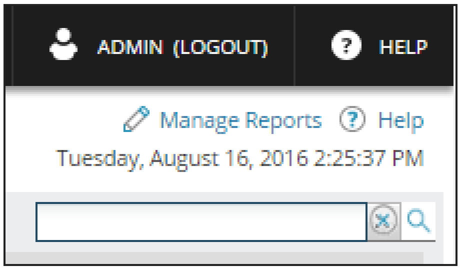
CAPTION	CARD NAME	IP ADDRESS	IP VERSION	DESCRIPTION	CLASS
● cur-3750	1	10.199.3.11	IPv4	WS-C3750G-48TS	3
● Tex-3750.aus.lab	1	10.199.1.10	IPv4	WS-C3750-24TS	3

Schedule an NCM report

Reports provide up-to-date information about your devices and help keep you informed to better manage your network. Schedule reports to save time and minimize your workload. You can choose when and how often to run a report for a device. A single report schedule can be assigned to multiple reports. You can also choose to email, print, or save the report information details.

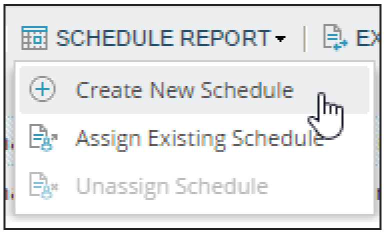
The following example schedules a weekly report for Cisco 3750 Stack - Physical Entity, Cisco Chassis IDs, and Cisco IOS Image Details. This report will run every Sunday and sends the details to all recipients by email.

1. Click Reports > All Reports.
2. Click Manage Reports.

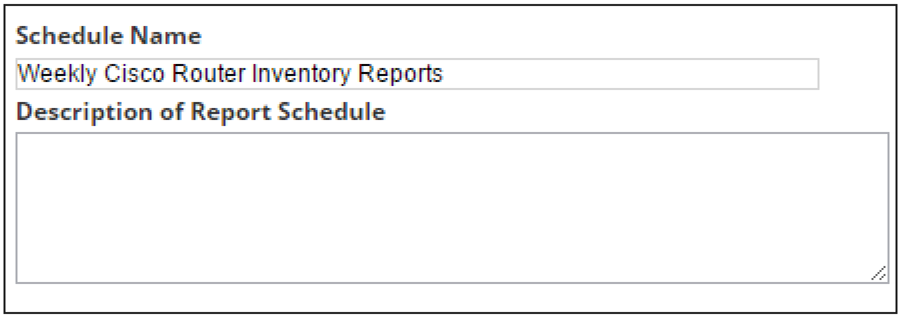


Tuesday, August 16, 2016 2:25:37 PM

3. Click Schedule Report > Create New Schedule.



4. Name your report schedule and provide a description.



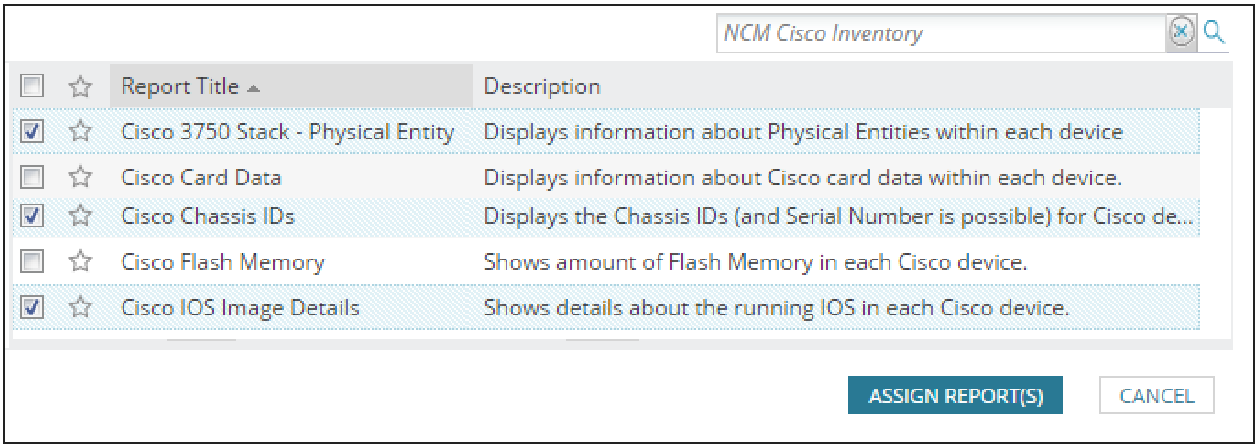
Schedule Name

Weekly Cisco Router Inventory Reports

Description of Report Schedule

5. Click Assign Report.

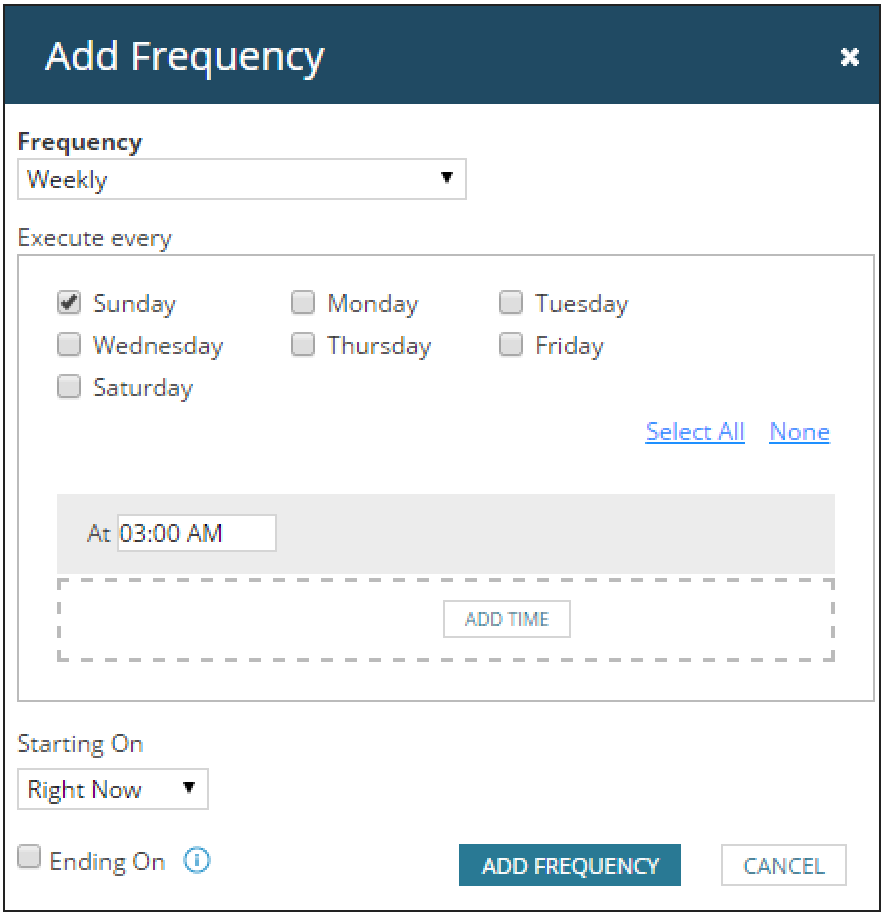
6. Search for NCM Cisco Inventory reports and select reports. This example shows three assigned reports.



NCM Cisco Inventory

□	☆	Report Title ▲	Description
☑	☆	Cisco 3750 Stack - Physical Entity	Displays information about Physical Entities within each device
□	☆	Cisco Card Data	Displays information about Cisco card data within each device.
☑	☆	Cisco Chassis IDs	Displays the Chassis IDs (and Serial Number is possible) for Cisco de...
□	☆	Cisco Flash Memory	Shows amount of Flash Memory in each Cisco device.
☑	☆	Cisco IOS Image Details	Shows details about the running IOS in each Cisco device.

7. Select the frequency to run the report.



Add Frequency

Frequency: Weekly

Execute every

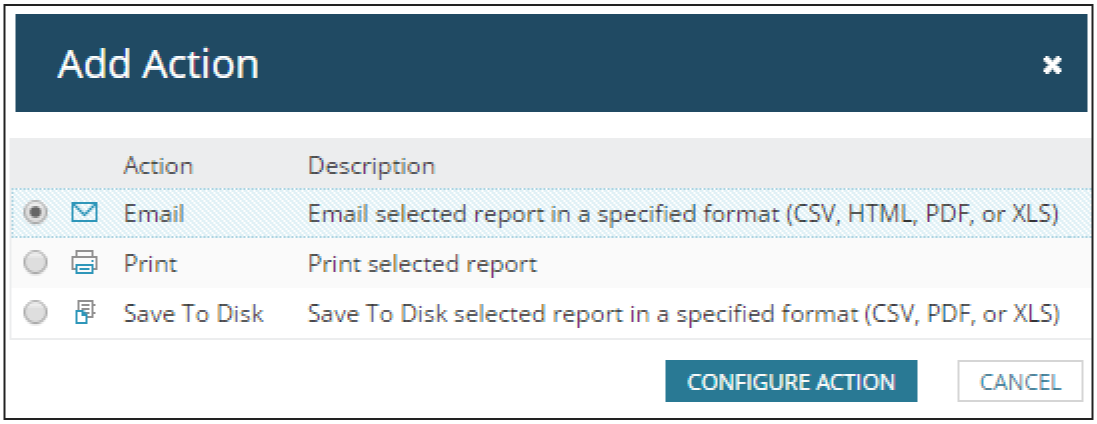
☑ Sunday ☐ Monday ☐ Tuesday
☐ Wednesday ☐ Thursday ☐ Friday
☐ Saturday

At 03:00 AM

Starting On: Right Now

☐ Ending On

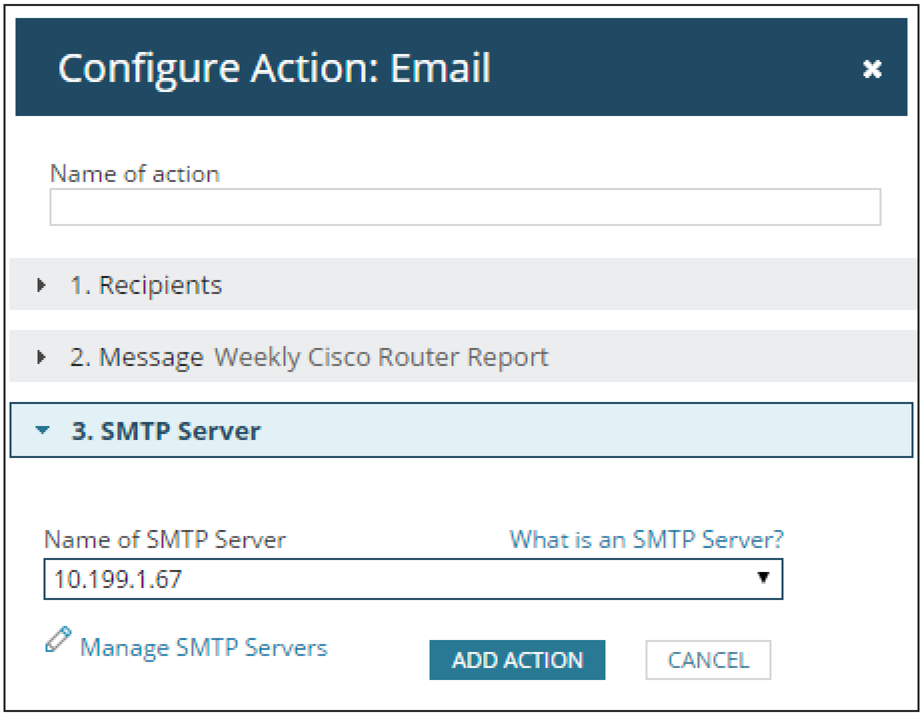
8. Select the actions you want to execute with assigned reports. This example shows the email option selected.



Add Action

	Action	Description
●	Email	Email selected report in a specified format (CSV, HTML, PDF, or XLS)
○	Print	Print selected report
○	Save To Disk	Save To Disk selected report in a specified format (CSV, PDF, or XLS)

9. Enter the recipients, a message, and the SMTP Server information to configure the email.



Configure Action: Email

Name of action

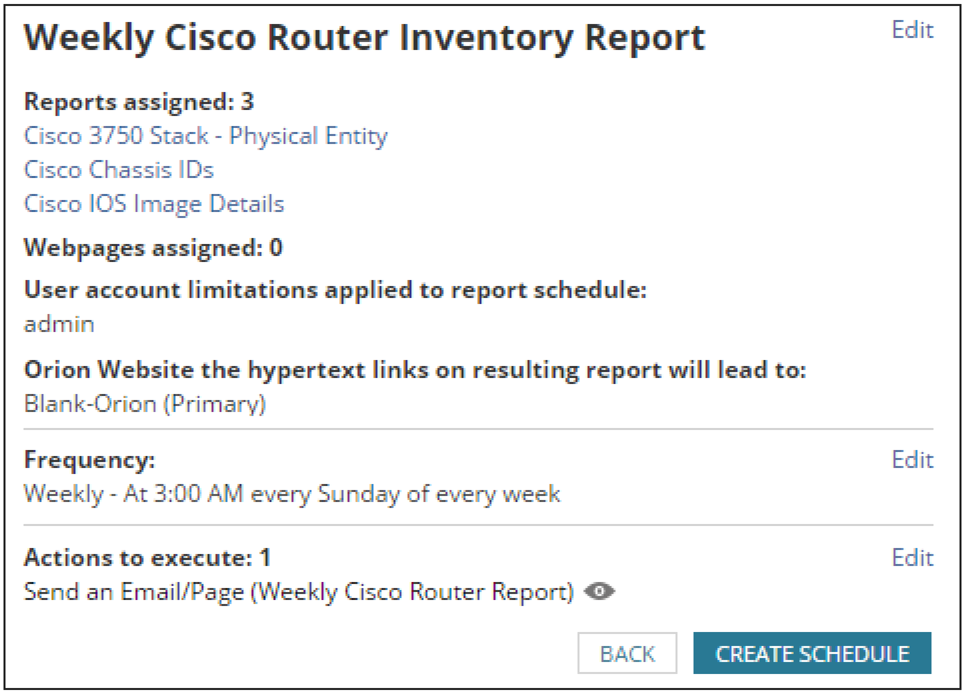
1. Recipients

2. Message Weekly Cisco Router Report

3. SMTP Server

Name of SMTP Server: 10.199.1.67

10. Review the report schedule configuration, and then click Create Schedule.



Weekly Cisco Router Inventory Report

Reports assigned: 3
Cisco 3750 Stack - Physical Entity
Cisco Chassis IDs
Cisco IOS Image Details

Webpages assigned: 0

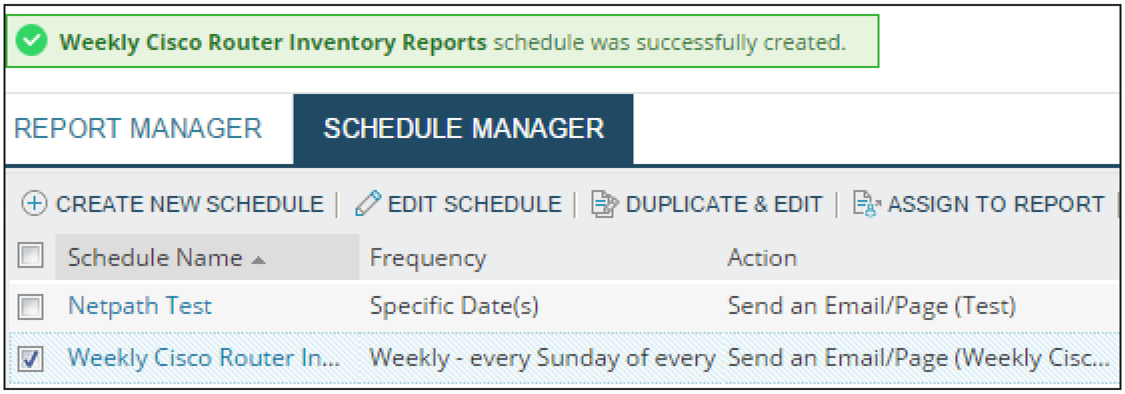
User account limitations applied to report schedule:
admin

Orion Website the hypertext links on resulting report will lead to:
Blank-Orion (Primary)

Frequency:
Weekly - At 3:00 AM every Sunday of every week

Actions to execute: 1
Send an Email/Page (Weekly Cisco Router Report)

The schedule is displayed in the Schedule Manager tab.



Weekly Cisco Router Inventory Reports schedule was successfully created.

	Schedule Name	Frequency	Action
□	Netpath Test	Specific Date(s)	Send an Email/Page (Test)
☑	Weekly Cisco Router In...	Weekly - every Sunday of every	Send an Email/Page (Weekly Cisc...

Compliance

This section contains the following topic:

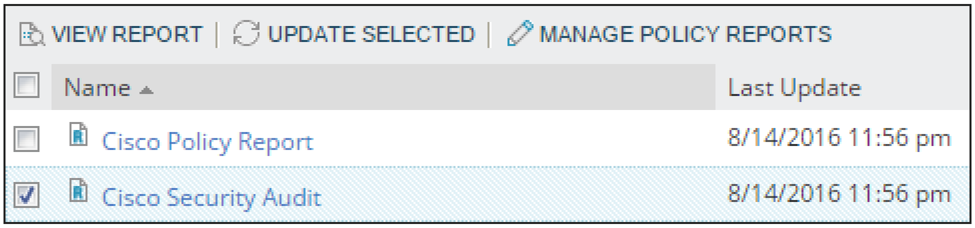
- Audit your Cisco routers

Audit your Cisco routers

Organizations must adhere to different policy compliance requirements such as HIPAA, SOX, DISA, STIG, FISMA, and PCI. Use the NCM compliance policy reports to verify and maintain compliance within your network. Policy reports help ensure that your device configurations conform to both internal business practices and federal regulations. You can use out-of-the-box reports, create your own report, or upload a report from THWACK.

The following example shows you how to run a Cisco Security Audit policy report.

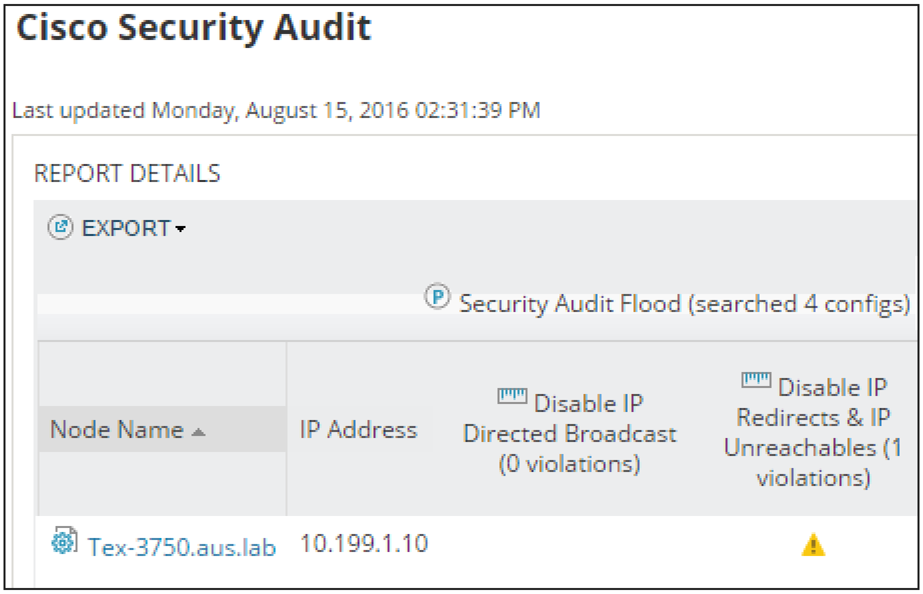
1. Click My Dashboards > Network Configuration > Compliance.
2. Select a report and click Update Selected.



□	Name ▲	Last Update
□	Cisco Policy Report	8/14/2016 11:56 pm
☑	Cisco Security Audit	8/14/2016 11:56 pm

When the report is complete the Last Update column displays the date you ran the report.

3. Click the report name to view the Report Details page. The Tex-3750.aus.lab router has one violation for Disable IP Redirects & IP Unreachables.



Cisco Security Audit

Last updated Monday, August 15, 2016 02:31:39 PM

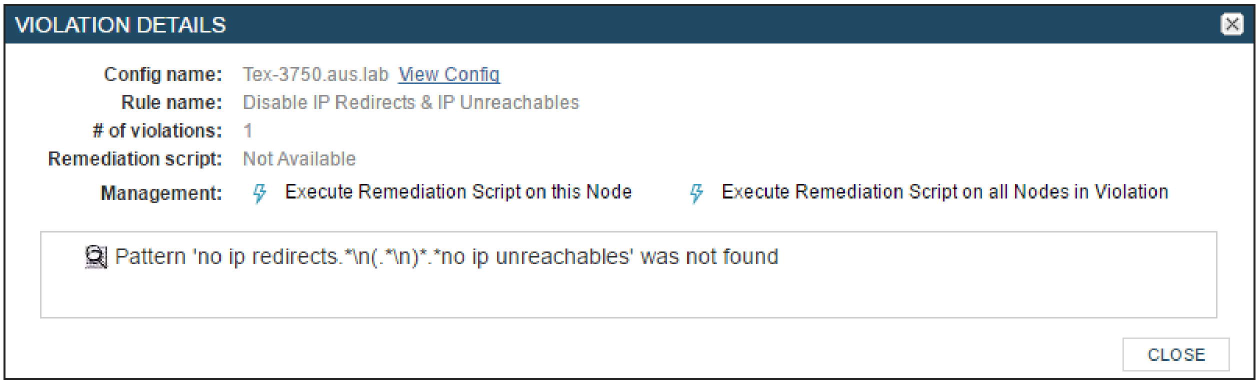
REPORT DETAILS

Security Audit Flood (searched 4 configs)

Node Name	IP Address	Disable IP Directed Broadcast (0 violations)	Disable IP Redirects & IP Unreachables (1 violations)
Tex-3750.aus.lab	10.199.1.10		⚠

4. On the Report Details page, click the violation icon to open the Violation Details page.

5. On the Violation Details page, click Execute Remediation Script on this Node.



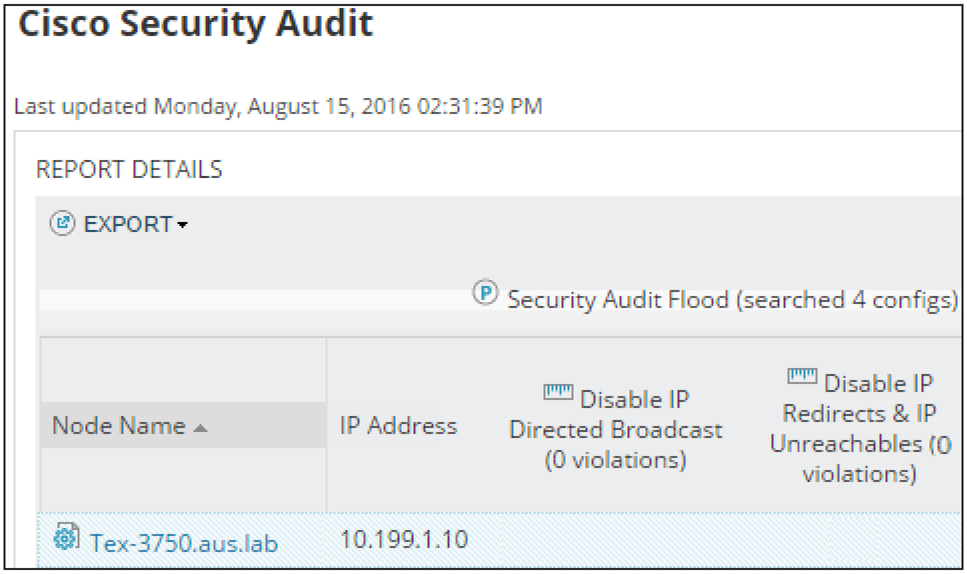
VIOLATION DETAILS

Config name:	Tex-3750.aus.lab View Config
Rule name:	Disable IP Redirects & IP Unreachables
# of violations:	1
Remediation script:	Not Available
Management:	Execute Remediation Script on this Node Execute Remediation Script on all Nodes in Violation

Pattern 'no ip redirects.*\n(.*\n)*.*no ip unreachables' was not found

6. Run the report again.

   The violation has now been resolved and is no longer displayed.



Cisco Security Audit

Last updated Monday, August 15, 2016 02:31:39 PM

REPORT DETAILS

Security Audit Flood (searched 4 configs)

Node Name ▲	IP Address	Disable IP Directed Broadcast (0 violations)	Disable IP Redirects & IP Unreachables (0 violations)
Tex-3750.aus.lab	10.199.1.10		