

**Air Force Life Cycle Management Center (AFLCMC)**

**Base Information Transport Infrastructure (BITI)**

**Base Area Network (BAN)**

**Network Management Systems (NMS)**

**CONTRACT NUMBER: FA8732-14-D-0019**

**DELIVERY ORDER NUMBER: FA8726-18-F-0039**

**Training Materials: Lab Book**

**Version 10**

**CDRL A008**

**CAGE Code 61443**

**Submitted to:**

AFLCMC/HNIB

U. S. AIR FORCE

HANSCOM AFB, MA

**Submitted by:**



AMERICAN SYSTEMS CORPORATION

14151 Park Meadow Drive

Chantilly, VA 20151

Phone: (703) 968-6300

**15 February 2021**

**Distribution Statement D:** Distribution authorized to the Department of Defense (DoD) and U.S. DoD contractors only; administrative/operation use; 15 February 2018. Other requests shall be referred to: Director, AFLCMC/AFNET Operations & Sustainment Branch (HNIB), Enterprise Information Technology & Cyber Infrastructure Division (HNI), 15 Eglin Street, Hanscom AFB, MA. 01731

**Destruction Notice:** Destroy by any method that shall prevent disclosure of contents or reconstruction of the document.

## Version History

Number	Date	Comment
3	10/11/2019	Initial submission, revision synchronized to match Training Lecture. Lab files submitted individually (16 files)
4	10/21/2019	Individual labs combined into a single document
5	10/14/2019	Optimized graphics and formatting, added cover page and revision log.
6	2/20/2020	Updated based on feedback and lessons learned from initial training sites.
7	6/25/2020	Corrected 4 errata points
8	10/07/2020	Adapted to Virtual Classroom and VM's
9	2/1/2021	Corrected text, updated diagrams
10	2/15/2021	SolarWinds 2020.2 updates

# Table of Contents

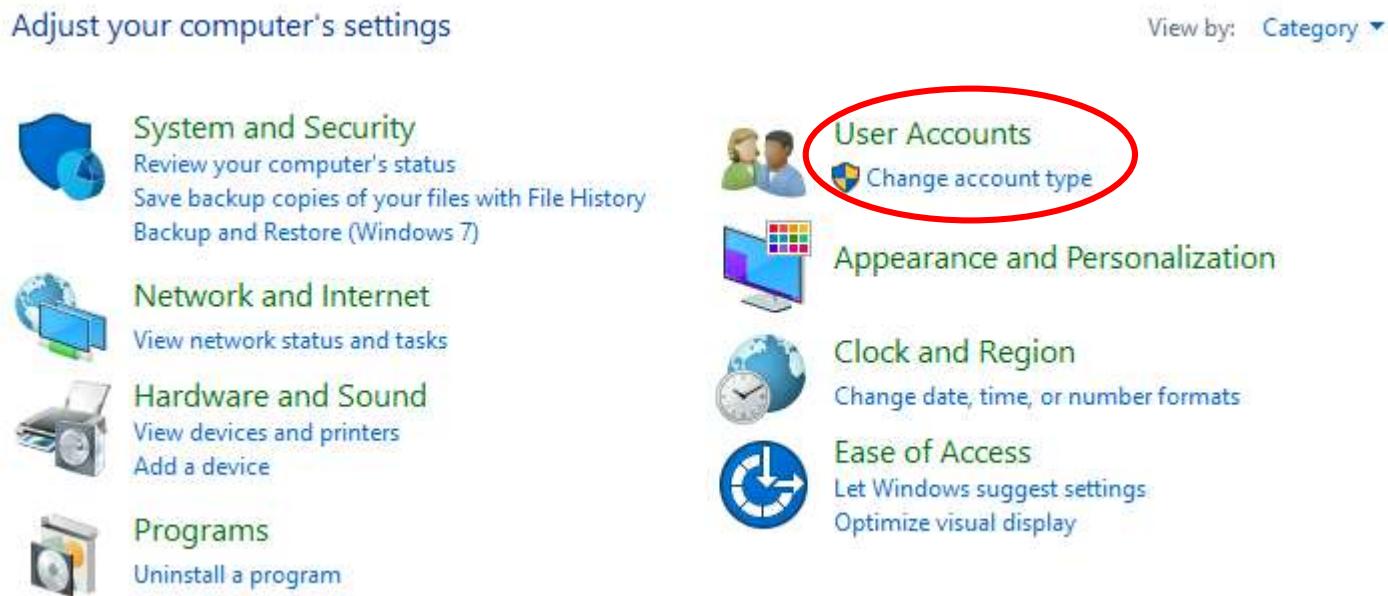
<b>Version History.....</b>	<b>2</b>
<b>Table of Contents .....</b>	<b>3</b>
<b>Lab 01 - Installing SolarWinds Orion and Configuration Wizard.....</b>	<b>4</b>
<b>Lab 02 – Network Discovery .....</b>	<b>26</b>
<b>Lab 03 - Custom Properties.....</b>	<b>50</b>
<b>Lab 04 - Groups .....</b>	<b>67</b>
<b>Lab 05 - Creating a Dashboard/View .....</b>	<b>77</b>
<b>Lab 06 – Account Management .....</b>	<b>93</b>
<b>Lab 07 - Manage Nodes .....</b>	<b>107</b>
<b>Lab 08 - Network Atlas .....</b>	<b>125</b>
<b>Lab 09 –Alerts.....</b>	<b>133</b>
<b>Lab 10 – Reports.....</b>	<b>163</b>
<b>Lab 11 – Script Management .....</b>	<b>191</b>
<b>Lab 12 – NCM Settings.....</b>	<b>201</b>
<b>Lab 13 - Device Templates .....</b>	<b>212</b>
<b>Lab 14 – Baseline Management.....</b>	<b>225</b>
<b>Lab 15 – NCM Jobs.....</b>	<b>235</b>
<b>Lab 16 - Compliance .....</b>	<b>245</b>
<b>Appendix A – Comprehensive Review .....</b>	<b>263</b>
<b>Appendix B: Custom Properties.....</b>	<b>267</b>

# Lab 01 - Installing SolarWinds Orion and Configuration Wizard

This guide will provide information required to install SolarWinds Orion products.

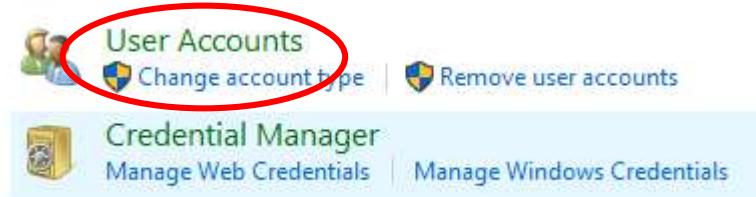
Step 1.0 – Set the User Account Control (UAC) setting to the bottom.

Step 1.1



Navigate as shown above.

## Step 1.2



Navigate as shown above.

## Step 1.3

Make changes to your user account

[Make changes to my account in PC settings](#)

[Manage another account](#)

[Change User Account Control settings](#)



Navigate as shown above.

## Step 1.4

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.

[Tell me more about User Account Control settings](#)

Always notify



Never notify me when:

- Apps try to install software or make changes to my computer
- I make changes to Windows settings

Not recommended.

Never notify



Move slider bar to the “Never Notify” level. Otherwise, the Installation Wizard and the Configuration Wizard may error out.  
Click ‘OK’

## Step 2.0 – Turn off Windows Defender

### Step 2.1

Adjust your computer's settings

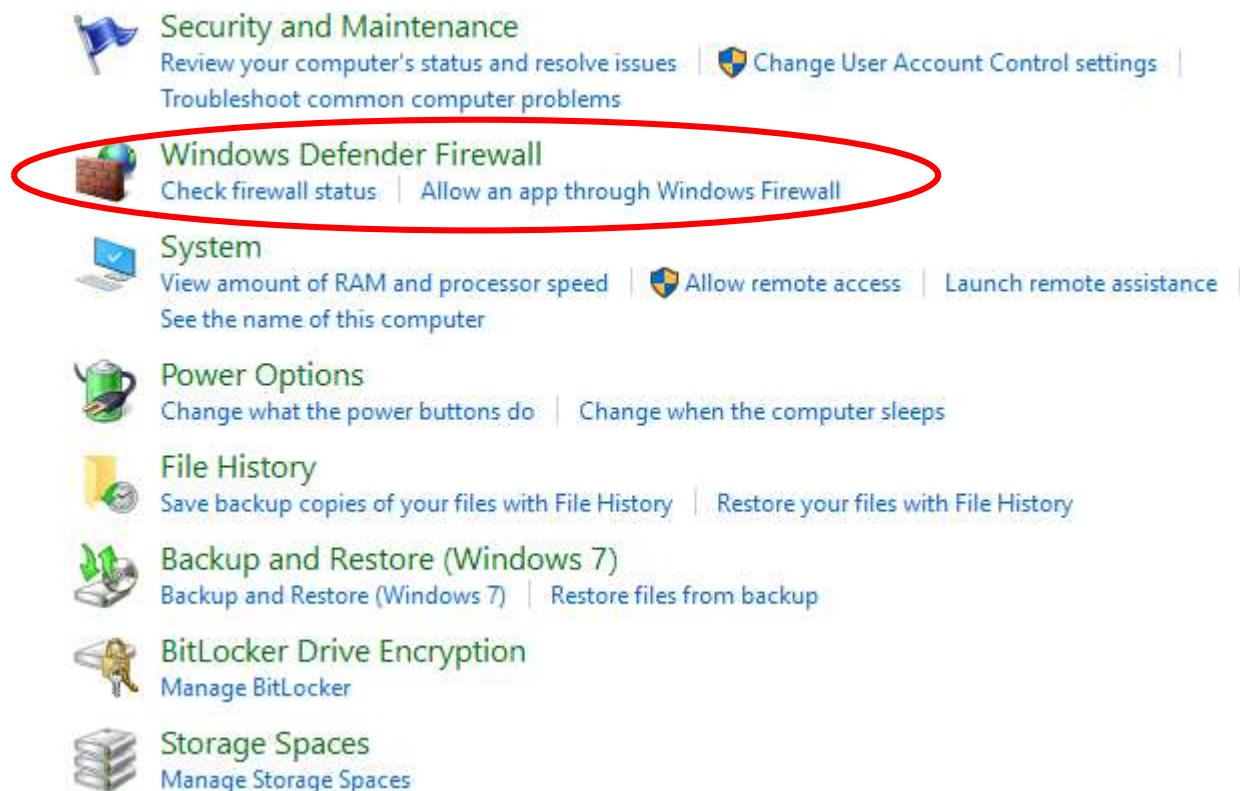
View by: Category ▾

The screenshot shows the Windows Control Panel interface. On the left, there is a list of categories: 'System and Security', 'Network and Internet', 'Hardware and Sound', and 'Programs'. The 'System and Security' category is circled in red. On the right, there are four more categories: 'User Accounts', 'Appearance and Personalization', 'Clock and Region', and 'Ease of Access'. Each category has a small icon next to its name and a brief description below it.

<b>System and Security</b> Review your computer's status Save backup copies of your files with File History Backup and Restore (Windows 7)	<b>User Accounts</b> Change account type
<b>Network and Internet</b> View network status and tasks	<b>Appearance and Personalization</b>
<b>Hardware and Sound</b> View devices and printers Add a device	<b>Clock and Region</b> Change date, time, or number formats
<b>Programs</b> Uninstall a program	<b>Ease of Access</b> Let Windows suggest settings Optimize visual display

Navigate as shown above.

## Step 2.2



Navigate as show above

## Step 2.3

The screenshot shows the Windows Defender Firewall settings window. On the left, there's a sidebar with links like Control Panel Home, Allow an app or feature through Windows Defender Firewall, Change notification settings, Turn Windows Defender Firewall on or off (which is circled in red), Restore defaults, Advanced settings, and Troubleshoot my network. The main area has two sections: 'Private networks' and 'Guest or public networks'. Each section shows the Windows Defender Firewall state as 'On', incoming connections set to block all apps not on the allowed list, active private networks listed as 'Network', and notification state set to 'Notify me when Windows Defender Firewall blocks a new app'. Both sections are labeled as 'Connected'.

Help protect your PC with Windows Defender Firewall	
Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.	
<b>Private networks</b> <span style="float: right;">Connected</span>	
Networks at home or work where you know and trust the people and devices on the network	
Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	Network
Notification state:	Notify me when Windows Defender Firewall blocks a new app
<b>Guest or public networks</b> <span style="float: right;">Connected</span>	
Networks in public places such as airports or coffee shops	
Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	Unidentified network
Notification state:	Notify me when Windows Defender Firewall blocks a new app

This window will show you the status of Windows Defender. We want to navigate to the left to turn off the Windows Defender.

## Step 2.4

### Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

#### Private network settings



Turn on Windows Defender Firewall

Block all incoming connections, including those in the list of allowed apps

Notify me when Windows Defender Firewall blocks a new app



Turn off Windows Defender Firewall (not recommended)

#### Public network settings



Turn on Windows Defender Firewall

Block all incoming connections, including those in the list of allowed apps

Notify me when Windows Defender Firewall blocks a new app



Turn off Windows Defender Firewall (not recommended)

Action: Select each of the “Turn off” options as seen above. Click “OK” when done.

## Step 2.5

### Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

The screenshot shows the Windows Defender Firewall settings. At the top, there's a red banner with the text "Update your Firewall settings" and a message stating "Windows Defender Firewall is not using the recommended settings to protect your computer." A "Use recommended settings" button is available. Below the banner, there are two main sections: "Private networks" and "Guest or public networks".

**Private networks:**

- Windows Defender Firewall state: Off
- Incoming connections: Block all connections to apps that are not on the list of allowed apps
- Active private networks: Network
- Notification state: Notify me when Windows Defender Firewall blocks a new app

**Guest or public networks:**

- Windows Defender Firewall state: Off
- Incoming connections: Block all connections to apps that are not on the list of allowed apps
- Active public networks: Unidentified network
- Notification state: Notify me when Windows Defender Firewall blocks a new app

You have turned off the Windows Defender.

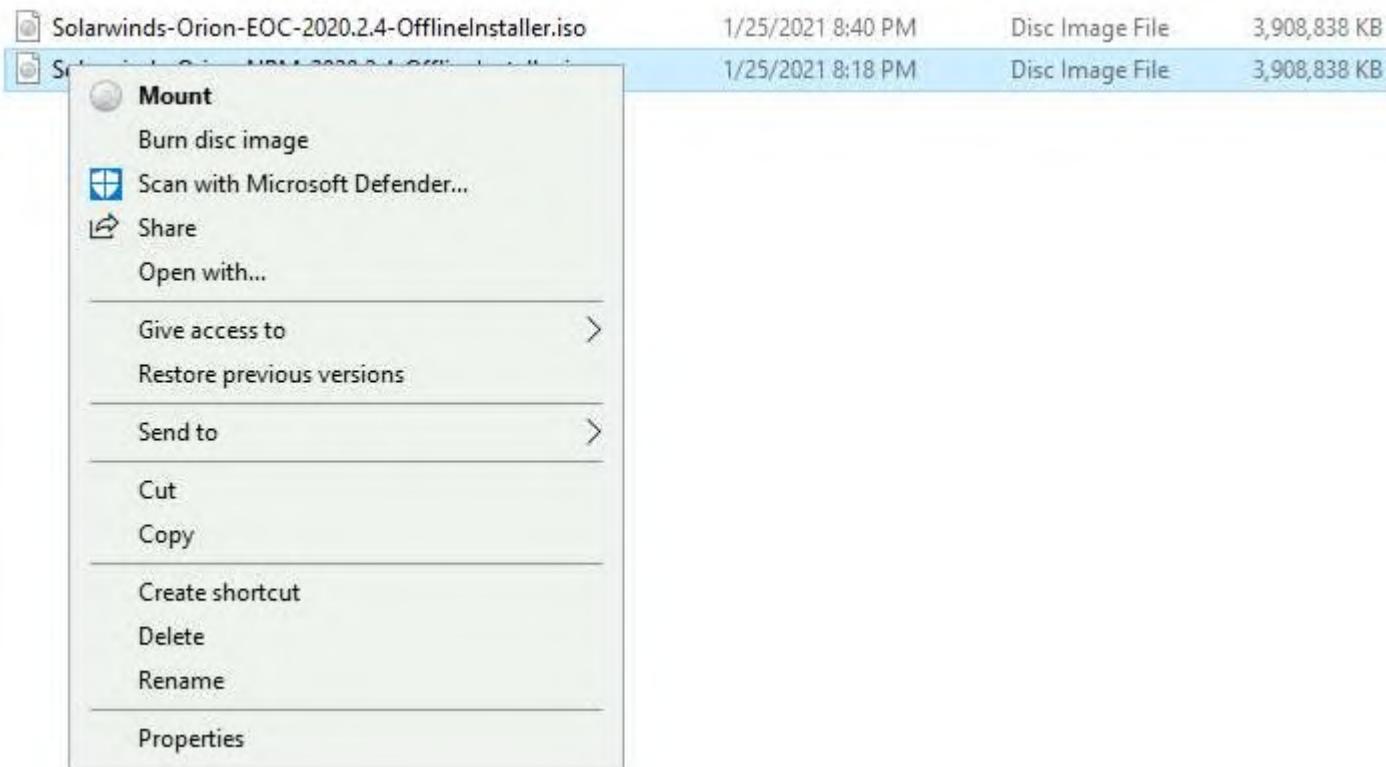
If your server STIGs and Hardening are set correctly your UAC and Windows Defender will be reset each night.

## Step 3.0 – Installing SolarWinds Orion Software

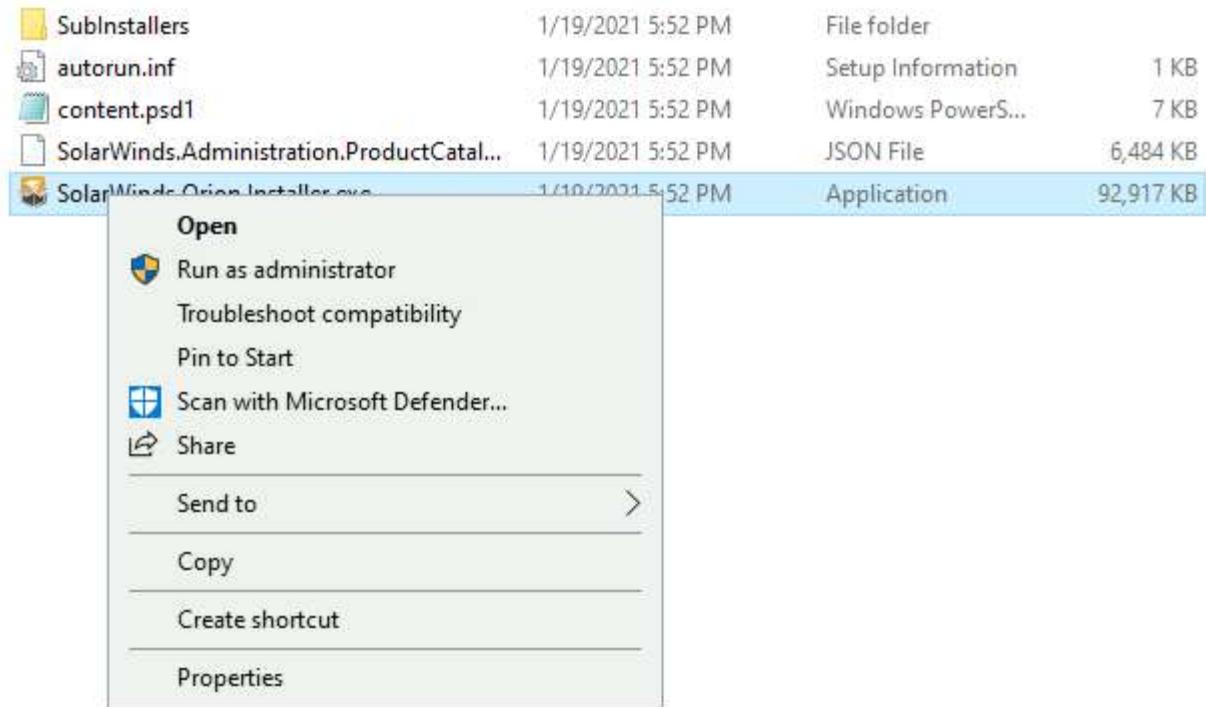
Name	Date modified	Type	Size
Solarwinds-Orion-EOC-2020.2.4-OfflineInstaller.iso	1/25/2021 8:40 PM	Disc Image File	3,908,838 KB
Solarwinds-Orion-NPM-2020.2.4-OfflineInstaller.iso	1/25/2021 8:18 PM	Disc Image File	3,908,838 KB

Navigate on the desktop to the Install folder. We will be installing SolarWinds-Orion-NPM-2020.2-Offline version. Always use the Offline version as our systems may not have access to the internet location of the Orion Installer Software.

## Step 3.1



Right-Click on the file to mount the ISO.



Even though you may be logged into the machine as an administrator, it is good practice to select and “Run as administrator”.

## Step 3.2

Once you click on Run as Administrator, it may take about 60 seconds for the Extractor to be visible on the screen. The installation process has some time where it seems there is nothing happening, but rest assured, it's Windows and there are always things happening in the background.

## Step 3.3



Copyright © 2020 SolarWinds Worldwide, LLC. All rights reserved.

## Step 3.4

The Setup Wizard will guide you through installing SolarWinds products. After installation, the Configuration Wizard will guide you through configuring your products.

**Welcome**

The Setup Wizard will guide you through installing SolarWinds products. After installation, the Configuration Wizard will guide you through configuring your products.

**Lightweight Installation**

- Installs SQL Server Express locally
- Database size limited to 10GB
- Good for evaluating products on the Orion Platform

**Standard Installation**

- Requires SQL Server
- Database size limited by storage
- Required for production environments

**Add a Scalability Engine**

- Requires an existing primary Orion server installation
- Add another poller or website
- Protect an existing server with HA

Setup will install files in the following folder:

DESTINATION FOLDER:

e:\Program Files (x86)\SolarWinds\Orion

BROWSE...

Select Language | ▾

**NEXT**

Lightweight Installation will be used for this course. We are in a small environment and working with just a couple products. This type of installation is not for a production environment.

Standard Installation is for the production environment. This installation will require a dedicated SQL Server.

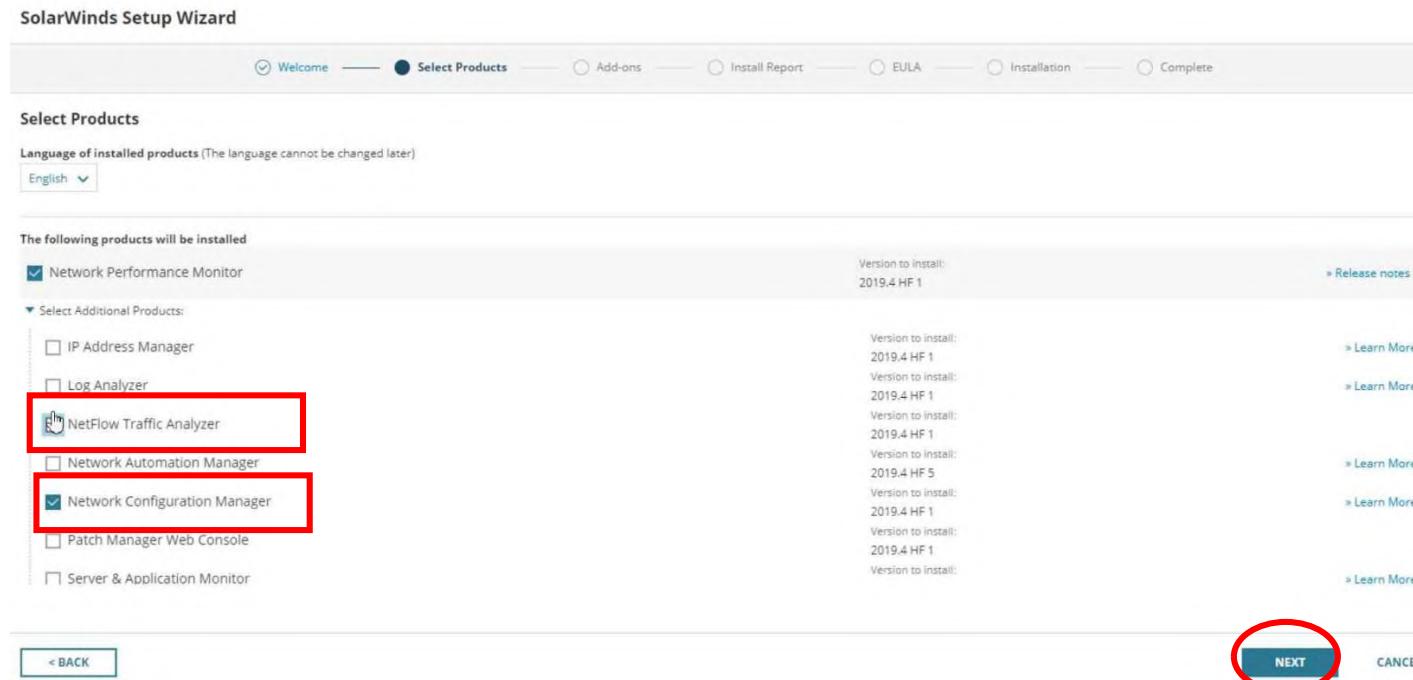
Scalability is designed for the Additional Pollers, Additional Webservers, and High Availability architectures.

In our classroom environment we will be installing on the E:\.

In production, DO NOT INSTALL ON C:\ EVER!!! Installation in production should be done on a separate volume.

Action: Click ‘NEXT’ when complete

## Step 3.5

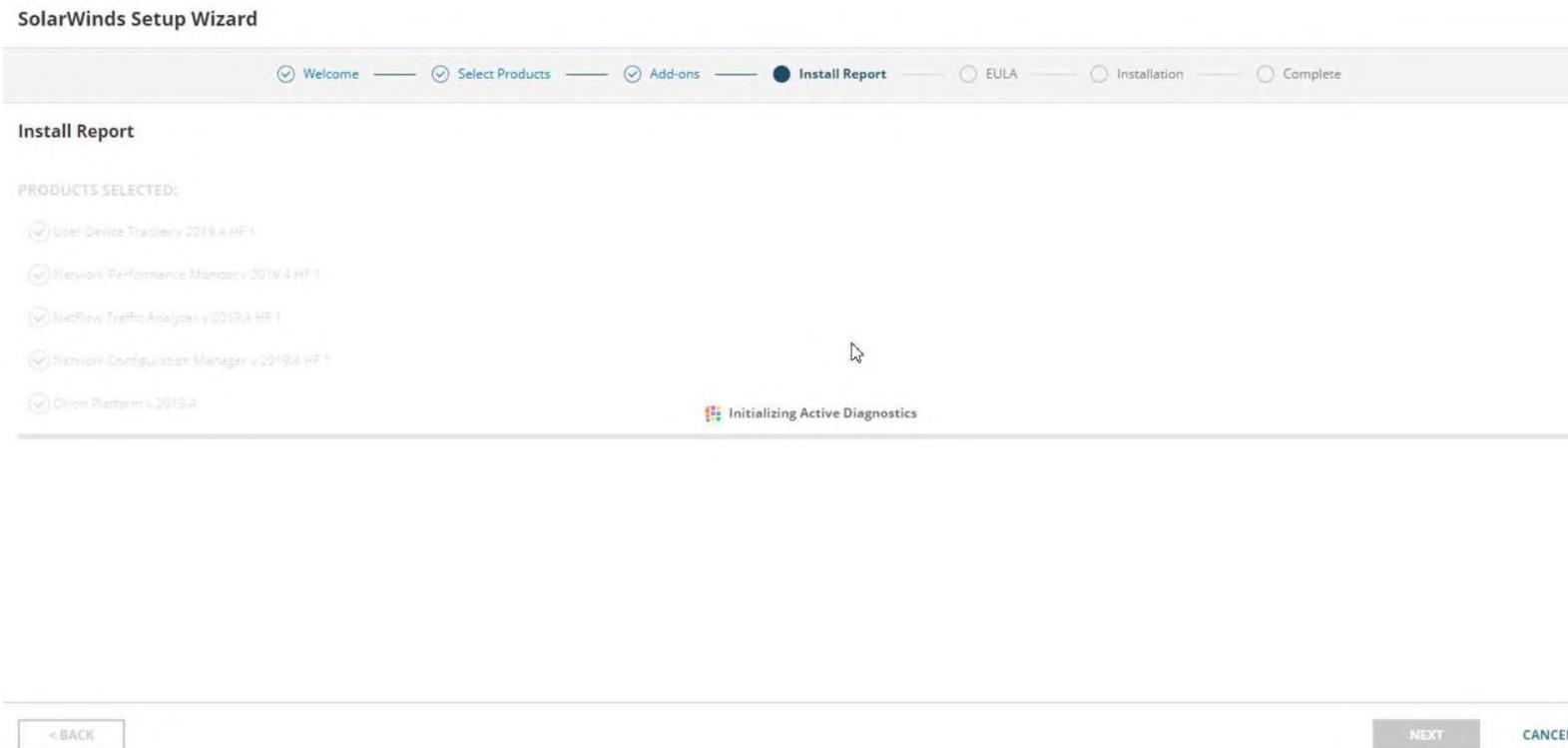


On this screen, we will have the opportunity to install other Orion Integrated products. Since we are installing NPM from the base software version is already include in this list of software. Today we will be adding on the a few other modules to our NPM install. Check the box next to the following modules:

- NetFlow Traffic Analyzer
- Network Configuration Manager
- User Device Tracker

Click ‘NEXT’.

## Step 3.6



The software packages selected previously are being organized and unpackaged for installation. Give it some time to complete. Then click “NEXT” when the report is finished.

## Step 3.7

### End User License Agreement (EULA)

SolarWinds Setup Wizard

✓ Welcome —— ✓ Select Products —— ✓ Add-ons —— ✓ Install Report —— ● EULA —— ○ Installation —— ○ Complete

#### EULA

You must accept the terms of this agreement before continuing.

**SOLARWINDS  
END USER LICENSE AGREEMENT**

BY ACCEPTING THIS AGREEMENT, EITHER BY INDICATING YOUR ACCEPTANCE, BY EXECUTING AN ORDER FORM THAT REFERENCES THIS AGREEMENT, OR BY DOWNLOADING, INSTALLING AND/OR UTILIZING THE SOFTWARE (DEFINED BELOW), YOU AGREE TO THIS AGREEMENT. THIS AGREEMENT IS A LEGALLY BINDING CONTRACT BETWEEN YOU AND SOLARWINDS WORLDWIDE AND SETS FORTH THE TERMS THAT GOVERN THE LICENSE PROVIDED TO YOU HEREUNDER. IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THIS AGREEMENT. ANY CHANGES, ADDITIONS OR DELETIONS BY YOU TO THIS AGREEMENT WILL NOT BE ACCEPTED AND WILL NOT BE A PART OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THIS AGREEMENT, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE.

This End User License Agreement (the "Agreement") is hereby entered into and agreed upon by you, either an individual or an entity, and its Affiliates ("You" or "Company") and SolarWinds Worldwide, LLC ("SolarWinds Worldwide") for the Software. This Agreement sets forth the obligations of each party.

**1. DEFINITIONS.**

**1.1 Affiliates** means an entity controlled by, under common control with, or controlling such party, where control is denoted by having fifty percent (50%) or more of the voting power (or equivalent) of the applicable entity. Subject to the terms and conditions of this Agreement, Affiliates may use the license granted hereunder. All references to SolarWinds shall be deemed to be references to SolarWinds Worldwide and its Affiliates, and all references to Company, You, or Your shall be deemed to be references to Company and its Affiliate(s).

**1.2 Computer** means the hardware, if the hardware is a single computer system, whether physical or virtual, or means the computer system with which the hardware operates, if the hardware is a computer system component.

**1.3 Documentation** means the official user documentation prepared and provided by SolarWinds Worldwide to You on the use of the Software. For the avoidance of doubt, any online community site; unofficial documentation, videos, white papers, or related media; or feedback does not constitute Documentation.

**1.4 Personal Data** means information that may be used to readily identify an individual person.

**1.5 Product Addendum(a)** means additional terms and conditions set forth in Section 12 that relate to the applicable Software.

I accept the terms of the License Agreement

< BACK NEXT CANCEL

You must read the entire agreement. Click 'NEXT'.

## Step 3.8

SolarWinds Setup Wizard

Welcome   Select Products   Add-ons   Install Report   EULA   Installation   Complete

Installation

Installing Microsoft Visual C++ 2008 SP1 Redistributable x86

HELPFUL RESOURCES TO GET YOU STARTED WITH YOUR SOLARWINDS PRODUCT:

**solarwinds customer success**  
A comprehensive introduction to your SolarWinds product, including best practices, real-world examples, tips, and more. Documentation, videos, training, knowledge base articles... it's all here.

**THWACK**  
SOLARWINDS IT COMMUNITY  
When we asked SolarWinds IT pros what advice they would give to themselves if they could go back in time, they all said, 'Join THWACK earlier!' Post questions, get real-time answers - learn from other SolarWinds users, Head Geeks, and community managers. Everyone is friendly and genuinely wants to help out their fellow IT pros. It's basically SolarWinds' special sauce!

**solarwinds customer portal**  
Get your activation keys, additional downloads, submit support tickets, renew your license maintenance, and more.

LEARN   JOIN   VISIT

< BACK   NEXT   CANCEL

Installation process is working. This process can take anywhere from 15 minutes to an hour depending on size of deployment. In our environment today the installation process will take roughly 25 minutes.

## Step 3.9

### SolarWinds Setup Wizard

#### Complete

##### **INSTALLATION PHASE IS COMPLETE. CONFIGURATION IS NECESSARY TO FINALIZE THE INSTALLATION.**

The SolarWinds Setup Wizard has completed. Complete the installation by clicking through the Configuration Wizard.

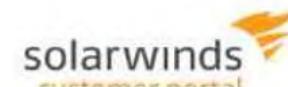
The following products have been successfully installed:

▼ New products installed:

-  User Device Tracker 2019.4 HF 2
-  Network Performance Monitor 2019.4 HF 2
-  NetFlow Traffic Analyzer 2019.4 HF 1
-  Network Configuration Manager 2019.4 HF 1
-  Orion Platform 2019.4



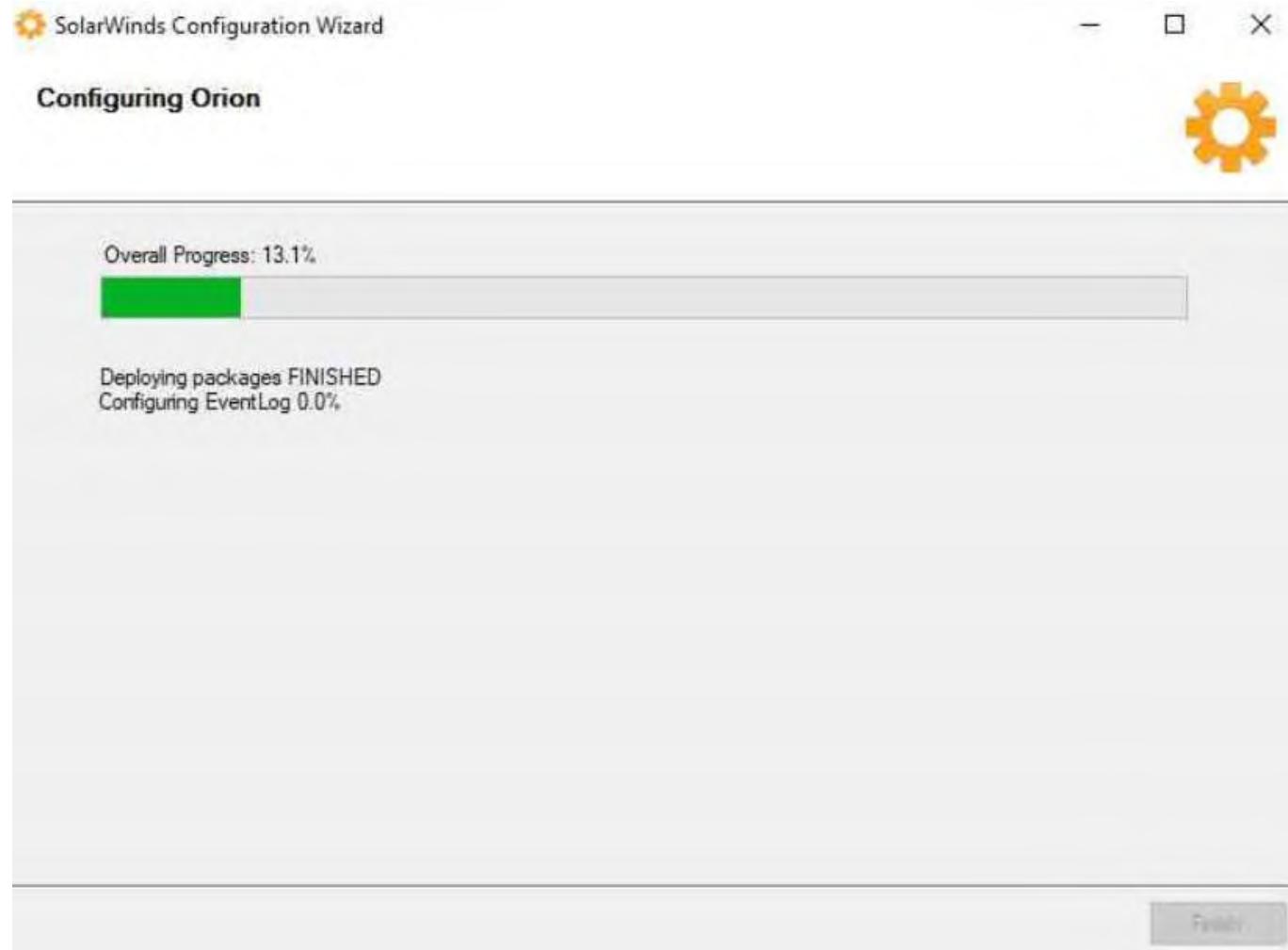
#### **GETTING HELP**



The SolarWinds Orion software has been installed.

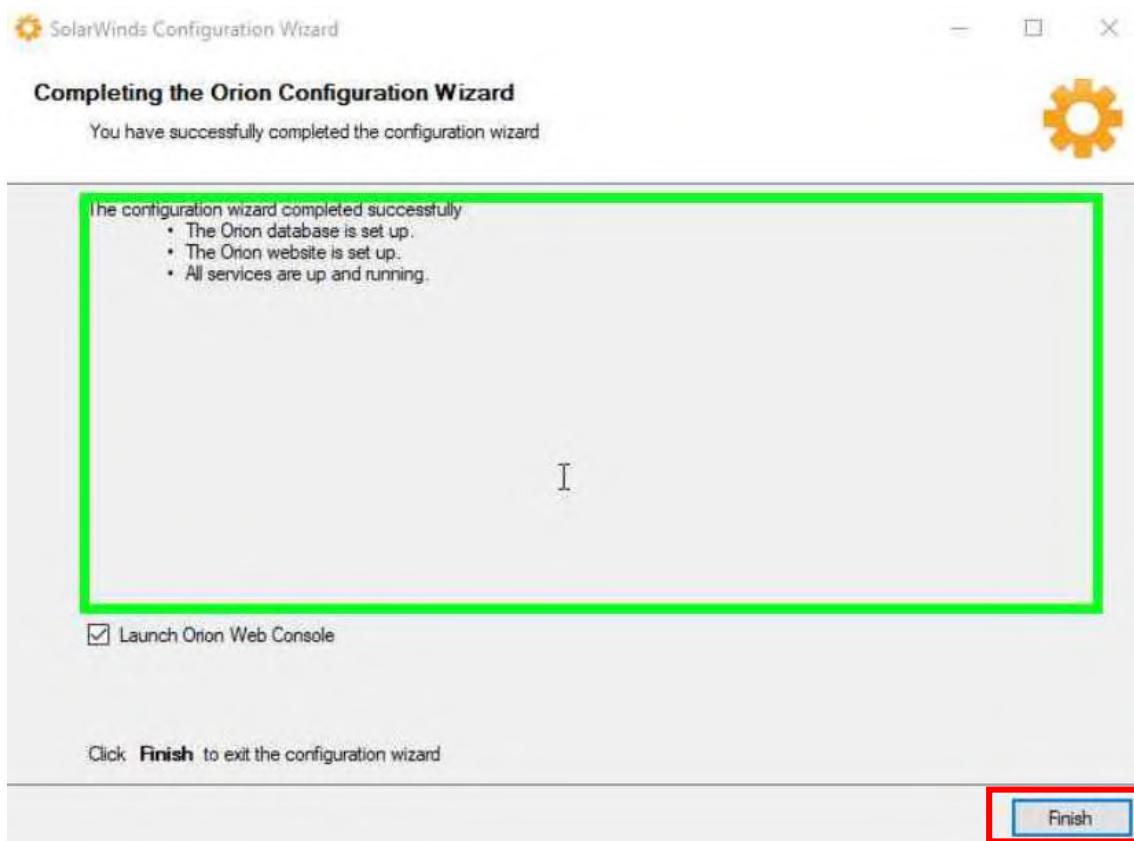
SolarWinds will now kick off the installation of any missing IIS components it requires. No action is needed here.

## Step 3.10



Once the IIS components are completed, SolarWinds will automatically start the Configuration Wizard. This process will develop the database and sync it to the Orion server. This process can take up to 60 minutes depending on the size of your deployment. Today it should take about 30 minutes.

## Step 3.11

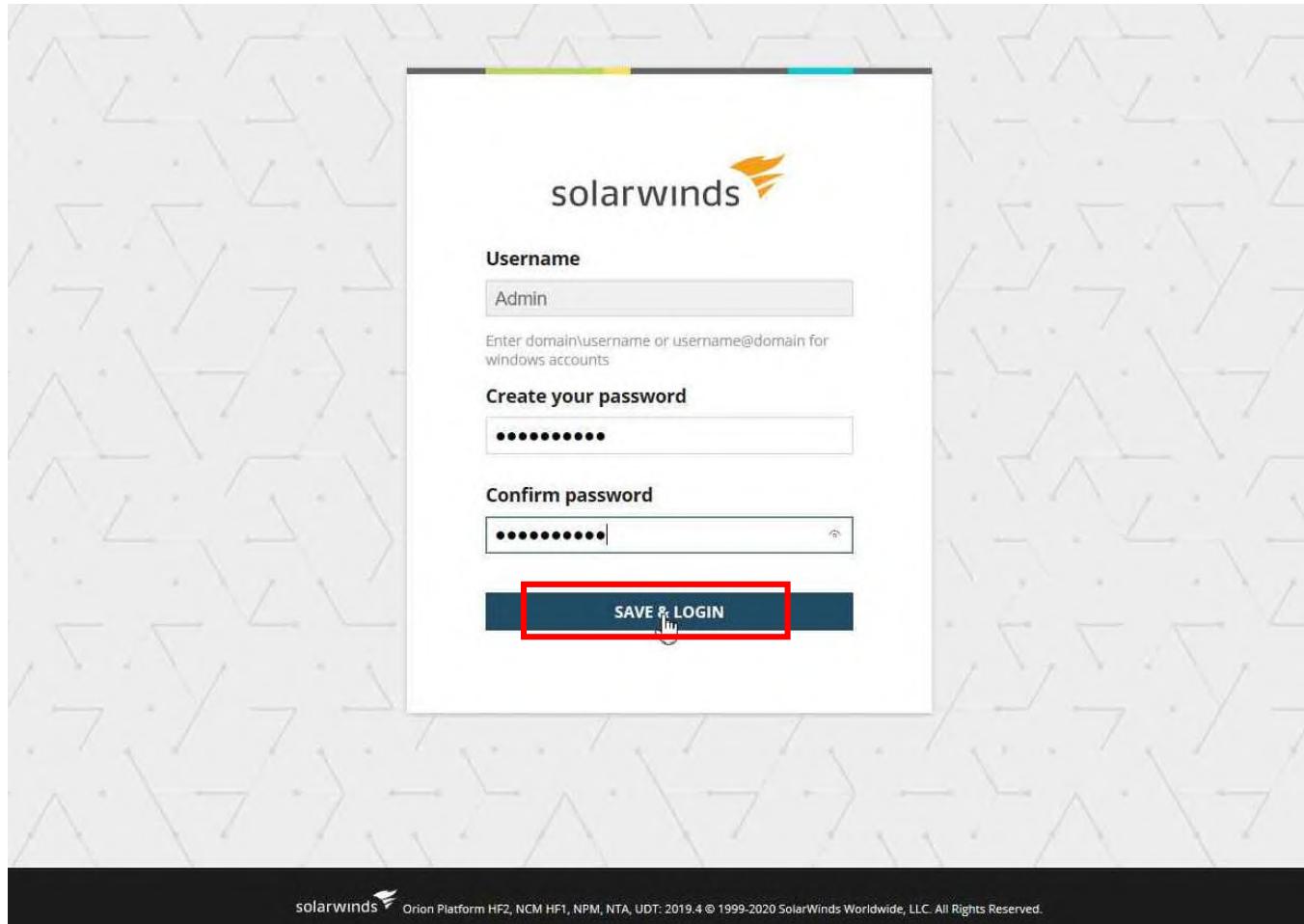


Configuration Wizard has completed successfully. You may now click the ‘FINISH’ button and access your SolarWinds Web Console from your workstation browser. Most server browsers may have been disabled by GPOs and STIG requirements.

If you have any errors here, try to rerun the Configuration Wizard to reset the errors. If any errors persist contact support for troubleshooting steps.

Action: Click ‘FINISH’ when complete.

## Step 3.12



Action: Supply an Admin password prior to login. Click 'SAVE & LOGIN'.

Admin Password: nisgaa

## Step 3.13

Admin ▶ Discovery Central ▶ Discovery Central

 Welcome to Discovery Central

Get started managing your environment.

 **NETWORK DISCOVERY**  
Scan your network for devices like routers, switches and servers. Volumes on these devices will also be discovered.  
You can run Network Sonar Discovery once, or create a profile and schedule your discovery to run in the background.  
» Learn more about Network Sonar Discovery

✓ 1 Nodes are monitored  
⌚ 0 Volumes are monitored

[DISCOVER MY NETWORK](#) [ADD A SINGLE NODE](#)

 **INTERFACE DISCOVERY**  
Find interfaces on network devices and begin monitoring traffic.  
You can run Network Sonar Discovery once, or create a profile and schedule your discovery to run in the background.  
» Learn more about Network Sonar Discovery

✓ 1 Interfaces are monitored

[DISCOVER MY NETWORK](#)

 **VIRTUALIZATION DISCOVERY**  
Add VMware, Hyper-V or Nutanix entities.

⌚ 0 virtual devices are monitored

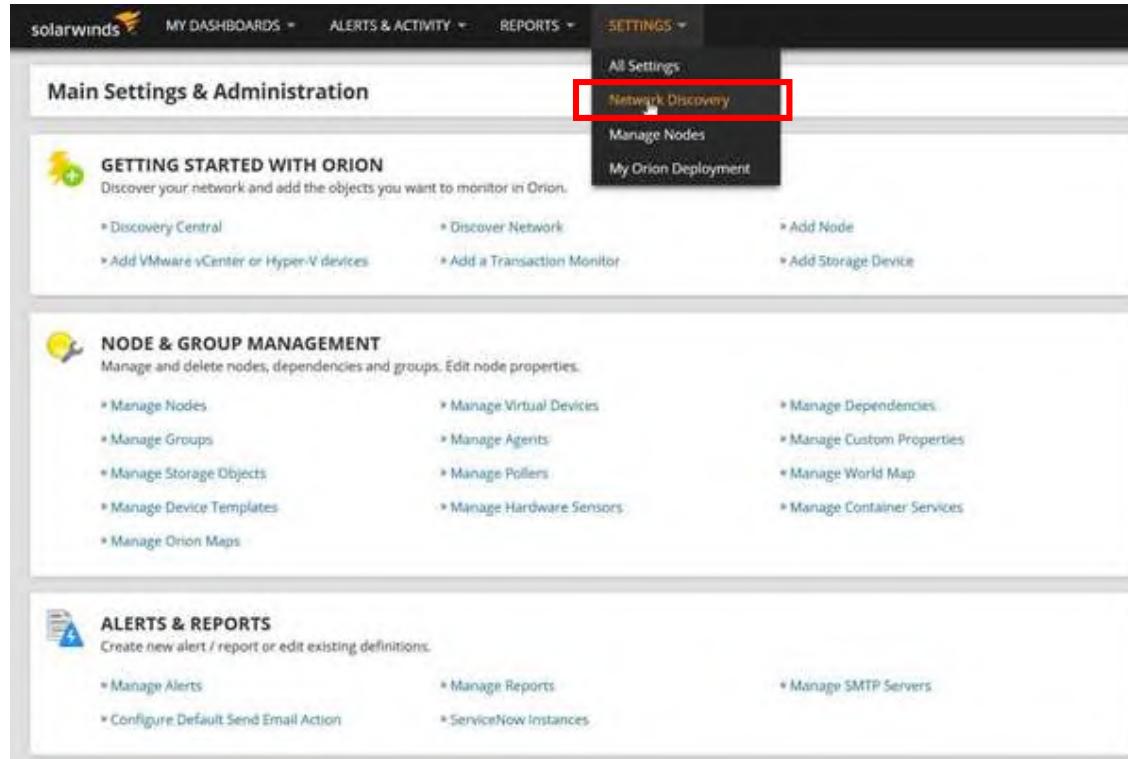
[VMWARE, HYPER-V OR NUTANIX ENTITIES](#)

The initial login screen will bring you to Discovery Central to start discovering your network and organizational IT resources.

This concludes the lab exercise.

# Lab 02 – Network Discovery

This lab will show the student how to run a discovery with SolarWinds and add nodes to the database.  
To use this lab the student will need to review the task and look for the Action heading for actions to take and tasks to perform.  
**Step 1.**



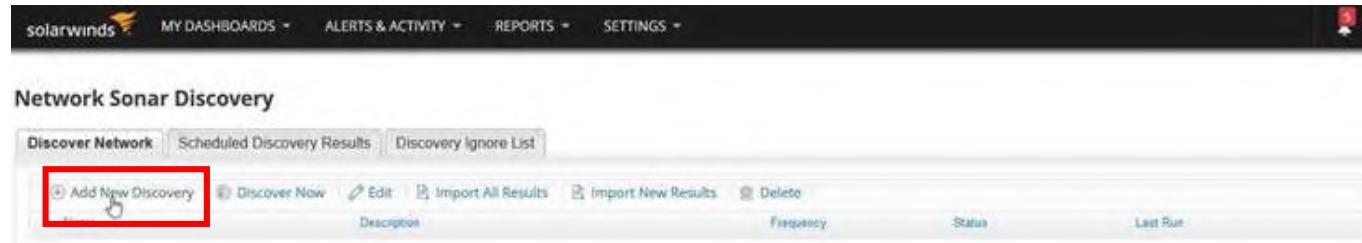
The screenshot shows the SolarWinds Orion interface. At the top, there's a navigation bar with links for 'MY DASHBOARDS', 'ALERTS & ACTIVITY', 'REPORTS', and 'SETTINGS'. The 'SETTINGS' dropdown is open, displaying 'All Settings' and 'Network Discovery' (which is highlighted with a red box), along with 'Manage Nodes' and 'My Orion Deployment'. Below the dropdown, there are three main sections: 'GETTING STARTED WITH ORION', 'NODE & GROUP MANAGEMENT', and 'ALERTS & REPORTS'. Each section contains a list of management tasks.

- GETTING STARTED WITH ORION**
  - \* Discovery Central
  - \* Discover Network
  - \* Add VMware vCenter or Hyper-V devices
  - \* Add a Transaction Monitor
  - \* Add Node
  - \* Add Storage Device
- NODE & GROUP MANAGEMENT**
  - \* Manage Nodes
  - \* Manage Groups
  - \* Manage Storage Objects
  - \* Manage Device Templates
  - \* Manage Orion Maps
  - \* Manage Virtual Devices
  - \* Manage Agents
  - \* Manage Pollers
  - \* Manage Hardware Sensors
  - \* Manage Dependencies
  - \* Manage Custom Properties
  - \* Manage World Map
  - \* Manage Container Services
- ALERTS & REPORTS**
  - \* Manage Alerts
  - \* Configure Default Send Email Action
  - \* Manage Reports
  - \* ServiceNow Instances
  - \* Manage SMTP Servers

Here we start at the 'Main Settings & Administration' page

Action: SETTINGS > Network Discovery

## Step 2.



The screenshot shows the SolarWinds Network Sonar Discovery interface. At the top, there is a navigation bar with links for 'MY DASHBOARDS', 'ALERTS & ACTIVITY', 'REPORTS', and 'SETTINGS'. Below the navigation bar, the title 'Network Sonar Discovery' is displayed. Underneath the title, there are three tabs: 'Discover Network' (which is selected and highlighted in blue), 'Scheduled Discovery Results', and 'Discovery Ignore List'. Below these tabs, there is a toolbar with several buttons: 'Add New Discovery' (highlighted with a red box and a cursor icon), 'Discover Now', 'Edit', 'Import All Results', 'Import New Results', and 'Delete'. The main area below the toolbar contains a table with columns for 'Description', 'Frequency', 'Status', and 'Last Run'. The first row of the table is partially visible.

Here we are going to start a new discovery process.

Action: Select the 'Add New Discovery' button as seen in the picture above.

### Step 3.

#### Network Sonar Wizard

The screenshot shows the 'Network Selection' step of the Network Sonar Wizard. At the top, a navigation bar includes links for NETWORK, VIRTUALIZATION, AGENTS, CONFIGURATION, SNMP, WINDOWS, MONITORING SETTINGS, DISCOVERY SETTINGS, and DISCOVERY SCHEDULING. The 'NETWORK' tab is selected.

**Using discovery for the first time?**

WE RECOMMEND SCANNING... **... a small subnet (/24) with your test environment** OR **... a few individual IP addresses for servers, routers and switches, and VMs**

This will let you see the **wealth of data that Orion provides as quickly as possible**. You can always add more later!

**IP RANGES** (+ Add Range)

**SUBNETS** (+ Add) Subnet (highlighted with a red box)  
Seed Router

**IP ADDRESSES** (i)

**ACTIVE DIRECTORY** (i) (+ Add Active Directory Domain Controller to query...)

Network Sonar Wizard offers four different types of discoveries. A discovery can be made by IP (Address) RANGES, SUBNETS, IP ADDRESSES/Hostname, or ACTIVE DIRECTORY scans.

## Step 4.

SUBNETS

Subnet IP Address in CIDR Format: [i](#)

10.50.2.0/24



 Add 

For the purpose of this lab we will be running a discovery using the IP ADDRESSES of the nodes in our networks.

Action: Enter the IP Addresses of the devices for discovery. Click 'NEXT' when done.

We will be discovering the **10.0.0.0/24** and **10.50.2.0/24** subnets for this lab exercise.

## Step 5.

### Network Sonar Wizard

Adding VMware, Hyper-V or Nutanix entities is handled through a separate workflow. Click Add VMware, Hyper-V or Nutanix entities here to open a separate wizard in a new tab. Finish adding VMware, Hyper-V or Nutanix entities in the separate wizard, then return to this tab and click Next to continue with the discovery wizard. Alternatively, you can skip adding VMware, Hyper-V or Nutanix entities now by clicking Next to continue with the discovery wizard. Add VMware, Hyper-V or Nutanix entities at a later time by navigating to Settings > All Settings > VMware, Hyper-V or Nutanix entities.

BACK      **NEXT**      CANCEL

If you have any virtualization technologies you wish to monitor, you will need to run through this special wizard to enter the required information. We will not be running any virtualization discoveries at this time.

Action: Click 'NEXT'.

## Step 6.

### Network Sonar Wizard

Check nodes polled by agents for updates

By selecting the following option, you can specify which nodes currently polled by an agent will be checked for updates. This setting is helpful when using a scheduled discovery to keep all or a subset of agents updated. Nodes currently polled by an agent will be checked based on settings of this step. [Learn more](#)

Check existing nodes polled by an agent for node changes and updates

Only those Agent managed nodes matching the criteria defined above will have discovery run against them, regardless of any IP/Subnet settings defined on the Network step of this wizard. [Learn more](#)

1 node currently polled by an agent

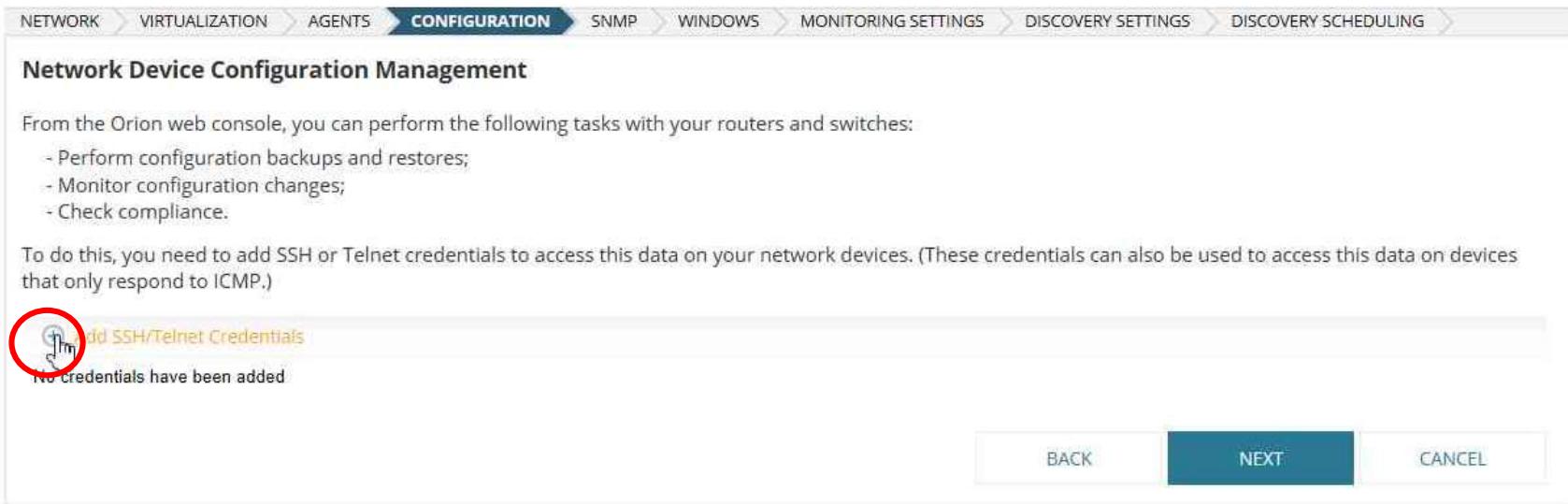
BACK      **NEXT**      CANCEL

This section will communicate to the node to see if there is a SolarWinds Agent currently installed. We will not be running any Agent checks for the purpose of this lab.

Action: Click 'NEXT'.

## Step 7.

### Network Sonar Wizard



The screenshot shows the Orion web console's Network Sonar Wizard. The 'CONFIGURATION' tab is selected. The main content area is titled 'Network Device Configuration Management'. It lists tasks such as performing backups, monitoring changes, and checking compliance. A section for adding SSH/Telnet credentials is present, with a 'No credentials have been added' message and a 'Add SSH/Telnet Credentials' button. The 'Add SSH/Telnet Credentials' button is highlighted with a red circle. At the bottom are 'BACK', 'NEXT', and 'CANCEL' buttons.

The SSH Credentials section is the location where you would provide the Network Service Account. This account will SSH into the network device to perform its assigned tasks.

Action: Click on the 'Add SSH/Telnet Credentials'. A pop-up menu will appear.

Action: Once the pop-up menu is completed you will be returned here. Click the 'NEXT' button.

## Step 8.

### Add New Connection Profile

Profile Name:  

CLI Login/User Name:  

CLI Password:  

Enable Level:   

Enable Password

Execute Commands and Scripts Using:  

Request Config Files Using:  

Transfer Config Files Using:

Telnet Port:

SSH Port:

Automatically test this profile against monitored nodes that allowed it. 

Action: As Follows

Enter a Name of the Account used to access your network devices.

Profile Name: Admin Cisco

CLI Login: admin

CLI Password: P@ssw0rd!1

Enable level: <No Enable Login>

Enable Password: [blank]

Execute Command and Scripts Using: SSH 2

Request Config Files Using: SSH 2

Transfer Config Files Using: SSH2

Telnet Port: will automatically change to port 23

SSH Port: will automatically change to port 22

Check Box: Yes, Automatically test this profile against monitored nodes that allow it.

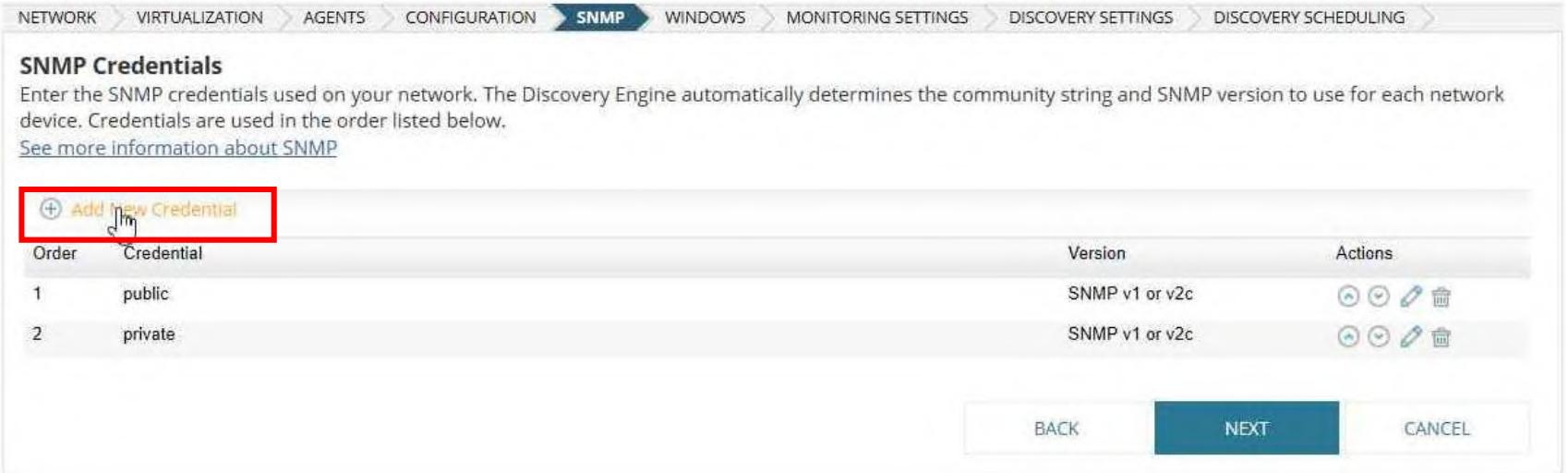
Click ‘ADD’ when the form is complete. This will add your new credential to the list.

**\*Note\*** Make sure you have turned on your GNS3 Network Simulator.

Click the ‘NEXT’ button when complete.

## Step 9.

### Network Sonar Wizard



The screenshot shows the 'SNMP Credentials' page of the Network Sonar Wizard. The top navigation bar includes links for NETWORK, VIRTUALIZATION, AGENTS, CONFIGURATION, **SNMP**, WINDOWS, MONITORING SETTINGS, DISCOVERY SETTINGS, and DISCOVERY SCHEDULING. The 'SNMP' link is highlighted. The main content area is titled 'SNMP Credentials' with the sub-instruction: 'Enter the SNMP credentials used on your network. The Discovery Engine automatically determines the community string and SNMP version to use for each network device. Credentials are used in the order listed below.' Below this, a link 'See more information about SNMP' is provided. A table lists existing credentials:

Order	Credential	Version	Actions
1	public	SNMP v1 or v2c	
2	private	SNMP v1 or v2c	

At the bottom are buttons for BACK, NEXT (highlighted in blue), and CANCEL.

This is where the SNMP Credentials will be supplied for SolarWinds to use to monitor the devices within its database. The public and private strings are already supplied and recommended to be used to look for any devices using the vendor default credentials.

Action: Click 'Add New Credential'.

Click 'NEXT'.

## Step 10.

**Add New Credential**

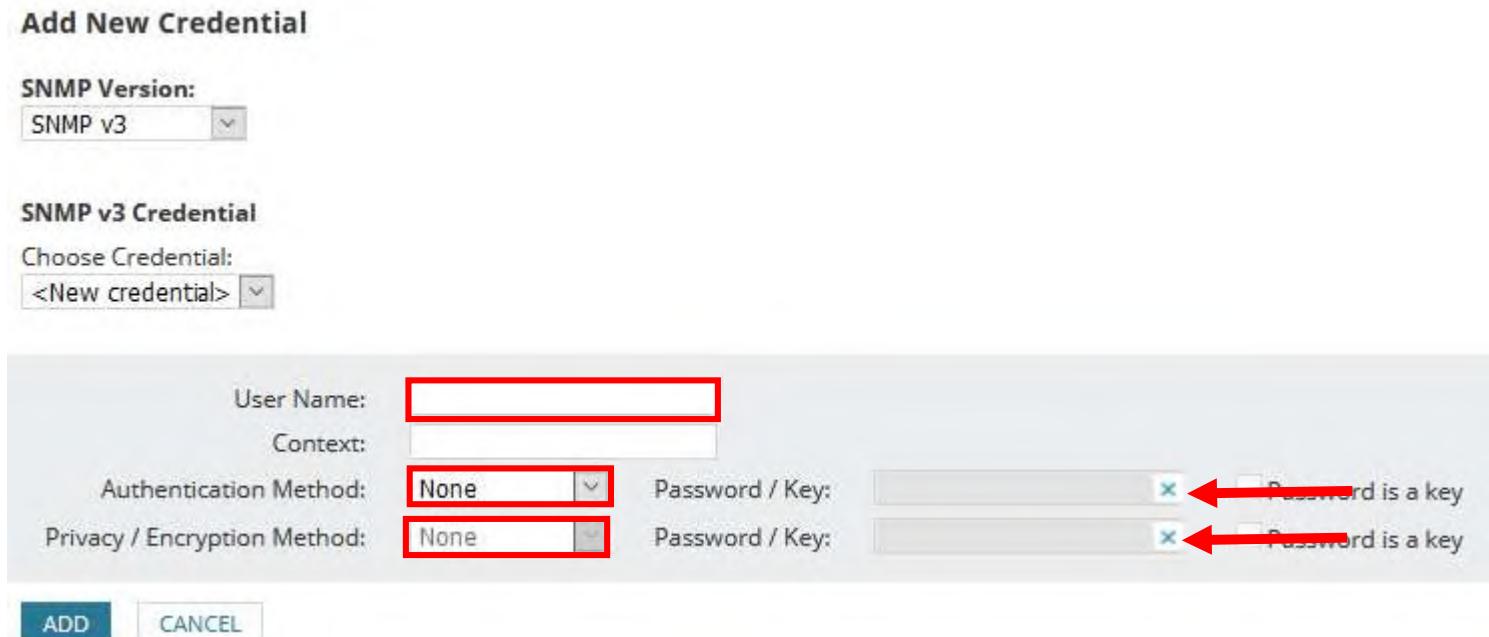
**SNMP Version:**  
SNMP v3

**SNMP v3 Credential**

Choose Credential:  
<New credential>

User Name:	[Redacted]	
Context:		
Authentication Method:	None	Password / Key: [Redacted] <input checked="" type="checkbox"/> Password is a key
Privacy / Encryption Method:	None	Password / Key: [Redacted] <input checked="" type="checkbox"/> Password is a key

**ADD**    **CANCEL**



We will be using SNMPv3 for this course. Department of Defense requirements require the use of SNMPv3 credentials for all networking devices.

Username: Orion

Authentication Method: SHA1

Privacy Method: AES 128

Password: nisgaa

Password: solarwinds

Action: Click 'ADD' when done.

## SNMP Credentials

Enter the SNMP credentials used on your network. The Discovery Engine automatically determines the community string and SNMP version to use for each network device. Credentials are used in the order listed below.

[See more information about SNMP](#)

Add New Credential			
Order	Credential	Version	Actions
1	public	SNMP v1 or v2c	
2	private	SNMP v1 or v2c	
3	User: Orion	SNMP v3	

BACK NEXT CANCEL

Be sure to leave the public and private SNMP community strings in your discovery. It will help you identify those devices that are not STIG compliant.

Action: Click 'NEXT' when complete.

## Step 11.

### Network Sonar Wizard

The screenshot shows the 'Windows Credentials' page of the Network Sonar Wizard. At the top, a navigation bar includes tabs for NETWORK, VIRTUALIZATION, AGENTS, CONFIGURATION, SNMP, WINDOWS (which is highlighted in blue), MONITORING SETTINGS, DISCOVERY SETTINGS, and DISCOVERY SCHEDULING. Below the tabs, the title 'Windows Credentials' is displayed, followed by the instruction: 'Enter the Windows credentials used on your network. Credentials are used in the order listed below.' A link 'Learn more about Windows credentials' is provided. A note states: 'WMI is used to collect CPU, memory, and volume data from Windows Servers that do not support SNMP, in addition to status, response time, and packet loss.' On the left, there is a button labeled '+ Add New Credential' and a message 'No Windows credentials added'. At the bottom right, there are three buttons: 'BACK', 'NEXT' (which is circled in red), and 'CANCEL'.

Windows Credentials can be supplied to help manage your SolarWinds Servers. This is optional and we will skip this step for this lab.

Action: Click 'NEXT'.

## Step 12.

### Network Sonar Wizard

MONITORING SETTINGS

**Monitoring Settings**

Specify how devices should be polled. You can choose what to monitor before the discovery begins, or after it has completed.

**DEVICE/NODE POLLING**

Include devices/nodes that respond to ICMP (ping) alone.  Yes

Devices that respond to SNMP or WMI will still be imported.

Preferred Polling Method:  SNMP  WMI

**HOW WOULD YOU LIKE TO SET UP WHAT TO MONITOR?**

How would you like to set up what to monitor?

**Manually set up monitoring after devices are discovered**   
Select this option to choose what to monitor based on what is found during the discovery. You have more control over what is included or excluded, but you must complete another wizard to finish the discovery process. Devices are not imported until you complete the Network Sonar Results wizard.

**Automatically monitor based on my defined monitoring settings**   
Select this option to choose what to monitor upfront in Define Monitoring Settings. You have less control over what is included or excluded, but your monitored devices are selected in a single wizard. Devices are automatically imported and monitoring is set up according to your settings when you complete the Network Sonar Wizard.

DEFINE MONITORING SETTINGS...

BACK NEXT > CANCEL

At this step in the Discovery Wizard process, we want to ensure we discover all nodes with ICMP at a bare minimum. By sliding the ‘Include devices that respond to ICMP (ping) alone.’ slider to ‘Yes’.

When running a discovery on networking devices you will want to use the SNMP option as the Preferred Polling Method.

How would you like to setup what to monitor? Always choose manually, because if you do not you will soon find yourself out of licensing space if running any license level under the unlimited license pack.

Click ‘NEXT’.

## Step 13.

The screenshot shows the 'Discovery Settings' page in SolarWinds. The navigation bar at the top includes links for NETWORK, VIRTUALIZATION, AGENTS, CONFIGURATION, SNMP, WINDOWS, MONITORING SETTINGS, DISCOVERY SETTINGS (which is highlighted in blue), and DISCOVERY SCHEDULING. The main content area is titled 'Discovery Settings' with the sub-instruction 'Customize your network discovery by configuring the following settings.' Below this, the 'DETAILS' section contains fields for 'Name' (Admin: 10/14/2020, 04:43 PM) and 'Description' (Network Management Subnet), with the 'Description' field highlighted by a red arrow. The 'RETRIES AND TIMEOUTS' section lists various parameters with their current values and dropdown menus for modification:

Setting	Current Value	Options
SNMP Timeout	3000 ms	3000 ms, 2000 ms, 1 retry(s)
Search Timeout	2000 ms	2000 ms, 1 retry(s), 10000 ms
SNMP Retries	1 retry(s)	1 retry(s), 0 hop(s)
WMI Retries	1 retry(s)	1 retry(s), 0 hop(s)
WMI Retry Interval	10000 ms	10000 ms, 60 min
Hop Count	0 hop(s)	0 hop(s)
Discovery Timeout	60 min	60 min

At the bottom right of the page are buttons for BACK, NEXT (which is highlighted with a red box), and CANCEL.

On this section of the discovery, we are provided with different timers for each protocol to discover a device. Generally, these timers are pretty good. There should be no need to change these variables unless there may be latency between the device and SolarWinds or is a small enough discovery for local devices.

Action: Supply a description for the discovery. Supply a short meaningful description for the purpose of this device.

Action: Click 'NEXT' when complete.

## Step 14.

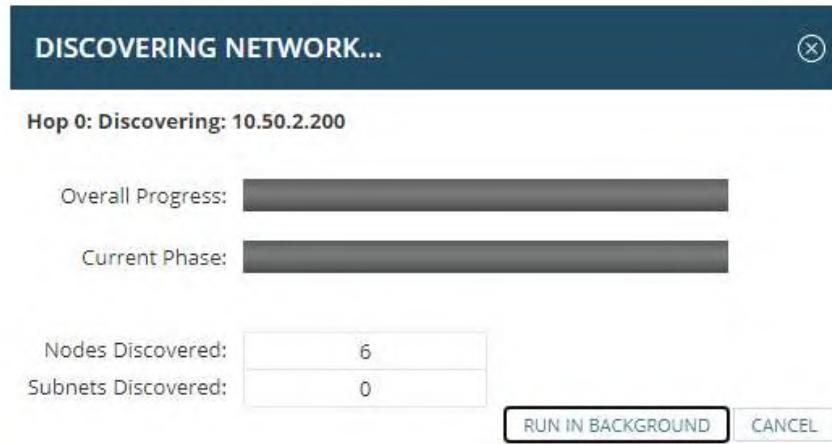
### Network Sonar Wizard

The screenshot shows the 'Discovery Scheduling' step of the Network Sonar Wizard. The 'Frequency' dropdown is set to 'Once' and is highlighted with a red box. Below it, the 'Execute immediately:' section contains two radio buttons: 'Yes, run this discovery now' (selected) and 'No, don't run now'. At the bottom right are three buttons: 'BACK', 'DISCOVER' (highlighted in blue), and 'CANCEL'.

We have reached the end of our Discovery Wizard configuration. You have the option to discover once or set a schedule for repeated discoveries.

Action: Select the 'Once' option

Action: Click on 'DISCOVER' when complete.



Sample of a discovery status notification. Right now, SolarWinds is testing and evaluating the best polling method for the nodes identified.

## Step 15.

### Device Types to Import

Select the device types to monitor.

Count	Device Type
1	Windows 10 Workstation
4	Cisco 3640
1	Unknown

NEXT

CANCEL

Once the Discovery Wizard has completed, SolarWinds will return with a list of items that have been successfully discovered. These items will be selected by default coming out of the discovery scan. You have the option to deselect any items you do not wish to import. For our purposes for this class we will select everything.

Also, if you do import an item that is already in the Node Database, SolarWinds will automatically SKIP the import. You will see this action during the import noted as “Already in Database, skipping import...”

Action: Click ‘NEXT’ when complete.

## Step 16.

**Network Sonar Results Wizard**

DEVICES > INTERFACES > PORTS > VOLUMES > IMPORT PREVIEW > RESULTS >

Select Interfaces to Import for Monitoring

80 interfaces selected

**Selection criteria**

Match all selected properties

Status	Port Mode	Hardware
<input checked="" type="checkbox"/> Operationally up	<input checked="" type="checkbox"/> Trunk	<input checked="" type="checkbox"/> Physical
<input checked="" type="checkbox"/> Operationally down	<input checked="" type="checkbox"/> Access	<input checked="" type="checkbox"/> Virtual
<input checked="" type="checkbox"/> Administratively shutdown	<input checked="" type="checkbox"/> Unknown	<input checked="" type="checkbox"/> Unknown

Advanced selection options

RESELECT INTERFACES

**List of Interfaces**

Selected (Available)	Interface Type
<input checked="" type="checkbox"/>	76 (of 76) Ethernet
<input checked="" type="checkbox"/>	4 (of 4) Other

Group by: Interface Type Show: All

80 interfaces selected

BACK      **NEXT**      CANCEL

On this screen we see the different types of interfaces available for importing into our SolarWinds Database.

Action: Click the box to select all interfaces then click 'NEXT'.

## Step 17.

**Network Sonar Results Wizard**

DEVICES > INTERFACES > **PORTS** > VOLUMES > IMPORT PREVIEW > RESULTS >

Select Ports to Import for Monitoring

76 ports selected

**Selection criteria**

Match all selected properties

Status	Port Mode	Hardware
<input checked="" type="checkbox"/> Operationally up	<input checked="" type="checkbox"/> Trunk	<input checked="" type="checkbox"/> Physical
<input checked="" type="checkbox"/> Operationally down	<input checked="" type="checkbox"/> Access	<input checked="" type="checkbox"/> Virtual
<input checked="" type="checkbox"/> Administratively shutdown	<input checked="" type="checkbox"/> Unknown	<input checked="" type="checkbox"/> Unknown

Advanced selection options

**RESELECT PORTS**

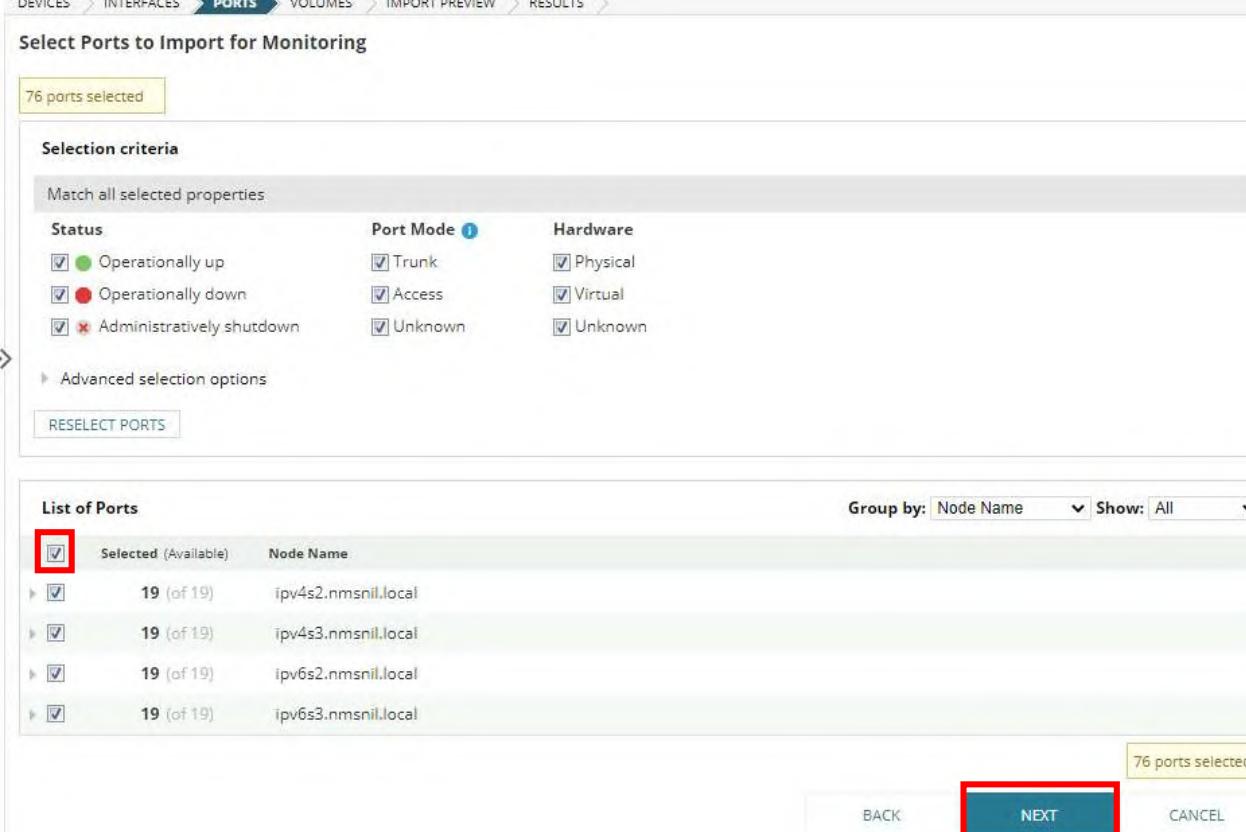
**List of Ports**

Selected (Available)	Node Name
<input checked="" type="checkbox"/>	19 (of 19) ipv4s2.nmsn1.local
<input checked="" type="checkbox"/>	19 (of 19) ipv4s3.nmsn1.local
<input checked="" type="checkbox"/>	19 (of 19) ipv6s2.nmsn1.local
<input checked="" type="checkbox"/>	19 (of 19) ipv6s3.nmsn1.local

Group by: Node Name Show: All

76 ports selected

BACK      **NEXT**      CANCEL



Here we will be selecting to manage, monitor, and analyze all ports.  
Action: Click the box to select all ports then click 'NEXT'.

## Step 18.



SolarWinds importing from a discovery will automatically add volumes such as RAM, Virtual Memory, and Fixed Disks. These boxes will be selected by default. It is by default that the peripherals are not selected. If you chose to monitor these items you must manually select them.

On Cisco Devices, there will not be any volumes, but other devices might.

Action: Click 'NEXT'

## Step 19.

### Network Sonar Results Wizard

DEVICES > INTERFACES > PORTS > VOLUMES > **IMPORT PREVIEW** > RESULTS

**Import Preview - STUDENT01-VM**

Select devices, interfaces, and volumes that you wish to ignore or import. All ignored items will be removed from this list and will not be found during any future network discovery, manual or scheduled. If you wish to ignore items, do so before importing.

Polling IP Address	Name	Machine Type	Volumes	Polling Method	Interfaces Count	UDT Port Count
10.50.2.1	student01-VM	Windows 10 Workstation	RAM, Virtual Memory, Fixed Disk (3)	WMI	0	0
10.50.2.2	10.50.2.2	Unknown		ICMP	0	0
10.50.2.61	ipv4s2.nmsnil.local	Cisco 3640		SNMP	20	19
10.50.2.62	ipv4s3.nmsnil.local	Cisco 3640		SNMP	20	19
10.50.2.63	ipv6s2.nmsnil.local	Cisco 3640		SNMP	20	19
10.50.2.64	ipv6s3.nmsnil.local	Cisco 3640		SNMP	20	19

BACK IGNORE **IMPORT** CANCEL

Here at the Discovery Wizard, we are given what is to be imported into the database.

Action: Click 'IMPORT'.

## Step 20.

Network Sonar Results Wizard

DEVICES > INTERFACES > PORTS > VOLUMES > IMPORT PREVIEW > RESULTS

**Import Results**

**Importing Interfaces**

92% Imported by Current Phase  
31% Imported Total

Interface FastEthernet1/9 - Fa1/9, Parent Node: ipv6s2.nmsnll.local, Import Status: added to the Orion DB.  
Interface FastEthernet1/10 - Fa1/10, Parent Node: ipv6s2.nmsnll.local, Import Status: added to the Orion DB.  
Interface FastEthernet1/11 - Fa1/11, Parent Node: ipv6s2.nmsnll.local, Import Status: added to the Orion DB.  
Interface FastEthernet1/12 - Fa1/12, Parent Node: ipv6s2.nmsnll.local, Import Status: added to the Orion DB.  
Interface FastEthernet1/13 - Fa1/13, Parent Node: ipv6s2.nmsnll.local, Import Status: added to the Orion DB.  
Interface FastEthernet1/14 - Fa1/14, Parent Node: ipv6s2.nmsnll.local, Import Status: added to the Orion DB.  
Interface FastEthernet1/15 - Fa1/15, Parent Node: ipv6s2.nmsnll.local, Import Status: added to the Orion DB.  
Interface Null0 - Nu0, Parent Node: ipv6s2.nmsnll.local, Import Status: skipped, already exists in Orion DB.  
Interface Vlan1 - VI1, Parent Node: ipv6s2.nmsnll.local, Import Status: added to the Orion DB.  
Interface FastEthernet0/0 - Fa0/0, Parent Node: ipv6s3.nmsnll.local, Import Status: skipped, already exists in Orion DB.  
Interface FastEthernet0/1 - Fa0/1, Parent Node: ipv6s3.nmsnll.local, Import Status: added to the Orion DB.  
Interface FastEthernet1/0 - Fa1/0, Parent Node: ipv6s3.nmsnll.local, Import Status: added to the Orion DB.  
Interface FastEthernet1/1 - Fa1/1, Parent Node: ipv6s3.nmsnll.local, Import Status: added to the Orion DB.  
Interface FastEthernet1/2 - Fa1/2, Parent Node: ipv6s3.nmsnll.local, Import Status: added to the Orion DB.  
Interface FastEthernet1/3 - Fa1/3, Parent Node: ipv6s3.nmsnll.local, Import Status: added to the Orion DB.  
Interface FastEthernet1/4 - Fa1/4, Parent Node: ipv6s3.nmsnll.local, Import Status: added to the Orion DB.  
Interface FastEthernet1/5 - Fa1/5, Parent Node: ipv6s3.nmsnll.local, Import Status: added to the Orion DB.  
Interface FastEthernet1/6 - Fa1/6, Parent Node: ipv6s3.nmsnll.local, Import Status: added to the Orion DB.  
Interface FastEthernet1/7 - Fa1/7, Parent Node: ipv6s3.nmsnll.local, Import Status: added to the Orion DB.  
Interface FastEthernet1/8 - Fa1/8, Parent Node: ipv6s3.nmsnll.local, Import Status: added to the Orion DB.  
Interface FastEthernet1/9 - Fa1/9, Parent Node: ipv6s3.nmsnll.local, Import Status: added to the Orion DB.  
Interface FastEthernet1/10 - Fa1/10, Parent Node: ipv6s3.nmsnll.local, Import Status: added to the Orion DB.  
Interface FastEthernet1/11 - Fa1/11, Parent Node: ipv6s3.nmsnll.local, Import Status: added to the Orion DB.  
Interface FastEthernet1/12 - Fa1/12, Parent Node: ipv6s3.nmsnll.local, Import Status: added to the Orion DB.

**BACK** **FINISH**

If a node has already been discovered, then the database will not add it for the second time. Only new items will be added to the database. After clicking ‘FINISH’, the following graphics will provide the results of your discovery.

Action: Click ‘FINISH’ when complete.



## Welcome to Discovery Central

Get started managing your environment.



### NETWORK DISCOVERY

Scan your network for devices like routers, switches and servers. Volumes on these devices will also be discovered. You can run Network Sonar Discovery once, or create a profile and schedule your discovery to run in the background.

» Learn more about Network Sonar Discovery

6 Nodes are monitored

5 Volumes are monitored

[DISCOVER MY NETWORK](#)

[ADD A SINGLE NODE](#)



### INTERFACE DISCOVERY

Find interfaces on network devices and begin monitoring traffic. You can run Network Sonar Discovery once, or create a profile and schedule your discovery to run in the background.

» Learn more about Network Sonar Discovery

81 Interfaces are monitored

[DISCOVER MY NETWORK](#)



#### AGENT DEPLOYMENT

Add an agent to a monitored device within your network. Agents provide an additional polling method for your devices.

» Learn more about using agents

✓ 1 agents have registered

[DEPLOY AGENT ON MY NETWORK](#)

[DOWNLOAD AGENT INSTALLATION FILES](#)



#### USER DEVICE TRACKER PORT DISCOVERY

Find ethernet ports on network devices and begin monitoring connections.

» Learn more about User Device Tracker Port Discovery

✓ 76 Ports are monitored

[DISCOVER MY PORTS](#)

[ADD PORTS FROM EXISTING ORION NODES](#)



#### USER DEVICE TRACKER ACTIVE DIRECTORY DOMAIN CONTROLLER DISCOVERY

Monitor Active Directory users and keep an eye on network users.

» Learn more about User Device Tracker Active Directory Domain Controller

⌚ 0 Active Directory Domain Controllers are monitored

[DISCOVER MY DC](#)



#### NETFLOW SOURCES

To receive NetFlow data, you must manually configure a network device to export flows. The device and the relevant interfaces must be monitored by Network Performance Monitor for the flows to be displayed.

» Learn more about NetFlow Sources

✓ 4 NetFlow sources are monitored

[HELP ME ENABLE NETFLOW>](#)

This concludes the lab exercise.

# Lab 03 - Custom Properties

The document will show you how to configure custom properties for your various nodes. Custom Properties (CPs) can be very useful in separating, segregating, and identifying your nodes into groups.

When naming CPs, it is best to group them in function sections. If you have a set of CPs which deal with location services or identification try using L# in the beginning of the CPs. If you need a group for Compliance, try using C#. This will help when selecting nodes from the various drop-down menus you will encounter through your SolarWinds development.

Examples of Custom Properties:

L1_Base	L2_Building	L3_Room	L4_Rack
Use Base USAF Geo-Location Code. 4 digits	Use number of the building. 4 digits	Use Room Number. 4 Digits	Use Rack number or location identifier
MPLS	1435	0020	101
TYMX	1814	0100	103
CATD	1712	101B	435C
C1_DeviceType	C2_OS	C3_Function	C4_Application
Router	IOS	Network Device	Sharepoint
Switch	NXOS	Server	SQL
Server	IOS-XE	Firewall	ADDC
Workstation	2016	Workstation	Web Server
	2019		Application Server
	2010		Orion

## Step 1.

The screenshot shows the SolarWinds Orion Summary Home page. At the top, there are navigation links: MY DASHBOARDS, ALERTS & ACTIVITY, REPORTS, and SETTINGS. A dropdown menu for SETTINGS is open, showing options: All Settings (which is highlighted with a red box and has a white cursor icon over it), Network Discovery, Manage Nodes, and My Orion Deployment. Below the menu is a world map with several nodes marked: New York, London, Tokyo, and Singapore. A circular badge on the map says "SAMPLE MAP" and "This map is not live!". To the left of the map, there's a sidebar with four sections: Start managing your NCM nodes (with a "START MANAGING YOUR NCM NODES" button), Set up the NCM Approval System (with a "SET UP THE NCM APPROVAL SYSTEM" button), Review NCM settings (with a "REVIEW NCM SETTINGS" button), and Define global login credentials (with a "DEFINE GLOBAL LOGIN CREDENTIALS" button). At the bottom left of the sidebar is a "REMOVE RESOURCE" button.

Action: Navigate to SETTINGS > All Settings

## Main Settings & Administration



### GETTING STARTED WITH ORION

Discover your network and add the objects you want to monitor in Orion.

» Discovery Central

» Discover Network

» Add Node

» Add VMware, Hyper-V or Nutanix entities



### NODE & GROUP MANAGEMENT

Manage and delete nodes, dependencies and groups. Edit node properties.

» Manage Nodes

» Manage Virtual Devices

» Manage Dependencies

» Manage Groups

» Manage Agents

» Manage Custom Properties

» Manage Pollers

» Manage World Map

» Manage Device Templates

» Manage Hardware Sensors

» Manage Container Services

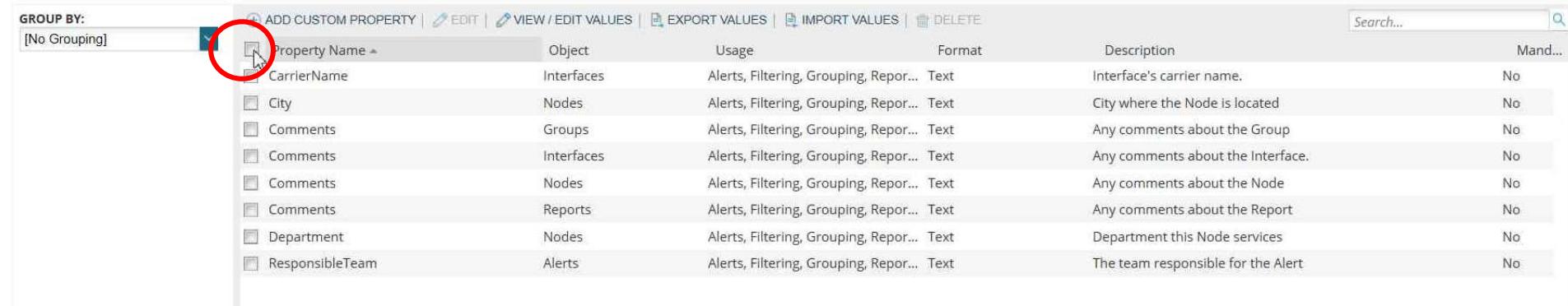
» Manage Orion Maps

Navigation: SETTINGS > All Settings > Main Settings & Administration> NODE & GROUP MANAGEMENT > Manage Custom Properties

## Step 2.

### Manage Custom Properties

Add descriptive properties to objects that you are monitoring. For example, you can add a property called "DeviceFunction" to describe how you use a device within your organization.



GROUP BY:	ADD CUSTOM PROPERTY   EDIT   VIEW / EDIT VALUES   EXPORT VALUES   IMPORT VALUES   DELETE	Search...				
[No Grouping]	Property Name	Object	Usage	Format	Description	Mand...
	CarrierName	Interfaces	Alerts, Filtering, Grouping, Repor... Text	Text	Interface's carrier name.	No
	City	Nodes	Alerts, Filtering, Grouping, Repor... Text	Text	City where the Node is located	No
	Comments	Groups	Alerts, Filtering, Grouping, Repor... Text	Text	Any comments about the Group	No
	Comments	Interfaces	Alerts, Filtering, Grouping, Repor... Text	Text	Any comments about the Interface.	No
	Comments	Nodes	Alerts, Filtering, Grouping, Repor... Text	Text	Any comments about the Node	No
	Comments	Reports	Alerts, Filtering, Grouping, Repor... Text	Text	Any comments about the Report	No
	Department	Nodes	Alerts, Filtering, Grouping, Repor... Text	Text	Department this Node services	No
	ResponsibleTeam	Alerts	Alerts, Filtering, Grouping, Repor... Text	Text	The team responsible for the Alert	No

Action: Here we are going to delete the native CPs and develop our own. Select the box to highlight all CPs.

## Step 3.

### Manage Custom Properties

Add descriptive properties to objects that you are monitoring. For example, you can add a property called "DeviceFunction" to describe how you use a device within your organization.



GROUP BY:	ADD CUSTOM PROPERTY   EDIT   VIEW / EDIT VALUES   EXPORT VALUES   IMPORT VALUES   DELETE	Search...				
[No Grouping]	Property Name	Object	Usage	Format	Description	Mand...
	CarrierName	Interfaces	Alerts, Filtering, Grouping, Repor... Text	Text	Interface's carrier name.	No
	City	Nodes	Alerts, Filtering, Grouping, Repor... Text	Text	City where the Node is located	No
	Comments	Groups	Alerts, Filtering, Grouping, Repor... Text	Text	Any comments about the Group	No
	Comments	Interfaces	Alerts, Filtering, Grouping, Repor... Text	Text	Any comments about the Interface.	No
	Comments	Nodes	Alerts, Filtering, Grouping, Repor... Text	Text	Any comments about the Node	No
	Comments	Reports	Alerts, Filtering, Grouping, Repor... Text	Text	Any comments about the Report	No
	Department	Nodes	Alerts, Filtering, Grouping, Repor... Text	Text	Department this Node services	No
	ResponsibleTeam	Alerts	Alerts, Filtering, Grouping, Repor... Text	Text	The team responsible for the Alert	No

Action: Highlighted CPs will be selected for deletion.  
Click 'DELETE'.

#### Step 4.



Action: Click the “DELETE” button to delete and remove CPs.

#### Step 5.

A screenshot of a web-based application titled "Manage Custom Properties". The header includes buttons for "ADD CUSTOM PROPERTY", "EDIT", "VIEW / EDIT VALUES", "EXPORT VALUES", "IMPORT VALUES", and "DELETE". A red arrow points to the "ADD CUSTOM PROPERTY" button. Below the header is a search bar and a table with columns: GROUP BY, Object, Usage, Format, Description, and Mand... (partially visible). The table shows a single row with "[No Grouping]" under GROUP BY and "No properties to display" under Object. The "ADD CUSTOM PROPERTY" button is located at the top left of the table area.

Action: Select “ADD CUSTOM PROPERTY”.

## Step 6.

### Add Custom Property



### Add Custom Property



Here you can create CPs for different object types. For our purposes we will be using Nodes as our object type. Click 'NEXT'.

## Step 7.

SELECT OBJECT > CHOOSE PROPERTIES > ASSIGN VALUES >

Create your own custom property, or choose a template from the list on the left.

**Property Templates**

- < Custom >
- AssetTag
- SerialNumber
- Comments
- Region
- Building
- Department
- Floor
- Closet
- Cabinet
- Rack
- Address
- City
- State
- Country
- ZipCode
- PostalCode
- ...

**Select Property**

Property Name:  No spaces allowed in this field

Description:

Format:  Any alpha and numeric text (up to 400 characters). [Edit](#)

Required property:  Value must be specified

Restrict values:  Create a drop-down list of values for this property. Admins can add to this list.

Value 1: Router

Value 2: Switch

Value 3: Firewall

Value 4: Server

Value 5: Printer

Usage:

Select how this property will be used:

Alerts

Filtering

Grouping

Reports

Object Details Views  
(Includes details pages for nodes, interfaces, volumes etc.)

Asset Inventory

This screen is where we identify our CP. We will need to fill out this page to create the CP.

Action:

**56** | Page

Lab 03 –Custom Properties

Property Name: Select a Property name without using any spaces.

Description: Best Practices dictate the use of a helpful description. This will allow everyone coming in behind you to see why this CP was created. Use the description box please.

Format: Various formats are available to you here. We will be using Text today.

Required Property: I like to use this selection to force my folks to always fill this field in, so data is accurate (to an extent). You may add nodes through the discovery processes, but you will not be able to edit node properties without having this field filled out.

Restrict Values: These values will be shown in your dropdown box for selection. If you need to add a value, there will be an option to do so at any time at the bottom of your drop-down menu.

Usage: Go ahead and select all for now. It will help down the road if you want to get further along in your SolarWinds development.

The table below is a list of Custom Properties that will be configured in this lab.

L1_Base	L2_Building	L3_Room	L4_Rack
Use Base USAF Geo-Location Code. 4 digits	Use number of the building. 4 digits	Use Room Number. 4 Digits	Use Rack number or location identifier
MPLS	1435	0020	101
TYMX	1814	0100	103
CATD	1712	101B	435C
C1_DeviceType	C2_OS	C3_Function	C4_Application
Router	IOS	Network Device	Sharepoint
Switch	NXOS	Server	SQL
Server	IOS-XE	Firewall	ADDC
Workstation	2016	Workstation	Web Server
	2019		Application Server
	2010		Orion

Click ‘NEXT’ when done.

## Step 8.

### Add Custom Property

SELECT OBJECT > CHOOSE PROPERTIES > **ASSIGN VALUES**

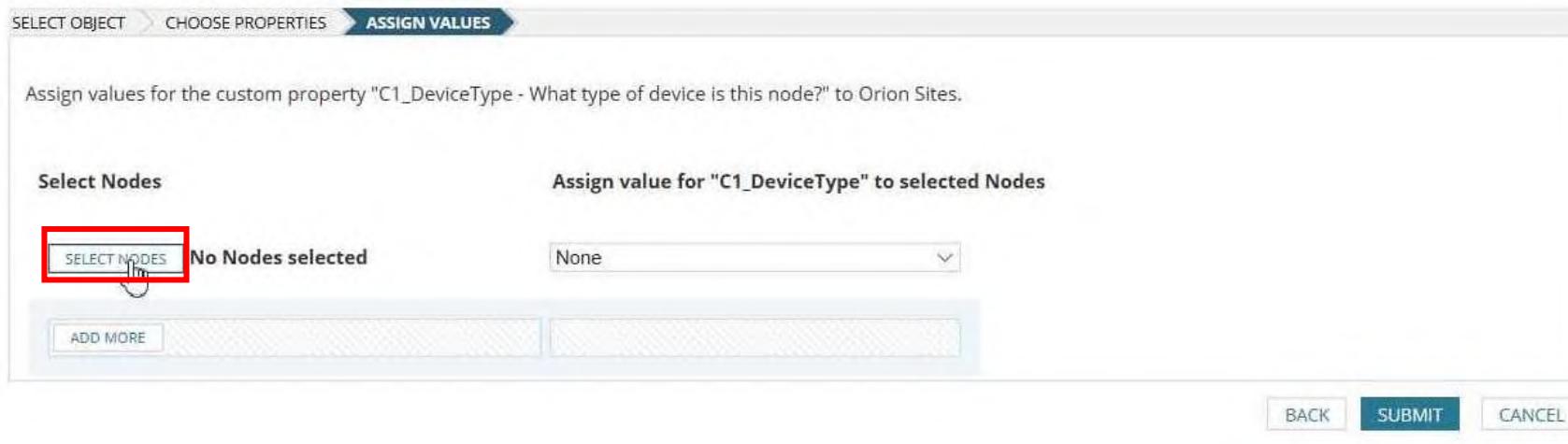
Assign values for the custom property "C1\_DeviceType - What type of device is this node?" to Orion Sites.

Select Nodes      Assign value for "C1\_DeviceType" to selected Nodes

**SELECT NODES**      No Nodes selected      None

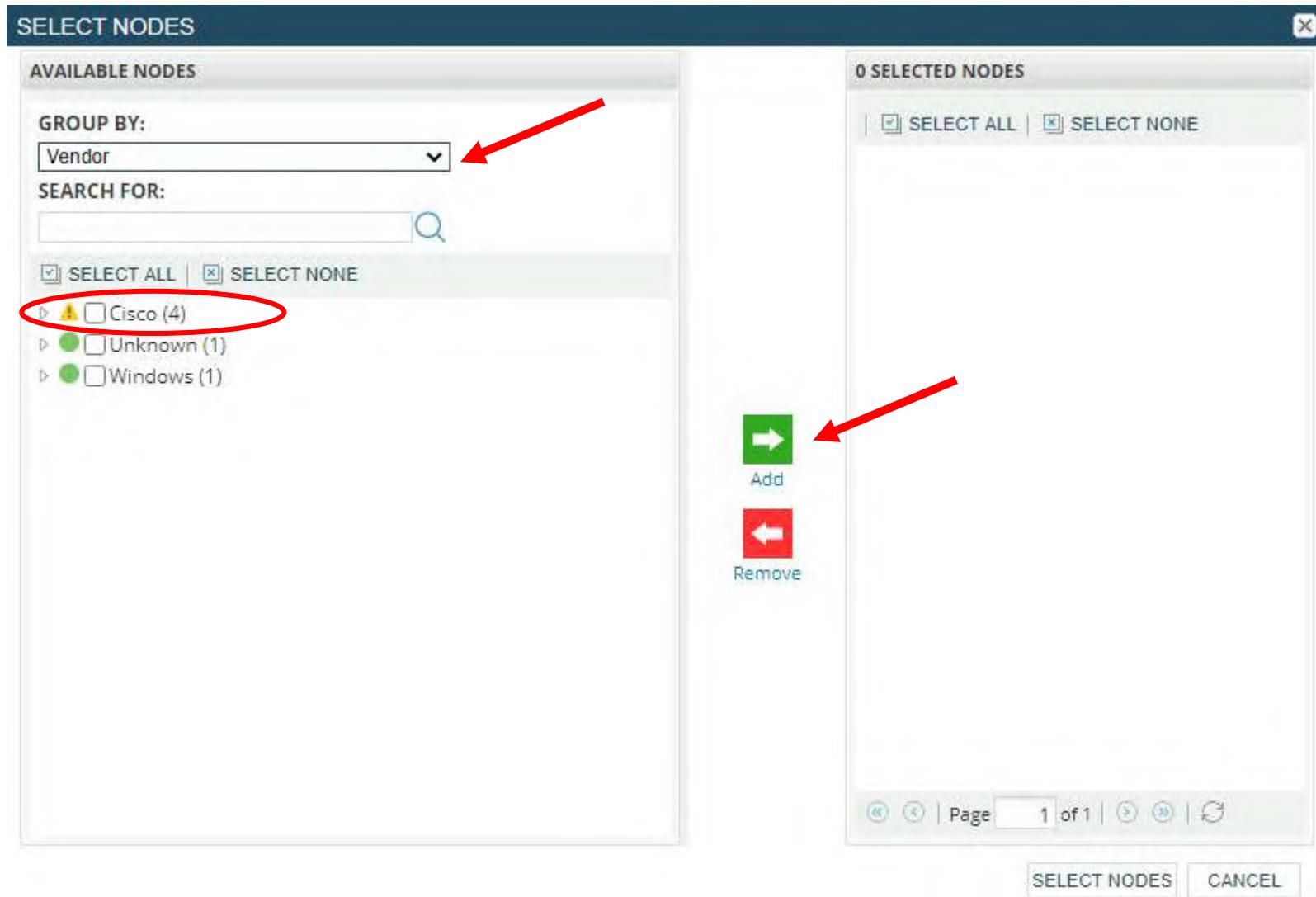
**ADD MORE**

BACK      SUBMIT      CANCEL



Action: Click on 'SELECT NODES'.

## Step 9.

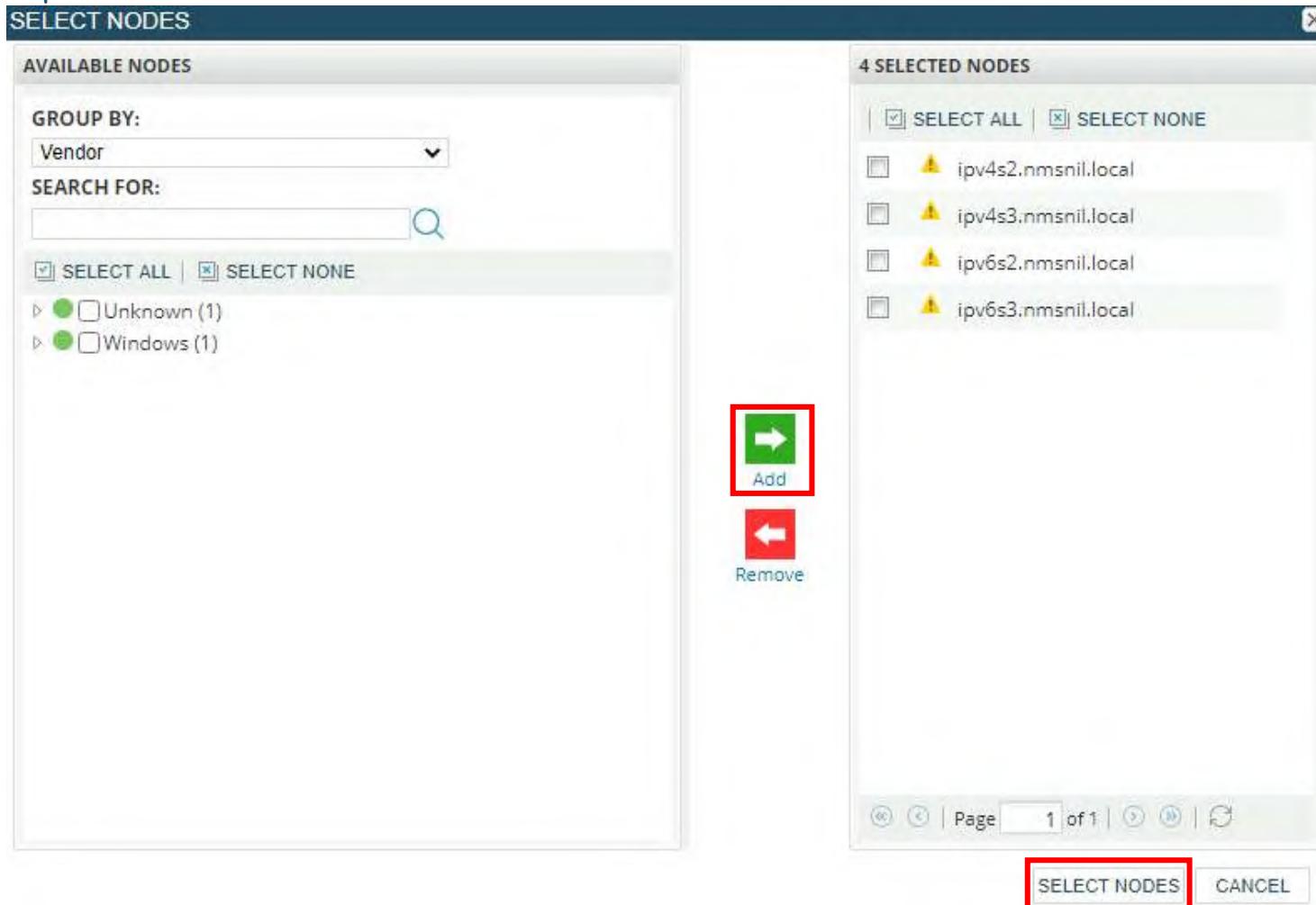


Action: On ‘SELECT NODES’ window, locate your Cisco devices in the box below. You may choose to group your nodes by ‘STATUS’ or any number of options in the GROUP BY box. Use the drop-down menu to review options.

Action: Select the Vendor option.

## Step 10.

### SELECT NODES



Notice: Do you see the Group By: heading on the left panel? This is a clue for you that your custom properties could be used to select a group of nodes for using your new CP. Key an eye open for this and you will see the power of CPs.

Action: On the 'SELECT NODES' window, moving selected nodes from Available Nodes left panel to selected right panel by clicking on the 'ADD' button.

## Step 11.

### Add Custom Property

SELECT OBJECT > CHOOSE PROPERTIES > ASSIGN VALUES

Assign values for the custom property "C1\_DeviceType - What type of device is this node?" to Orion Sites.

Select Nodes      Assign value for "C1\_DeviceType" to selected Nodes

SELECT NODES 4 Nodes selected      None  ←

Action: Use this drop-down menu to assign your chosen nodes to a CP value.

### Add Custom Property

SELECT OBJECT > CHOOSE PROPERTIES > ASSIGN VALUES

Assign values for the custom property "C2\_OS - What is the operating systems running on this node?" to Orion Sites.

Select Nodes      Assign value for "C2\_OS" to selected Nodes

SELECT NODES 4 Nodes selected      IOS  ×

SELECT NODES 1 Nodes selected      2016  ×

Here we have added our Windows Node and selected the 2016 variable to the device.

Click on 'SUBMIT'.

## Step 12.

### Manage Custom Properties

Add descriptive properties to objects that you are monitoring. For example, you can add a property called "DeviceFunction" to describe how you use a device within your organization.

Manage Custom Properties						
Successfully assigned values for P4_Email. » Show assignments						
GROUP BY:						Search...
[No Grouping]	+ ADD CUSTOM PROPERTY	EDIT	VIEW / EDIT VALUES	EXPORT VALUES	IMPORT VALUES	DELETE
	Property Name	Object	Usage	Format	Description	Mand...
	C1_DeviceType	Nodes	Alerts, Filtering, Grouping, Repor...	Text	What type of device is this node?	No
	C2_OS	Nodes	Alerts, Filtering, Grouping, Repor...	Text	What is the operating system of this node?	No
	C3_Function	Nodes	Alerts, Filtering, Grouping, Repor...	Text	What IT function does this device serve?	No
	C4_Application	Nodes	Alerts, Filtering, Grouping, Repor...	Text	What application does this node service?	No
	L1_Base	Nodes	Alerts, Filtering, Grouping, Repor...	Text	What base does this device reside on?	No
	L2_Building	Nodes	Alerts, Filtering, Grouping, Repor...	Text	What building will house this device?	No
	L3_Room	Nodes	Alerts, Filtering, Grouping, Repor...	Text	What room is this device in?	No
	L4_Rack	Nodes	Alerts, Filtering, Grouping, Repor...	Text	Which rack or desk location is this device?	No
	M1_PollingMethod	Nodes	Alerts, Filtering, Grouping, Repor...	Text	Which polling method should this node use?	No
	M2_CredentialSet	Nodes	Alerts, Filtering, Grouping, Repor...	Text	Which set of credentials should this node use?	No
	M3_PollingEngine	Nodes	Alerts, Filtering, Grouping, Repor...	Text	Which polling engine should node use?	No
	P1_Unit	Nodes	Alerts, Filtering, Grouping, Repor...	Text	Which unit or comm squadron does this contact belong?	No
	P2_Name	Nodes	Alerts, Filtering, Grouping, Repor...	Text	What is the name of the contact?	No
	P3_Phone	Nodes	Alerts, Filtering, Grouping, Repor...	Text	What is the phone number for this contact?	No
	P4_Email	Nodes	Alerts, Filtering, Grouping, Repor...	Text	What is the email address for this contact?	No
«   »   Page		1 of 1	»   »   »	NUMBER OF ITEMS PER PAGE:	20	Displaying properties 1 - 15 of 15

Action: Association of nodes to Custom Property values.

Success: You have a new CP ready for action.

Displaying Node Database and Custom Properties

This section will add your Custom Properties value to a node outside the Custom Property creation process.

## Step 13.

The screenshot shows the SolarWinds Orion interface. At the top, there is a navigation bar with links for 'MY DASHBOARDS', 'ALERTS & ACTIVITY', 'REPORTS', 'SETTINGS', 'ADMIN (LOGOUT)', and 'HELP'. The 'SETTINGS' menu is open, showing 'All Settings', 'Network Discovery', and 'Manage Nodes' (which is highlighted with a red box). Below this, the 'Manage Custom Properties' page is displayed. The page title is 'Manage Custom Properties' and it includes a sub-header 'Add descriptive properties to objects that you are monitoring. For example, you can add "My Location" or "My Function" to describe how you use a device within your organization.' A table lists various custom properties with columns for 'Property Name', 'Object', 'Usage', 'Format', 'Description', and 'Mand...'. The table contains 15 rows, each with a checkbox in the first column. The last row is 'P4\_EmailAddress'. At the bottom of the table, there are pagination controls ('Page 1 of 1'), a 'NUMBER OF ITEMS PER PAGE' dropdown set to '20', and a note 'Displaying properties 1 - 15 of 15'.

Manage Custom Properties					
Add descriptive properties to objects that you are monitoring. For example, you can add "My Location" or "My Function" to describe how you use a device within your organization.					
GROUP BY: [No Grouping]					
<a href="#">ADD CUSTOM PROPERTY</a>   <a href="#">EDIT</a>   <a href="#">VIEW / EDIT VALUES</a>   <a href="#">EXPORT VALUES</a>   <a href="#">IMPORT VALUES</a>   <a href="#">DELETE</a>					
Property Name	Object	Usage	Format	Description	Mand...
C1_DeviceType	Nodes	Alerts, Filtering, Grouping, Repor...	Text	What type of device is this node?	No
C2_OS	Nodes	Alerts, Filtering, Grouping, Repor...	Text	What type of OS is this node using?	No
C3_Function	Nodes	Alerts, Filtering, Grouping, Repor...	Text	What function does this device provide for the Organization?	No
C4_Application	Nodes	Alerts, Filtering, Grouping, Repor...	Text	What application does this node serve?	No
L1_Base	Nodes	Alerts, Filtering, Grouping, Repor...	Text	Which base does this node reside?	No
L2_Building	Nodes	Alerts, Filtering, Grouping, Repor...	Text	Which building does this node reside?	No
L3_Room	Nodes	Alerts, Filtering, Grouping, Repor...	Text	Which room does this node reside?	No
L4_Rack	Nodes	Alerts, Filtering, Grouping, Repor...	Text	Which rack does this node reside?	No
M1_PollingMethod	Nodes	Alerts, Filtering, Grouping, Repor...	Text	Which polling method should this node be using?	No
M2_CredentialSet	Nodes	Alerts, Filtering, Grouping, Repor...	Text	What is the credential set used for this node?	No
M3_PollingEngine	Nodes	Alerts, Filtering, Grouping, Repor...	Text	Which polling engine is this node assigned to?	No
P1_Unit	Nodes	Alerts, Filtering, Grouping, Repor...	Text	Which unit would be the POC for this node?	No
P2_Name	Nodes	Alerts, Filtering, Grouping, Repor...	Text	What is the name of this POC?	No
P3_Phone	Nodes	Alerts, Filtering, Grouping, Repor...	Text	What is the phone number for this POC?	No
P4_EmailAddress	Nodes	Alerts, Filtering, Grouping, Repor...	Text	What is the email address of this POC?	No

Navigation: SETTINGS > Manage Nodes

## Step 14.

The screenshot shows the 'Manage Nodes' interface. At the top, there's a search bar with 'Show: Nodes' and a 'SEARCH' button. Below the search bar, a message says 'You can switch to the new Manage Entities page.' with a '» Show me' link. The main area has a 'Group by:' dropdown set to 'Vendor' and a 'Windows (1)' node listed. The header includes buttons for 'ADD NODE', 'CUSTOM PROPERTY EDITOR', 'EDIT PROPERTIES', 'LIST RESOURCES', 'ASSIGN POLLERS', 'MAINTENANCE MODE', 'MORE ACTIONS', and 'DELETE'. The 'MORE ACTIONS' button is circled in red. The table below has columns for 'Name', 'Polling IP Address', and 'Status'. The 'Name' column is sorted by 'Name'.

We are looking to expand our view of the Custom Properties in the Manage Nodes view.

Action: Click on the blue arrows on the upper right-hand corner of this screen as shown above.

## Step 15.

This screenshot shows the 'Node Custom Properties' dialog box. On the left, there's a list of checked custom properties: C1\_DeviceType, C2\_OS, C3\_Function, C4\_Application, L1\_Base, L2\_Building, L3\_Room, L4\_Rack, M1\_PollingMethod, M2\_CredentialSet, M3\_PollingEngine, P1\_Unit, P2\_Name, P3\_Phone, and P4\_EmailAddress. At the bottom right are two buttons: 'OK' (highlighted with a red box) and 'CANCEL'.

Action: Select all the Custom Properties you had configured in the previous Lab. Click 'OK'.

## Step 16.

The screenshot shows the 'Manage Nodes' interface. At the top, there's a search bar with 'Show: Nodes' and a 'SEARCH' button. Below the search bar is a message: 'You can switch to the new Manage Entities page.' with a 'Show me' link. A 'Group by:' dropdown is set to 'Vendor'. The main area displays a table with one row. The table has columns for 'Name', 'Polling IP Address', and 'Status'. The first row shows 'DESKTOP-514M24G' with IP '255.255.255.255' and status 'Node status is Unknown.'. Above the table are several buttons: 'ADD NODE', 'CUSTOM PROPERTY EDITOR', 'EDIT PROPERTIES', 'LIST RESOURCES', 'ASSIGN POLLERS', 'MAINTENANCE MODE', 'MORE ACTIONS', and 'DELETE'. To the right of the table, there are links for various custom properties: C1\_DeviceType (CP), C2\_OS (CP), C3\_Function (CP), C4\_Application (CP), L1\_Base (CP), L2\_Building (CP), L3\_Room (CP), and L4\_Rack (CP).

Here we see all our Custom Properties displayed for our current node selected. From here we will need to fill in the blanks appropriately.

## Step 17.

To continue with this exercise, review all nodes and populate all Custom Properties for those nodes.

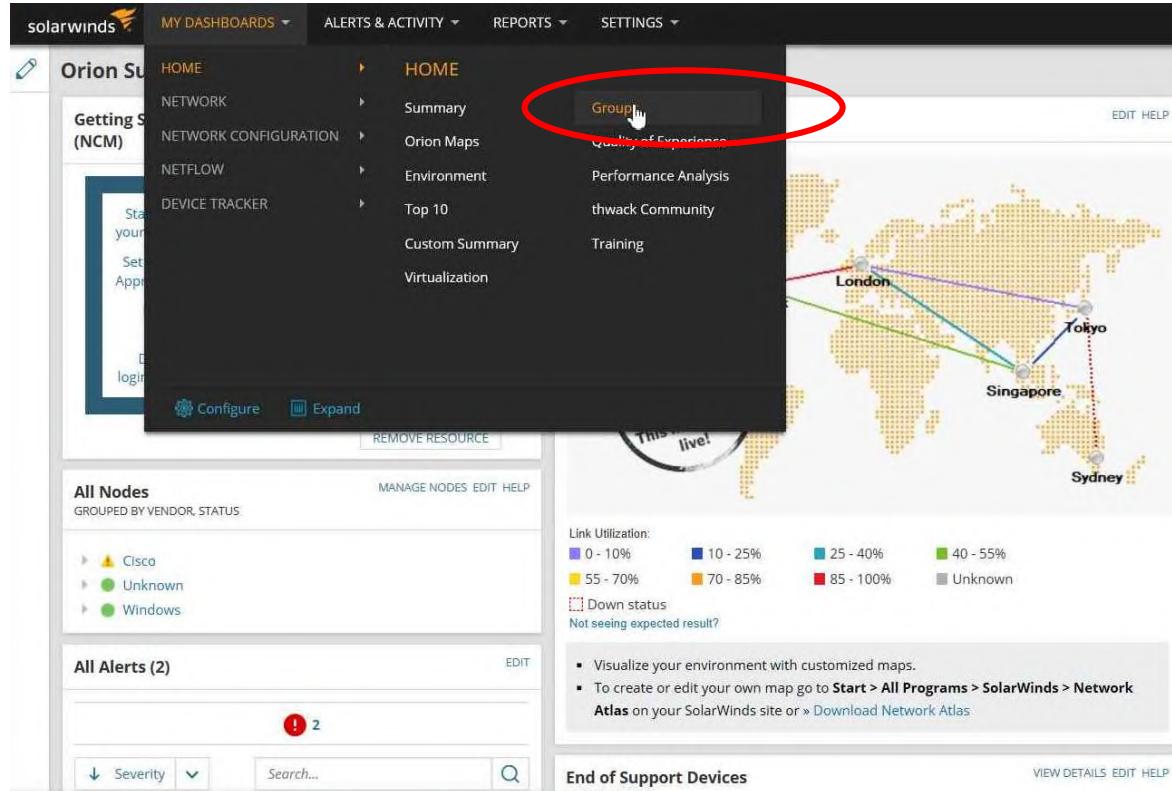
This concludes the lab exercise.

This page left intentionally blank.

# Lab 04 - Groups

In this lab we will create a group with a dynamic query based of using a custom property.

## Step 1.



The screenshot shows the SolarWinds Orion NPM interface. At the top, there's a navigation bar with 'MY DASHBOARDS', 'ALERTS & ACTIVITY', 'REPORTS', and 'SETTINGS'. Below this is a left sidebar with sections like 'Orion Summary', 'Getting Started (NCM)', 'NETWORK', 'NETWORK CONFIGURATION', 'NETFLOW', 'DEVICE TRACKER', and 'Virtualization'. A red circle highlights the 'Groups' option under the 'HOME' menu, which is currently expanded. The main area features a world map with network links between cities like London, Tokyo, Singapore, and Sydney. Below the map is a section titled 'Link Utilization' with a legend and a note about 'Down status'. At the bottom, there are sections for 'All Nodes', 'All Alerts (2)', and 'End of Support Devices'.

Action: Navigate to MY DASHBOARDS > HOME > Groups. The upper left most widget is called Group Summary. Click on 'Manage Groups'.

## Step 2.

### Groups Summary

All Groups      MANAGE GROUPS EDIT HELP  
NO GROUPING APPLIED

#### GETTING STARTED: CREATE GROUPS

Use groups to logically organize monitored objects.

Organize monitored objects on the basis of shared properties or conditions. For example, create a group to include all objects of a designated status or create a group containing all monitored network objects in a specific physical location.

**CREATE A GROUP**

### Map

EDIT HELP

Billing

Order Processing

Order Fulfilment Systems

- Visualize your environment with customized maps.
- To create or edit your own map go to **Start > All Programs > SolarWinds > Network Atlas** on your SolarWinds site or » [Download Network Atlas](#)

Action: To create a new group, click on the 'CREATE A GROUP' button as seen above.

### Step 3.

Add New Group

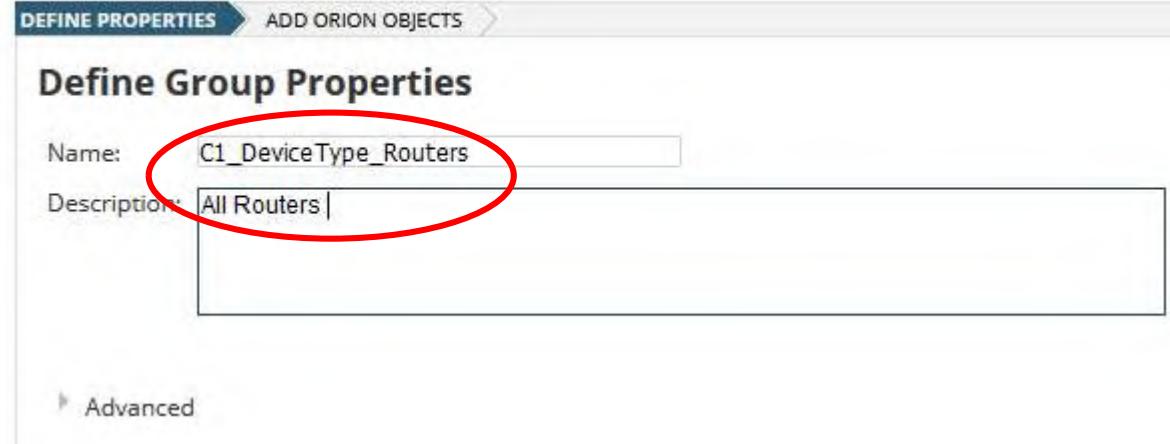
DEFINE PROPERTIES > ADD ORION OBJECTS

Define Group Properties

Name: C1\_DeviceType\_Routers

Description: All Routers |

Advanced



Here we have two data input windows which should be filled in.

Action: Provide a meaningful descriptive name for the group. It is best to use the custom properties that are going to be used in the dynamic queries.  
Type 'C1\_DeviceType\_Router'.

Action: Provide a meaningful & descriptive sentence which describes the purpose of this group.  
Type 'This group will contain all Routers.'

If you put "Temp" or "Test" in these boxes, do not expect to keep it long. Testing and Temporary items should be removed or modified with 48 hours. You do not want a system full of Testing or Temporary items.

## Step 4.

### Add & Remove Orion Objects - C1\_DeviceType\_L2SW

Add Orion objects to your group by dragging them from the left to the right panel or select multiple objects using checkboxes and use "Add Objects to Group" button. Dynamic query objects can be used to populate groups dynamically.

The screenshot shows the 'Add & Remove Orion Objects' dialog box. On the left, under 'AVAILABLE OBJECTS', there are filters for 'SHOW ONLY: Nodes' and 'GROUP BY: Vendor'. A search bar and 'SEARCH FOR:' field are also present. Below these are 'SELECT ALL' and 'SELECT NONE' checkboxes. A list of objects is shown: Cisco (1), Unknown (1), and Windows (1). On the right, under 'C1\_DEVICETYPE\_L2SW', there is an 'ADD DYNAMIC QUERY' button, which is highlighted with a red box. Other buttons include 'EDIT DYNAMIC QUERY', 'VIEW DYNAMIC QUERY RESULTS', 'SELECT ALL', and 'SELECT NONE'. At the bottom of the dialog are 'SUBMIT' and 'CANCEL' buttons.

You have the option to manually add nodes or use a dynamic query. Manually adding nodes can be an administrative burden on your team and will not provide the most accurate count of nodes. The use of Dynamic Query is the best way to go about organizing your groups.

Action: Click on 'ADD DYNAMIC QUERY'.

## Step 5.

### Build Dynamic Query

Dynamic query objects can be added to groups. Each dynamic query can only include one type of Orion object (node, application, etc.)

The screenshot shows a configuration interface for building a dynamic query. At the top, there is a field labeled "Dynamic query object name" containing the value "C1\_DeviceType\_Router". Below this, a section titled "Dynamic query:" contains three dropdown menus. The first menu is set to "Orion Object", the second to "is", and the third to "Node". Under "Orion Object", the value "C1\_Device Type" is selected. Under "Node", the value "Router" is selected. There is also a small trash can icon next to the "Router" selection. At the bottom of the interface are three buttons: "PREVIEW", "SAVE" (which is highlighted in blue), and "CANCEL".

Action: Dynamic query object name should be mentioning the basis of the query. Try to use the name of the Custom Property or type of node you wish to have in this group.

## Step 6.

### Build Dynamic Query

Dynamic query objects can be added to groups. Each dynamic query can only include one type of Orion object (node, application, etc.)

The screenshot shows the 'Build Dynamic Query' interface. At the top, there is a text input field labeled 'Dynamic query object name:' containing 'C1\_DeviceType\_Router'. Below it, a section labeled 'Dynamic query:' has two dropdown menus: 'Orion Object' and 'Node'. The 'Orion Object' dropdown is set to 'C1\_DeviceType' and the 'Node' dropdown is set to 'Router'. To the right of these dropdowns is a trash bin icon. A red arrow points to the 'is' dropdown menu, which is open and lists several options: 'Caption', 'Contact', 'Description', 'DNS', 'External', 'Has Dynamic IP', 'Integrations', 'Integrations - Description', 'IOS Image', 'IOS Version', 'IP Address', 'IP Version', 'IP\_Address', 'Is OrionServer', 'IsServer', 'L1\_Location', 'L2\_Room', and 'Location'. The 'Caption' option is highlighted with a blue selection bar.

Action: For this lab we will be using the groups based on “Nodes”. If you click on the Nodes drop down menu there are many other options to use.

Action: Click on ‘ADD CONDITION’. This allow us to use the custom properties already configured on the system to group our nodes.

## Step 7.

### Build Dynamic Query

Dynamic query objects can be added to groups. Each dynamic query can only include one type of Orion object (node, application, etc.)

The screenshot shows a 'Build Dynamic Query' dialog box. At the top, there is a field labeled 'Dynamic query object name:' containing 'C1\_DeviceType\_Router'. Below this, the 'Dynamic query:' section is visible, featuring three dropdown menus: 'Orion Object' set to 'Node', 'is' as the Boolean identifier, and 'C1\_DeviceType' as the string or variable. A red box highlights the entire 'Dynamic query:' section. At the bottom of the dialog are three buttons: 'PREVIEW', 'SAVE' (which is highlighted in blue), and 'CANCEL'.

The next field in the query is the Boolean identifier. Simply choose what best fits the criteria. In this Lab, we will be using the 'is' operand because we are looking for a defined variable. Last field in this query is the string or variable we are grouping on.

Actions:

- Select in first query field 'C1\_DeviceType'
- Select in the second query field 'is';
- Type in the third query field 'Router'
- Click on 'SAVE' when done.

## Step 8.

### Add New Group

DEFINE PROPERTIES ADD ORION OBJECTS

Add Orion Objects to your new group

Add Orion objects to your group by dragging them from the left to the right panel or select multiple objects using checkboxes and use "Add Objects to Group" button. Dynamic query objects can be used to populate groups dynamically.

AVAILABLE OBJECTS

SHOW ONLY: Nodes

GROUP BY: Vendor

SEARCH FOR:

SELECT ALL |  SELECT NONE

- CANON INC. (1)
- Fortinet, Inc. (3)
- Meraki Networks, Inc. (1)
- QNAP SYSTEMS, INC (2)
- Unknown (36)
- Windows (7)

C1\_DEVICETYPE\_ROUTERS

+ ADD DYNAMIC QUERY | EDIT DYNAMIC QUERY | VIEW DYNAMIC QUERY RESULTS |  SELECT ALL |  SELECT NONE

C1\_DeviceType\_Router

Add to Group | Remove

We have completed building our dynamic query.

Action: Click 'CREATE GROUP' in the bottom right hand corner of the screen.

## Step 9.

### Manage Groups

Groups may contain any number of Orion objects. You may alert and report on groups. Groups also have summary and detail views.

Group by:	Parent (Groups)	View mode:	All Groups							
				ADD NEW GROUP	EDIT PROPERTIES	ADD & REMOVE OBJECTS	VIEW DYNAMIC QUERY RESULTS	DELETE		
	Name				Object type	Description				
<input checked="" type="checkbox"/>	C1_DeviceType_Routers				Group	All Routers				
<input type="checkbox"/>	C1_DeviceType_Router				Dynamic Query					
<input type="checkbox"/>	C1_DeviceType_Servers				Group	All Servers in the Organization				
<input type="checkbox"/>	C1_DeviceType_Servers				Dynamic Query					
<input type="checkbox"/>	C1_DeviceType_Switches				Group	All Layer 2 Switches in Organization				
<input type="checkbox"/>	C1_DeviceType_Switches				Dynamic Query					
<input type="checkbox"/>	C3_Function_SolarWinds				Group	All SolarWinds Servers				
<input type="checkbox"/>	C3_Function_SolarWinds				Dynamic Query					

SolarWinds will return us back to the Manage Groups dashboard and our new group will be in the list sorted by Alphabetical order.

For the rest of this lab create the following Groups:

- All Routers
- All Windows

This concludes the lab exercise.

This page intentionally left blank.

# Lab 05 - Creating a Dashboard/View

This lab will enable the student to create a view, place it in the menu bar, and then allow the user to access a customized Dashboard.

## Step 1.

The screenshot shows the SolarWinds Orion interface. At the top, there is a navigation bar with links for 'MY DASHBOARDS', 'ALERTS & ACTIVITY', 'REPORTS', and 'SETTINGS'. The main content area is titled 'Main Settings & Administration'. It features three main sections: 'GETTING STARTED WITH ORION', 'NODE & GROUP MANAGEMENT', and 'ALERTS & REPORTS'. Each section contains several sub-links for managing network objects and dependencies.

- GETTING STARTED WITH ORION**
  - » Discovery Central
  - » Add VMware vCenter or Hyper-V devices
  - » Discover Network
  - » Add a Transaction Monitor
  - » Add Node
  - » Add Storage Device
- NODE & GROUP MANAGEMENT**
  - » Manage Nodes
  - » Manage Groups
  - » Manage Storage Objects
  - » Manage Device Templates
  - » Manage Orion Maps
  - » Manage Virtual Devices
  - » Manage Agents
  - » Manage Pollers
  - » Manage Hardware Sensors
  - » Manage Dependencies
  - » Manage Custom Properties
  - » Manage World Map
  - » Manage Container Services
- ALERTS & REPORTS**
  - » Manage Alerts
  - » Configure Default Send Email Action
  - » Manage Reports
  - » ServiceNow Instances
  - » Manage SMTP Servers

Let us start from the Settings Page once more. As you have noticed this is a common starting point for all administrative actions within SolarWinds.  
Action: Scroll down to the bottom of the Settings Page.

## Step 2.

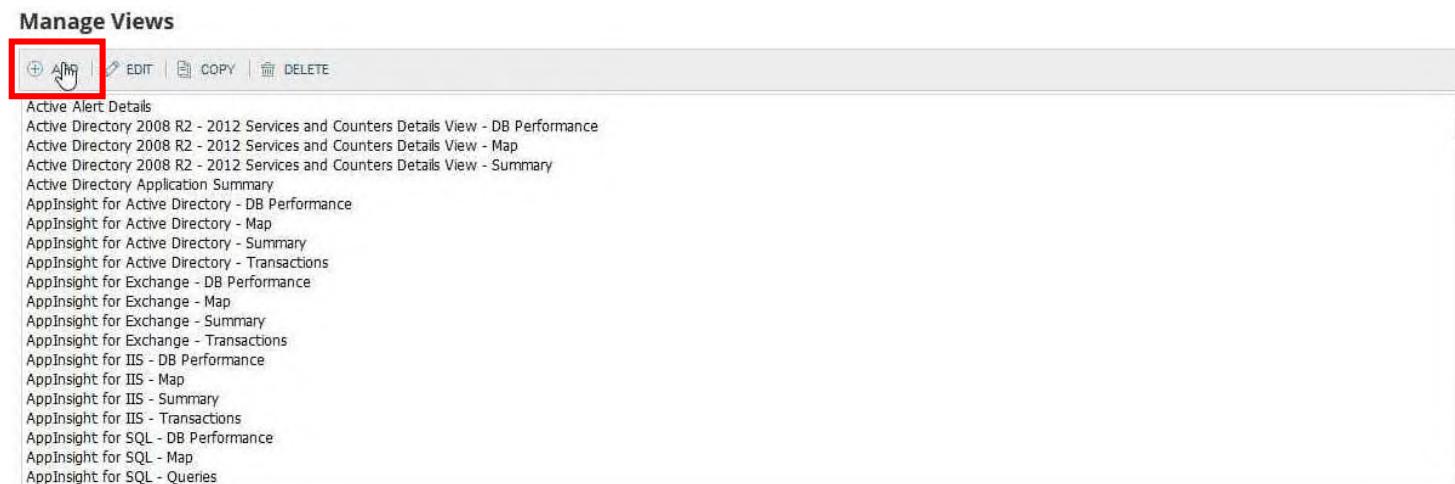


The screenshot shows a web-based interface titled 'VIEWS'. At the top left is a small icon of a computer monitor with two windows. To its right, the word 'VIEWS' is displayed in large, bold, black capital letters. Below this, a sub-header reads 'Customize content of views or create new views'. Underneath, there are several navigation links: '» Manage Views' (which is circled in red), '» Add New View', '» Views by Device Type', '» Views by Application Type', and '» Created NOC Views'.

The View section is where we will begin our configuration.

Action: Click 'Manage Views'.

## Step 3.



The screenshot shows a window titled 'Manage Views'. At the top, there is a toolbar with several icons: a plus sign for 'ADD', a magnifying glass for 'SEARCH', 'EDIT', 'COPY', and 'DELETE'. The 'ADD' button is highlighted with a red box and has a cursor icon pointing at it. The main area of the window lists numerous pre-built views, each consisting of a brief description followed by a hyphen and a longer, more detailed name. The list includes:

- Active Alert Details
- Active Directory 2008 R2 - 2012 Services and Counters Details View - DB Performance
- Active Directory 2008 R2 - 2012 Services and Counters Details View - Map
- Active Directory 2008 R2 - 2012 Services and Counters Details View - Summary
- Active Directory Application Summary
- AppInsight for Active Directory - DB Performance
- AppInsight for Active Directory - Map
- AppInsight for Active Directory - Summary
- AppInsight for Active Directory - Transactions
- AppInsight for Exchange - DB Performance
- AppInsight for Exchange - Map
- AppInsight for Exchange - Summary
- AppInsight for Exchange - Transactions
- AppInsight for IIS - DB Performance
- AppInsight for IIS - Map
- AppInsight for IIS - Summary
- AppInsight for IIS - Transactions
- AppInsight for SQL - DB Performance
- AppInsight for SQL - Map
- AppInsight for SQL - Queries

Here we see a large number of pre-built Views to choose. We will be creating our own today.

Action: Click on 'ADD' in the Manage Views window menu bar.

## Step 4.

Add New View

Name of New View  

Type of View  



VIEW TYPES:

SUMMARY

Summary views display network-wide information.

NODE DETAILS

Node Details Views display information about a single node.

VOLUME DETAILS

Volume Details views display information about a single volume.

ACTIVE ALERT DETAILS

Active Alert Details views display information about single active alert.

CLOUD SUMMARY VIEW

QOE APPLICATION DETAILS

Shows details of QoE Application

QOE APPLICATION CATEGORY DETAILS

Shows details of QoE Application Category

The first thing we need to do is to provide the view with a name. This name will be used in the display of your My Dashboards drop down.

Action: Add a name to the field. Type ‘CFP Dashboard’.

We have a choice on the type of view, but for our purposes here we will stick with Summary View.

Action: Click ‘Submit’ when complete.

## Step 5.

### Customize CFP Dashboard

Name

Type of view: **Summary**

#### LEFT NAVIGATION

Is there a lot of content on this view? Break it up into smaller pages with tabs on the left.

Enable left navigation

The screenshot shows the 'Customize CFP Dashboard' interface. At the top, there's a 'Name' field with 'CFP Dashboard' and a 'UPDATE' button. Below it, 'Type of view' is set to 'Summary'. Under 'LEFT NAVIGATION', there's a tip about using tabs on the left for large content areas, followed by a checkbox for 'Enable left navigation'. Below this, there are two columns labeled 'COLUMN 1' and 'COLUMN 2', each containing a 'Resources' section. Column 1 has a width of 500 px, and Column 2 has a width of 400 px. To the right, there's a third column area with a 'TIP: You can use up to 6 columns' message and an 'ADD NEW COLUMN' button.

#### NOC VIEW » List of created NOC views

Network Operations Center (NOC) View automatically rotates through all tabs in the left hand navigation pane of a page.

Enable NOC view mode

This screen will provide the opportunity to customize which widgets we want in our view. In this lab we are going to place Compliance Policy type widgets in our view.

On the next step of this configuration, we are going to Tabs to your dashboard and widgets to the columns of each.

## Step 6.

### Customize CFP Dashboard

Name  UPDATE

Type of view: **Summary**

LEFT NAVIGATION

Is there a lot of content on this view? Break it up into smaller pages with tabs on the left.  
 Enable left navigation

Tab Name: Summary UPDATE

Tab Icon:

COLUMN 1  COLUMN 2  COLUMN 3  COLUMN 4

Width: 500 px Move to a different tab

Width: 400 px Move to a different tab

Width: 450 px Move to a different tab

Width: 450 px Move to a different tab

Select the “Enabled left navigation” box, this will provide the ability to add multiple tabs on the left-hand side will be shown.

We are going to add 3 different tabs. As you create each tab, be sure to click the ‘UPDATE’ button to the right of the “Tab Name” field as shown by the arrow above.

Summary Tab – Already configured

Network Systems Tab

SolarWinds Systems Tab

Network Compliance Tab

On the Summary Tab:

In Column 1 add the following widget(s):

Event Summary

In Column 2 add the following widget(s):

None

In Column 3 add the following widget(s):

Network Wide Bytes Transferred

QoE Statistics

In Column 4 add the following widget(s):

Total Nodes by OS

Total Interfaces by Type

Action: Click on 'Network Systems' Tab you have created

## Step 7.

### Customize CFP Dashboard

Name    
Type of view: **Summary**

#### LEFT NAVIGATION

Is there a lot of content on this view? Break it up into smaller pages with tabs on the left.

Enable left navigation

The screenshot shows the 'Customize CFP Dashboard' interface. At the top, there's a 'Name' field set to 'CFP Dashboard' with an 'UPDATE' button. Below that, 'Type of view' is set to 'Summary'. On the left, there's a 'LEFT NAVIGATION' section with a checkbox for 'Enable left navigation' which is checked. The main area is divided into three columns:

- Column 1:** Contains a 'Network Systems' tab (highlighted with a red box) and a 'SolarWinds Systems' tab (with a cursor over it). The 'Network Systems' tab has three resource widgets: 'Multiple Object Chart' (with a plus sign icon circled in red), 'Custom Network Wide Chart' (with a plus sign icon circled in red), and 'Find Connected Port for End Host' (with a plus sign icon circled in red). The width is set to 500 px.
- Column 2:** Contains a 'SolarWinds Systems' tab (with a cursor over it) and a 'Network Compliance' tab. The 'SolarWinds Systems' tab has three resource widgets: 'Custom Network Wide Chart' (with a plus sign icon circled in red), 'Total Nodes By OS', and 'NCM Node List'. The width is set to 400 px.
- Column 3:** Contains a 'Network Compliance' tab and an 'Add tab' button. The 'Network Compliance' tab has three resource widgets: 'Find Connected Port for End Host' (with a plus sign icon circled in red), 'Total Nodes By OS', and 'NCM Node List'. The width is set to 450 px.

At the bottom of each column, there are 'Move to a different tab' buttons.

On the Network Systems Tab:

In Column 1 add the following widget(s):

Multiple Object Chart

In Column 2 add the following widget(s):

Custom Network Wide Chart

In Column 3 add the following widget(s):

Find Connected Port for End Host

Total Nodes by OS

NCM Node List

Action: Click on 'SolarWinds Systems' Tab

## Step 8.

### Customize CFP Dashboard

Name CFP Dashboard

Type of view: **Summary**

#### LEFT NAVIGATION

Is there a lot of content on this view? Break it up into smaller pages with tabs on the left.

Enable left navigation

The screenshot shows the 'Customize CFP Dashboard' page. At the top, there's a 'Name' field set to 'CFP Dashboard' with an 'UPDATE' button. Below it, 'Type of view' is set to 'Summary'. On the left, there's a 'LEFT NAVIGATION' section with tabs for 'Summary', 'Network Systems', 'SolarWinds Systems' (which is highlighted with a red box), 'Network Compliance', and an 'Add tab' option. The main area is divided into three columns:

- COLUMN 1:** Tab Name: SolarWinds Systems, Tab Icon: Home. Resources: Top 10 Disk Queue Length, Top 10 Errors & Discards This Hour, Top 10 Avg. Disk sec/Transfer. Width: 500 px. Action: Move to a different tab.
- COLUMN 2:** Tab Name: SolarWinds Systems (same as Column 1). Resources: Guests with Problems, Hosts with Problems. Width: 400 px. Action: Move to a different tab.
- COLUMN 3:** Tab Name: SolarWinds Systems (same as Column 1). Resources: Last 10 Audit Events. Width: 450 px. Action: Move to a different tab.

In each column's resource list, there's a red circle around the '+' icon, indicating where new widgets can be added.

On the SolarWinds Systems Tab:

In Column 1 add the following widget(s):

- Top 10 Disk Queue Length
- Top 10 Errors & Discards this Hour
- Top 10 Avg. Disk sec/Transfer

In Column 2 add the following widget(s):

Guests with Problems

Hosts with Problems

In Column 3 add the following widget(s):

Last 10 Audit Events

Action: Click on the 'Network Compliance' Tab when complete.

## Step 9.

Customize CFP Dashboard

Name: CFP Dashboard

Type of view: Summary

LEFT NAVIGATION

Is there a lot of content on this view? Break it up into smaller pages with tabs on the left.

Enable left navigation

Tab Name: Network Compliance   
Tab Icon:

COLUMN 1

TIP: You can use up to 6 columns

Resources

Policy Violations

Policy Violations

Add New Column

Width: 500 px

The screenshot shows the 'Customize CFP Dashboard' interface. On the left, there's a 'LEFT NAVIGATION' section with tabs for 'Summary', 'Network Systems', 'SolarWinds Systems', and 'Network Compliance'. The 'Network Compliance' tab is highlighted with a red box. On the right, there's a 'COLUMN 1' configuration area. It shows a 'Resources' section with two 'Policy Violations' widgets. To the right of the first widget is a 'DUPLICATE' button, which is circled in red. Below the column configuration, there's a note about width and a link to move to a different tab.

On the Network Compliance Tab:

In Column 1 add the following widget(s):

Policy Violations

Policy Violations

SolarWinds has added just one of the Policy Violations selections. In order to get multiples of the same widget, look to the right of the column. The three small icons going down will be duplicates.

Action: Highlight the Policy Violations and click the duplicate button to the right, twice.

Action: Highlight one of the Policy Violation widgets and move it to the right one column. This is shown by clicking on the ' > ' located second from the top just to the right of column 1. They are difficult to see.

## Step 10.

NOC VIEW » List of created NOC views  
Network Operations Center (NOC) View automatically rotates through all tabs in the left hand navigation pane of a page.  
 Enable NOC view mode

Link to NOC View: [CFP Dashboard - NOC](#)

Rotate tabs every  seconds  Every tab listed in left navigation will be used.

**VIEW LIMITATION**  
You can create a view limitation that will limit the network devices that can be displayed on this view. Account limitations for the logged-in account will also be applied to this view when it is displayed.

No View Limitation defined.

The NOC VIEW will allow you to rotate the screens based on the time per screen. Default is 15 seconds.

The VIEW LIMITATION section will allow you to define who should be able to see this view or what devices are allowed to use this view.

Action: Click “DONE” when finished.

## Step 11.

 **CUSTOMIZE NAVIGATION & LOOK**  
Add, edit or delete items in menu bar, change color scheme etc.

\* Customize Menu Bars  \* Color Scheme \* External Websites

Action: Navigate to the SETTINGS > All Settings > CUSTOMIZE NAVIGATION & LOOK section

Action: Click on ‘Customize Menu Bars’

## Step 12.

### Select a Menu Bar to Customize

Any menu bar can be assigned to any tab. Menu bars are assigned to tabs per user.

Menu Bar: Admin



Menu Bar: APM\_TabMenu



Menu Bar: Databases\_TabMenu



Menu Bar: Default



Menu Bar: Guest



Menu Bar: NCM\_TabMenu



Here is where all SolarWinds Menu Bars configurations reside. We are going to place it in the Network Configuration Product section of the My Dashboards. Locate NCM\_TabMenu (at the bottom of this picture).

Action: Click 'Edit' on the NCM\_TabMenu.

## Step 13.

### Edit NCM\_TabMenu Menu Bar

Drag items from the Available Items column to the Selected Items column to build your menu bar. Rearrange items by dragging them. Select the 'Submit' button to save changes.

Available items	Selected items
% Loss & Traffic	
Accounts	
Admin	
All Interfaces	
All Maps	
All Nodes	
All Volumes	
Apps	
BGP	
CBQoS Polling	
CFP Dashboard	
Conversations	CFP Dashboard
Countries	
Custom Summary	
Customize	

**SUBMIT** **CANCEL**

In this list of different views, we will need to locate our CFP Dashboard view. It is listed in alphabetical order so location will be easy.

Action: Locate CFP Dashboard view, Left Click & Hold, then drag and drop to the Selected Items column and place under 'End of Support' item in the dashboard list.

## Step 14.

### Edit NCM\_TabMenu Menu Bar

Drag items from the Available Items column to the Selected Items column to build your menu bar. Rearrange items by dragging them. Select the 'Submit' button to save changes.

Available items	Selected items
% Loss & Traffic	
Accounts	
Admin	
All Interfaces	
All Maps	
All Nodes	
All Volumes	
Apps	
BGP	
CBQoS Polling	

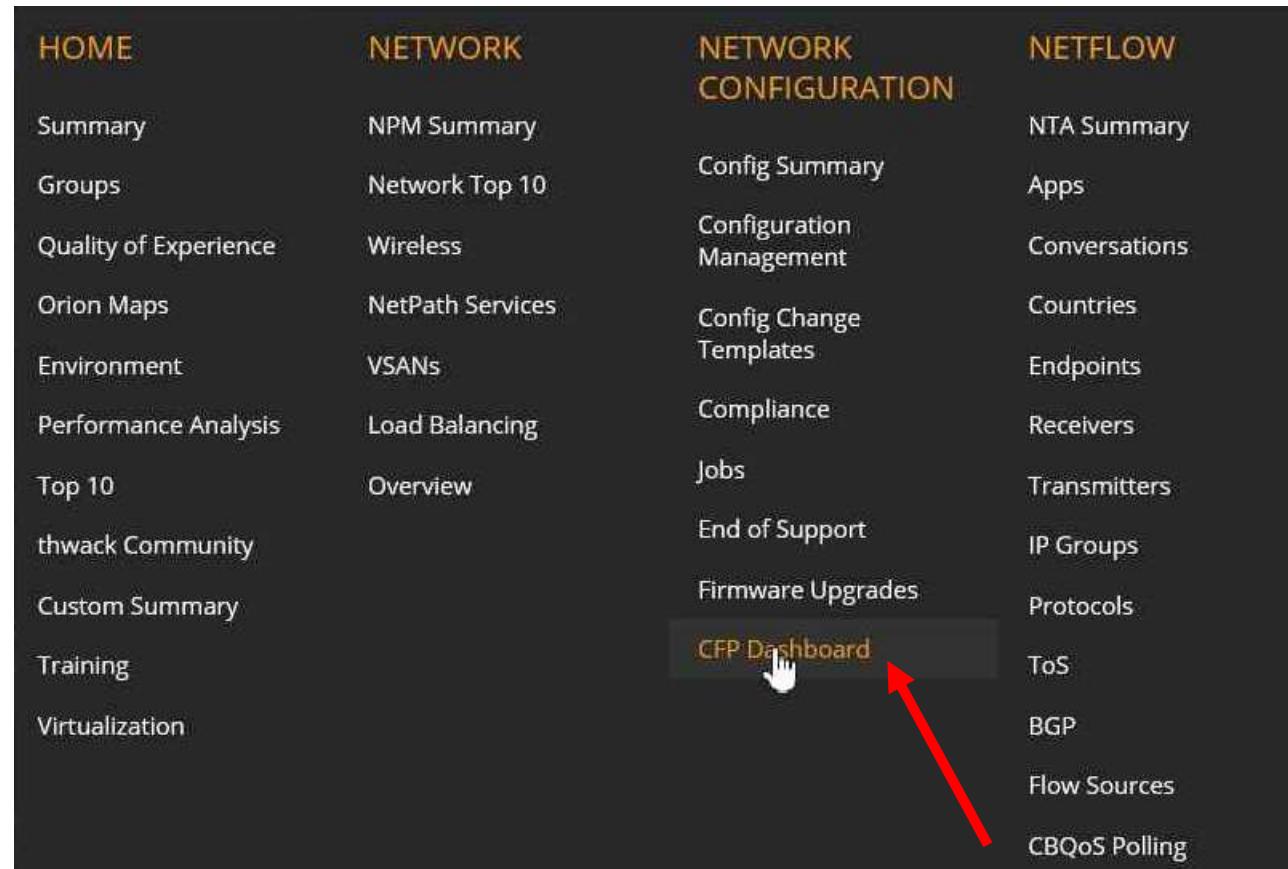
**SUBMIT** **CANCEL**

Here at the top we drag it into place. The Menu Bar will make room for it when you hover over the window. You can also order your selections this way.

Action: Place/drop your CFP Dashboard view at the bottom of the Selected items list.

Action: Click 'SUBMIT' when complete

## Step 15.



We see that our new view, is now listed in the My Dashboards section and ready to develop further.

## Step 16.

The screenshot shows the SolarWinds interface. At the top, there's a navigation bar with links for 'MY DASHBOARDS', 'ALERTS & ACTIVITY', 'REPORTS', and 'SETTINGS'. Below the navigation bar is a sidebar titled 'CUSTOMIZE PAGE' with several items: 'Network Systems' (which is highlighted with a red box), 'Network Systems (Time (TCP Handshake))', 'SolarWinds Systems', and 'Network Compliance'. The main area of the dashboard is titled 'Summary' and contains a chart with three columns: 'AVERAGE RESPONSE TIME', 'AVG APPLICATION RESPONSE TIME', and 'AVG NETWORK RESPONSE TIME'. Below the chart, there's a section titled 'Time (TCP Handshake)' with 'EXPORT', 'EDIT', and 'HELP' buttons. A large callout box in the center of the dashboard area says 'Data is not available' and has a link 'Why not?'. At the bottom right of the dashboard area, there are 'EDIT' and 'HELP' buttons.

We are now able to see our new View and the supporting sub-Views/

This concludes the lab exercise.

# Lab 06 – Account Management

This lab will go through the steps to setup a SolarWinds User Account.

## Step 1.

**Main Settings & Administration**

**GETTING STARTED WITH ORION**  
Discover your network and add the objects you want to monitor in Orion.

- » Discovery Central
- » Add VMware vCenter or Hyper-V devices
- » Discover Network
- » Add a Transaction Monitor
- » Add Node
- » Add Storage Device

**NODE & GROUP MANAGEMENT**  
Manage and delete nodes, dependencies and groups. Edit node properties.

- » Manage Nodes
- » Manage Groups
- » Manage Storage Objects
- » Manage Device Templates
- » Manage Orion Maps
- » Manage Virtual Devices
- » Manage Agents
- » Manage Pollers
- » Manage Hardware Sensors
- » Manage Dependencies
- » Manage Custom Properties
- » Manage World Map
- » Manage Container Services

**ALERTS & REPORTS**  
Create new alert / report or edit existing definitions.

- » Manage Alerts
- » Configure Default Send Email Action
- » Manage Reports
- » ServiceNow Instances
- » Manage SMTP Servers

Starting at the SETTINGS > All Settings page we will begin the account creation process.

## Step 2.

The screenshot shows the Orion Platform's navigation menu. The sections listed are:

- THRESHOLDS & POLLING**
  - \* Polling Settings
  - \* Orion Thresholds
  - \* SRM Thresholds
  - \* Node Child Status Participation
  - \* Custom Poller Thresholds
  - \* Virtualization Thresholds
  - \* NPM Thresholds
- CREDENTIALS**
  - Add, edit, delete credentials.
  - \* Manage Windows Credentials
  - \* Manage SNMPv3 Credentials
- USER ACCOUNTS**
  - Create, edit or delete user accounts, specify management rights and limitations.
  - \* Manage Accounts (highlighted with a red box)
  - \* SAML Configuration
  - \* Account List
  - \* Advanced AD Settings
- VIEWS**
  - Customize content of views or create new views.
  - \* Manage Views
  - \* Views by Device Type
  - \* Add New View
  - \* Views by Application Type
  - \* Created NOC Views

The USER ACCOUNTS section is towards the bottom of the page. Scroll down to the bottom and locate the “USER ACCOUNTS” section.

Action: Click on ‘Manage Accounts’

## Step 3.

### Manage Accounts

Add individual accounts to Orion. If a user has an individual account and is a member of a group, individual account permissions/settings will be applied and all group permissions/settings will be ignored.

INDIVIDUAL ACCOUNTS	WINDOWS GROUPS	SAML GROUPS						
<a href="#">+ ADD NEW ACCOUNT</a>	<a href="#">EDIT</a>   <a href="#">CHANGE PASSWORD</a>   <a href="#">DELETE</a>	Search individual accounts by name						
Name	Account Type	Enabled	Expiration	Last Login	Account Limitation	Admin Rights	Node Mgmt	Map Mgmt
Admin	Orion	Yes	Never	Saturday, January 25, 2020 ...	None	Yes	Yes	Yes
Guest	Orion	No	Never	Never	None	No	No	No

There will be two default accounts that come with a new SolarWinds installation.

The Admin Account should have a password assigned to it.

The Guest Account should be deleted from the system.

## Step 4.

### Add New Account

SELECT TYPE > ENTER ACCOUNT INFO > DEFINE SETTINGS >

I would like to create:

 Orion individual account  
Add a new SQL-based account. [Learn more](#)

 Windows individual account  
Add existing Active Directory or local accounts to Orion. [Learn more](#)

 Windows group account  
Add existing Active Directory or local group accounts to Orion. [Learn more](#)

 SAML individual account  
Add a new SAML account. [Learn more](#)

 SAML group account  
Add a new SAML group account [Learn more](#)

As seen above, there are 5 different types of SolarWinds accounts that can be created. We will be focusing on the Orion Account for this lab.

The other accounts will require either Active Directory Authentication or SAML integration.

Action: Click the radio button for 'Orion individual account'

Step 5.

## Add New Account

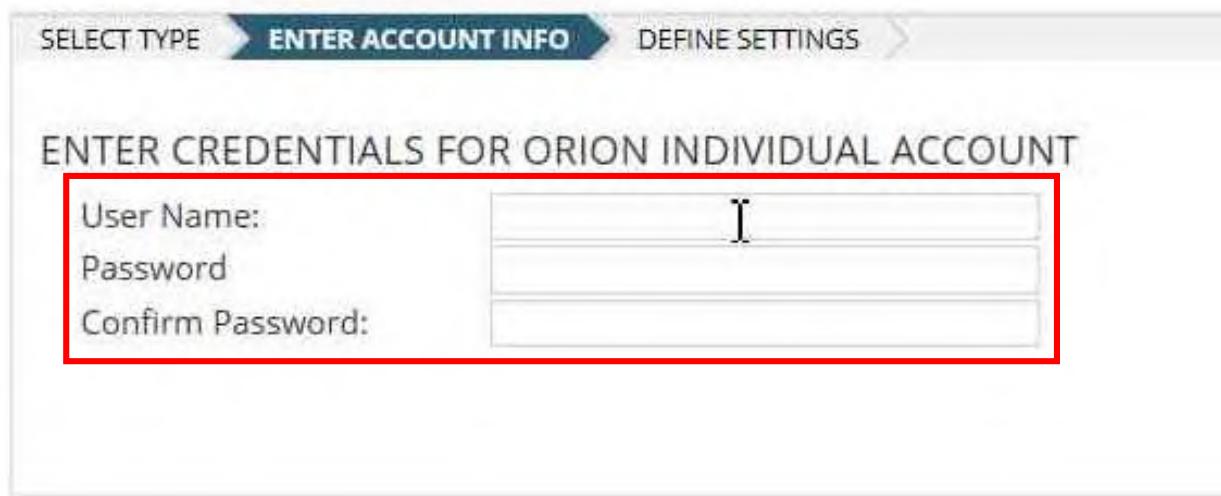
SELECT TYPE ➔ **ENTER ACCOUNT INFO** ➔ DEFINE SETTINGS ➔

ENTER CREDENTIALS FOR ORION INDIVIDUAL ACCOUNT

User Name:

Password

Confirm Password:



Action: Enter a username, enter a password, confirm the password.

## Step 6.

SELECT TYPE > ENTER ACCOUNT INFO > **DEFINE SETTINGS**

DEFINE SETTINGS FOR ORION INDIVIDUAL "COURTESYIT" ACCOUNT

Account Enabled	<input type="button" value="Yes"/>
Account Expires	<input type="text" value="Never"/> <input type="button" value="..."/>
Disable Session Timeout	<input type="button" value="No"/>
Allow Administrator Rights	<input type="button" value="Yes"/> 
Allow Node Management Rights	<input type="button" value="Yes"/>
Allow Map Management Rights	<input type="button" value="Yes"/>

**REPORTS**

Allow Report Management Rights	<input type="button" value="No"/>
Report Limitation Category	<input type="button" value="Default"/> <input type="button" value="..."/>

**ALERTS**

Allow Alert Management Rights	<input type="button" value="Yes"/>
Alert Limitation Category	<input type="button" value="No Limitation"/> <input type="button" value="..."/>

The next few sections will be the heart of the lab. We will cover different types of access and access control. This top section is to define basic settings for Web Console usages and SolarWinds Administrative access. Each item on the left has a corresponding description on the right. Your organization will have standard account settings for each of these. For our purposes here we will be setting the account up as an administrator.

Action: Allow Administrator Rights select 'Yes'

Once this is selected several other selections will automatically switch to 'Yes'

## Step 7.

### ACCOUNT LIMITATIONS

There are no account limitations defined. To create account limitations, click the "Add Limitation" button.

**ADD LIMITATION**



#### Select Limitation Type For Account "CourtesyIT"

Select a Limitation Type for this Account. Limitations are used to limit the Network Devices each Account can view. For example: You could easily create a Limitation for an Account that allows them to only view a single Network Device. Or, you could limit this Account to only viewing Cisco devices. Or... only view Network Devices with a System Location of "Building B".

- |  |  |
|--|--|
| <input type="radio"/> Single Network Node          | Limit the Account to a Single Network Node   |
| <input type="radio"/> Group of Nodes               | Limit the Account to a group of selected Nodes   |
| <input type="radio"/> Node Name Pattern            | Limit the Account to a group of Nodes with similar Node Names. The Node Name is the Name you assigned the Node within Web Node Management. |
| <input type="radio"/> System Name Pattern          | Limit the Account to a group of Nodes with similar System Names  |
| <input type="radio"/> Group of Machine Types       | Limit the Account to specific Types of Devices   |
| <input type="radio"/> Machine Type Pattern         | Limit the Account to specific types of devices based on a Device Type pattern  |
| <input type="radio"/> Hardware Manufacturer        | Limit the Account to specific Hardware Manufacturers   |
| <input type="radio"/> Device Status                | Limit the Account based on the Node's Status ( Up, Down, Warning )   |
| <input type="radio"/> System Location              | Limit the Account to a specific list of device Locations. The Node's System Location is discovered and used.                               |
| <input type="radio"/> System Location Pattern      | Limit the Account based on a Location pattern. The Node's System Location is discovered and used.  |
| <input type="radio"/> System Contact               | Limit the Account to a specific list of device Contacts. Each Node's System Contact is discovered and used.                                |
| <input type="radio"/> System Contact Pattern       | Limit the Account based on a Contact pattern. Each Node's System Contact is discovered and used.   |
| <input type="radio"/> Single Machine Type          | Limit the Account to a single Machine Type   |
| <input type="radio"/> Single Hardware Manufacturer | Limit the Account to a single Hardware Manufacturer  |
| <input type="radio"/> IP Address Pattern           | Limit the Account to Nodes within a specific Subnet or Network   |
| <input type="radio"/> Node Category                | Limit nodes by category (Network device, Server, Other)  |
| <input type="radio"/> Group of Volumes             | Limit the Account to a selected Group of Volumes   |
| <input type="radio"/> Single Group                 | Limit the Account to a Single Group  |
| <input checked="" type="radio"/> Group of Groups   | Limit the Account to a group of selected Groups  |
| <input type="radio"/> Group Name Pattern           | Limit the Account to a group of Groups with similar Group Names  |
| <input type="radio"/> Single Report                | Limit the Account to a single Report   |

- 
- A red circle highlights the 'Group of Groups' radio button, and a red arrow points from the left towards it.

As you scroll down the page you will come across the Account Limitations section. This section will allow you to assign nodes based on Groups or Custom Properties to those users who may need access to selected devices.

**Configure Limitation**

GROUP OF GROUPS  
Limit the Account to a group of selected Groups

C1\_DeviceType\_IL3S  
 C1\_DeviceType\_IRTR  
 C1\_DeviceType\_L2SW  
 C3\_Function\_Workstations  
 C4\_Application\_SolarWinds

**SUBMIT**



## Step 8.

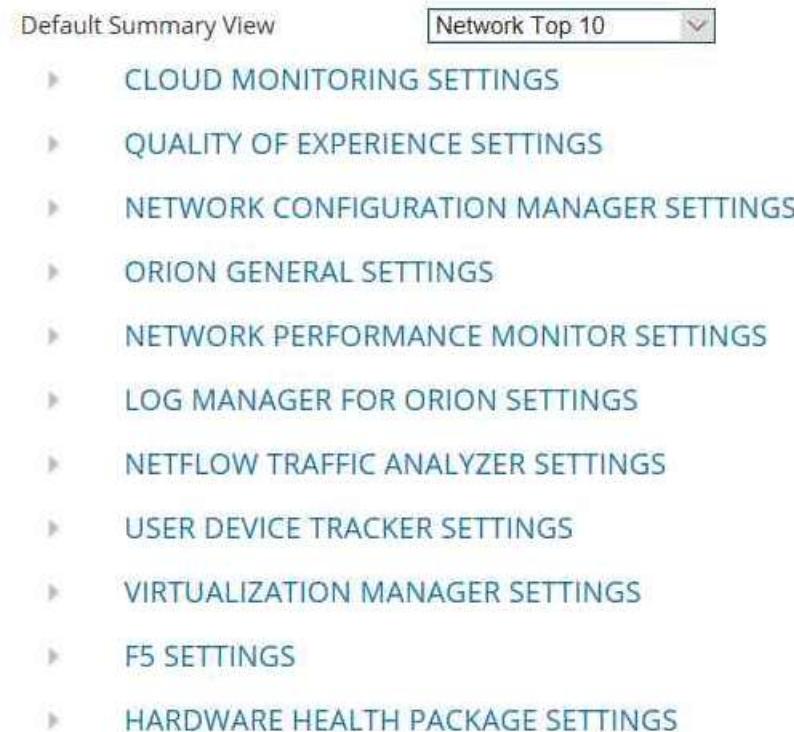
### DEFAULT MENU BAR AND VIEWS

Select the menu bar for this account. To view the contents of each menu bar, go to the [Customize Menu Bars](#) page.

HomeTab Menu Bar	Default
NetworkTab Menu Bar	Network_TabMenu
Network ConfigurationTab Menu Bar	NCM_TabMenu
NetflowTab Menu Bar	NTA_TabMenu
Device TrackerTab Menu Bar	DeviceTracker_TabMenu
Show Alerts Menu	Yes
Show Events Menu	Yes
Show Message Center Menu	Yes
Show Syslogs Menu	Yes
Show Traps Menu	Yes
Show All Reports Menu	Yes
Tabs ordering	

The DEFAULT MENU BAR AND VIEWS section is where you can select which products this account can see, and which ones would be hidden from view or access. At the bottom of this section a default home page can be set based on your organization's preferences.

## Step 9.



- ▶ HARDWARE HEALTH BASEBOARD MANAGEMENT CONTROLLER SETTINGS
- ▶ NETWORK INTERFACE SETTINGS
- ▶ PERFORMANCE ANALYSIS SETTINGS
- ▶ POWER CONTROL UNIT SETTINGS
- ▶ RECOMMENDATIONS SETTINGS
- ▶ SSH SETTINGS
- ▶ CLOUD MONITORING PER PROVIDER SETTINGS
- ▶ WIRELESS SETTINGS
- ▶ WIRELESS HEAT MAP SETTINGS

This section is the Products section. Various SolarWinds products have their own roles, functions, and abilities to assign to different users.

## Step 10.

The screenshot shows the 'NETWORK CONFIGURATION MANAGER SETTINGS' section. Under 'NCM Role', there are five options: 'Administrator' (selected), 'Engineer', 'WebUploader', 'WebDownloader', and 'WebViewer'. Below this, a table lists various NCM views and their descriptions:

View	Description
Learn more about NCM roles	Provides an array of information pertaining to the intersection of the nodes you are managing in SolarWinds NCM and SolarWinds NPM.
NCM Config Details View	Offers the complete device configuration file and a history of configuration files for a node.
NCM Compliance Report View	Provides a number of compliance reports, including HIPAA and SOX Security Reports.
NCM Compliance Report Result View	Offers NCM Policy report results, for example, the HIPAA Security Report details.
NCM EW Chart Details View	Offers detailed data of EnergyWise-enabled and EnergyWise-capable nodes.
NCM Find Connected Port for End Host Result View	Offers the NCM Find Connected Port for End Host results, including Host Name, MAC Address, IP Address, Port Description, etc.
NCM Execute Config Change Template View	Provides the ability to execute config change template on devices.
NCM Config Change Templates View	Provides the ability to view config change templates.
NCM Shared Config Change Templates on thwack View	Provides the ability to view shared config change templates on thwack.
NCM Security Policy Details View	Provides the ability to view security policy details.

Under the NETWORK CONFIGURATION MANAGER (NCM) SETTINGS section you see different roles for the user and what that user is allowed to do. Your network engineers should be Administrators while help desk personnel should be WebDownloader. Your organization will need to devise a set of policies to govern these permissions.

## Step 11.

The screenshot shows the 'NETWORK PERFORMANCE MONITOR SETTINGS' section. It includes two dropdown menus: 'VSAN Details' and 'Multicast Group Details', each with a description to its right:

- 'VSAN Details' dropdown: This view is used when details about a single VSAN are displayed.
- 'Multicast Group Details' dropdown: Multicast Group Details views display information about a single Multicast Group.

The NETWORK PERFORMANCE MONITOR SETTINGS section is very sparse and does not need to be changed.

## Step 12.

NETFLOW TRAFFIC ANALYZER SETTINGS	
NetFlow Traffic Analyzer View	NetFlow Traffic Analyzer Summary
NetFlow Node Details	NetFlow Node Details
NetFlow Application Details	NetFlow Application
NetFlow Interface Details	NetFlow Interface Details
NetFlow Conversation	NetFlow Conversation
NetFlow Country	NetFlow Country
NetFlow Domain	NetFlow Domain
NetFlow Endpoint	NetFlow Endpoint
NetFlow IPAddressGroup	NetFlow IP Address Group
NetFlow Protocol	NetFlow Protocol
NetFlow Type of Service	NetFlow Type of Service
NetFlow CBQoS	CBQoS Details
NetFlow Autonomous Systems	NetFlow Autonomous Systems
NetFlow Autonomous System Conversations	NetFlow Autonomous System Conversations
NetFlow NBAR2 Application Details	NetFlow NBAR2 Application

This view is used when NetFlow Summary are displayed.

This view is used when details about a single NetFlow Node are displayed.

This view is used when details about a single NetFlow Application are displayed.

This view is used when details about a single NetFlow Interface are displayed.

This view is used when details about a conversation displayed.

This view is used when details about a country displayed.

This view is used when details about a domain displayed.

This view is used when details about an endpoint displayed.

This view is used when details about a IP Address Group displayed.

This view is used when details about a protocol displayed.

This view is used when details about a type of service displayed.

This view is used when details about CBQoS class map displayed

This view is used when details about Autonomous Systems displayed

This view is used when details about AS Conversations displayed

This view is used when details about a single NetFlow NBAR2 Application are displayed.

The NETFLOW TRAFFIC ANALYZER SETTINGS section have a few different settings. Generally, these do not need to be changed. Defaults here are good.

Action: Scroll to the bottom of the page and click “SAVE”.

Manage Accounts

Add individual accounts to Orion. If a user has an individual account and is a member of a group, individual account permissions/settings will be applied and all group permissions/settings will be ignored.

INDIVIDUAL ACCOUNTS    WINDOWS GROUPS    SAML GROUPS

Name	Account Type	Enabled	Expiration	Last Login	Account Limitation	Admin Rights	Node Mgmt	Map Mgmt
Admin	Orion	Yes	Never	Saturday, January 25, 2020 ...	None	Yes	Yes	Yes
courtesysit	Orion	Yes	Never	Never	Group of Groups	No	No	No
Guest	Orion	No	Never	Never	None	No	No	No

Displaying accounts 1 - 3 of 3 Number of items per page: 10

solarwinds Orion Platform HF2, NCM HF1, NPM, NTA, UDT: 2019.4 © 1999-2020 SolarWinds Worldwide, LLC. All Rights Reserved.

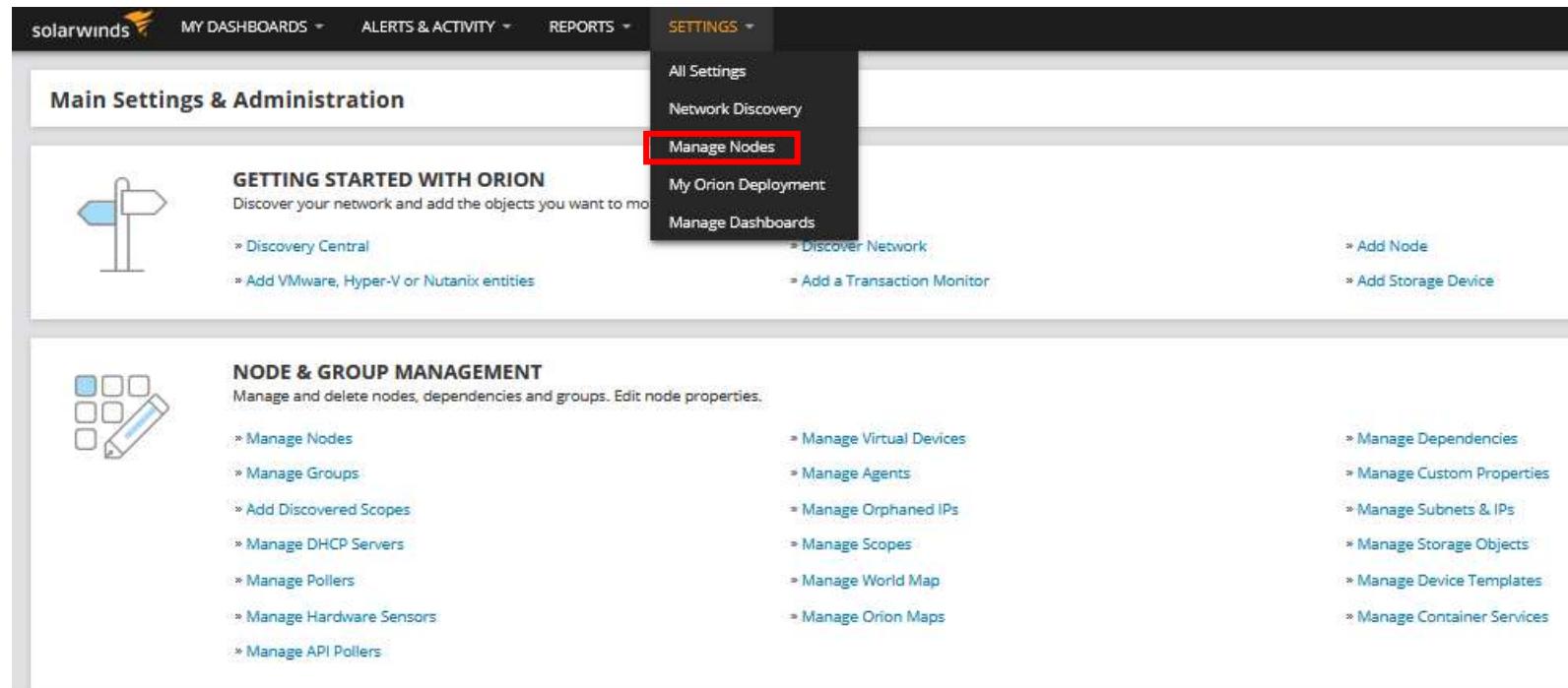
This concludes the lab exercise.

This page intentionally left blank.

# Lab 07 - Manage Nodes

This lab will cover how to Manage Nodes in your SolarWinds database.

## Step 1.



The screenshot shows the SolarWinds Orion web interface. At the top, there is a navigation bar with links for 'MY DASHBOARDS', 'ALERTS & ACTIVITY', 'REPORTS', and 'SETTINGS'. A dropdown menu is open under 'SETTINGS', and the option 'Manage Nodes' is highlighted with a red box. Below the navigation bar, there is a section titled 'Main Settings & Administration' with a 'GETTING STARTED WITH ORION' guide. On the left, there is a 'NODE & GROUP MANAGEMENT' section with various management options like 'Manage Nodes', 'Manage Groups', etc. To the right of this section, there is a list of additional management tasks such as 'Discover Network', 'Add Node', 'Add Storage Device', etc.

Here we are going to start from the SETTINGS > All Settings page. You will see this page is a common reference point for SolarWinds Administrators.

## Step 2.

<input type="checkbox"/>	Name	Polling IP Address	C1_DeviceType (CP)	C2_OS (CP)	C3_Function (CP)	C4_Application (CP)	<a href="#">»</a>
<input type="checkbox"/>	10.50.2.2	10.50.2.2					
<input type="checkbox"/>	ipv4s2.nmsnil.local	10.50.2.61	Router	IOS	Network Device	Infrastructure	
<input type="checkbox"/>	ipv4s3.nmsnil.local	10.50.2.62	Router	IOS	Network Device	Infrastructure	
<input type="checkbox"/>	ipv6s2.nmsnil.local	10.50.2.63	Router	IOS	Network Device	Infrastructure	
<input type="checkbox"/>	ipv6s3.nmsnil.local	10.50.2.64	Router	IOS	Network Device	Infrastructure	
<input type="checkbox"/>	student01-VM	10.0.0.10	Server	2019	Server	Orion	

The section to the left of the page is the node group section. You can sort the nodes in the database based on SolarWinds Properties and Custom Properties. Once an item is selected on the left, the nodes will appear on the right in a list format. Take a moment to look at the different possibilities of sorting nodes.

Action: Choose several different types of Properties on the left to display nodes on the right.

### Step 3.

Manage Nodes

Show: Nodes

Group by: [No Grouping] ▾

ADD NODE CUSTOM PROPERTY EDITOR EDIT PROPERTIES LIST RESOURCES ASSIGN POLLERS MAINTENANCE MODE MORE ACTIONS DELETE

Name	Polling IP Address	C1_DeviceType (CP)	C2_OS (CP)	C3_Function (CP)	C4_Application (CP)
10.50.2.2	10.50.2.2				
ipv4s2.nmsnil.local	10.50.2.61	Router	IOS	Network Device	Infrastructure
ipv4s3.nmsnil.local	10.50.2.62	Router	IOS	Network Device	Infrastructure
ipv6s2.nmsnil.local	10.50.2.63	Router	IOS	Network Device	Infrastructure
ipv6s3.nmsnil.local	10.50.2.64	Router	IOS	Network Device	Infrastructure
student01-VM	10.0.0.10	Server	2019	Server	Orion

Page 1 of 1 Page size 40 Displaying objects 1 - 6 of 6

Group by: [No Grouping] ▾

- Machine Type
- Node Category
- Polling Engine
- Polling Method
- SNMP Version
- Status
- Location
- Contact
- Community
- RWCommunity
- IsServer
- Is OrionServer
- IP Version
- Unmanage Window
- VLAN ID
- Agent - .Net Framework release value
- Agent - Agent Status

Here is an example of different properties to group nodes by. When you select an item, you will be shown the following:

- Node Name
- Polling IP Address
- Status

## Step 4.



<input type="checkbox"/>	Name	Polling IP Address	C1_DeviceType (CP)	C2_OS (CP)	C3_Function (CP)	C4_Application (CP)	<a href="#">»</a>
<input type="checkbox"/>	10.50.2.2	10.50.2.2					
<input type="checkbox"/>	ipv4s2.nmsnll.local	10.50.2.61	Router	iOS	Network Device	Infrastructure	
<input type="checkbox"/>	ipv4s3.nmsnll.local	10.50.2.62	Router	iOS	Network Device	Infrastructure	
<input type="checkbox"/>	ipv6s2.nmsnll.local	10.50.2.63	Router	iOS	Network Device	Infrastructure	
<input type="checkbox"/>	ipv6s3.nmsnll.local	10.50.2.64	Router	iOS	Network Device	Infrastructure	
<input type="checkbox"/>	student01-VM	10.0.0.10	Server	2019	Server	Orion	

### Add Node

From this location we can add a node or invoke a network discovery wizard session.

Action: Click on the 'ADD NODE' button from the above tool bar.

This will bring you to the Add Node page where you can choose to add a single node or run a network discovery wizard as shown below.

## Add Node

DEFINE NODE > CHOOSE RESOURCES > ADD POLLERS > ADD UDT PORTS > CHANGE PROPERTIES >

### 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 Discovery](#).

Polling Hostname or IP Address:  IPv4 and IPv6 formats are both valid  
 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 element on the node but not the node itself.

**Status Only: ICMP**  
Limited data (status, response time, and packet loss) is collected using ICMP (ping). Useful for devices which do not support SNMP or WMI.

**Most Devices: SNMP and ICMP**  
Standard polling method for network devices such as switches and routers, as well as Unix/Linux servers.

SNMP Version:  SNMPv2c is used, by default, when SNMPv3 is neither required nor supported.

SNMP Port:   
 Allow 64 bit counters

Community String:  Press down arrow to view all  
Read/Write Community String:

**Windows Servers:** WMI and ICMP  
Recommended agentless polling method for Windows servers.

**Windows & Unix/Linux Servers: Agent**  
Optional agent useful for monitoring Windows & Unix/Linux hosts in remote or distributed environments, such as the cloud. Credentials are needed only for installing the agent.  
[agent](#)

## Step 5.



The screenshot shows a table titled "CUSTOM PROPERTY EDITOR" with a red box highlighting the title bar. The table has columns: Name, Polling IP Address, C1\_DeviceType (CP), C2\_OS (CP), C3\_Function (CP), and C4\_Application (CP). The data rows include nodes like "10.50.2.2", "ipv4s2.nmsn1.local", "student01-VM", etc., with their respective details. At the bottom, there are navigation buttons for "Page", "Page size", and a status message "Displaying objects 1 - 6 of 6".

Name	Polling IP Address	C1_DeviceType (CP)	C2_OS (CP)	C3_Function (CP)	C4_Application (CP)
10.50.2.2	10.50.2.2				
ipv4s2.nmsn1.local	10.50.2.61	Router	iOS	Network Device	Infrastructure
ipv4s3.nmsn1.local	10.50.2.62	Router	iOS	Network Device	Infrastructure
ipv6s2.nmsn1.local	10.50.2.63	Router	iOS	Network Device	Infrastructure
ipv6s3.nmsn1.local	10.50.2.64	Router	iOS	Network Device	Infrastructure
student01-VM	10.0.0.10	Server	2019	Server	Orion

The Custom Property Editor will allow you to make changes to the custom properties of your nodes.

### Custom Property Editor

Click in the grid cell to edit the values.



This screenshot shows the same data as the previous table, but in a more spreadsheet-like "Custom Property Editor" view. It includes a "GROUP BY" dropdown set to "[No Grouping]". The columns are labeled "Caption", "IP\_Address", "C1\_DeviceType (required)", "C2\_OS (required)", "C3\_Function (required)", and "C4\_Application (required)". Each row corresponds to a node from the table above, with the "Caption" column showing the node name and the "IP\_Address" column showing its IP address.

Caption	IP_Address	C1_DeviceType (required)	C2_OS (required)	C3_Function (required)	C4_Application (required)
10.50.2.2	10.50.2.2				
ipv4s2.nmsn1.local	10.50.2.61	Router	iOS	Network Device	Infrastructure
ipv4s3.nmsn1.local	10.50.2.62	Router	iOS	Network Device	Infrastructure
ipv6s2.nmsn1.local	10.50.2.63	Router	iOS	Network Device	Infrastructure
ipv6s3.nmsn1.local	10.50.2.64	Router	iOS	Network Device	Infrastructure
student01-VM	10.0.0.10	Server	2019	Server	Orion

This view acts like an Excel spreadsheet. You can change a single cell or multiple cells. Take a moment to fill in any blanks you may have.

Action: Click on Settings > Manage Nodes.

## Step 6.

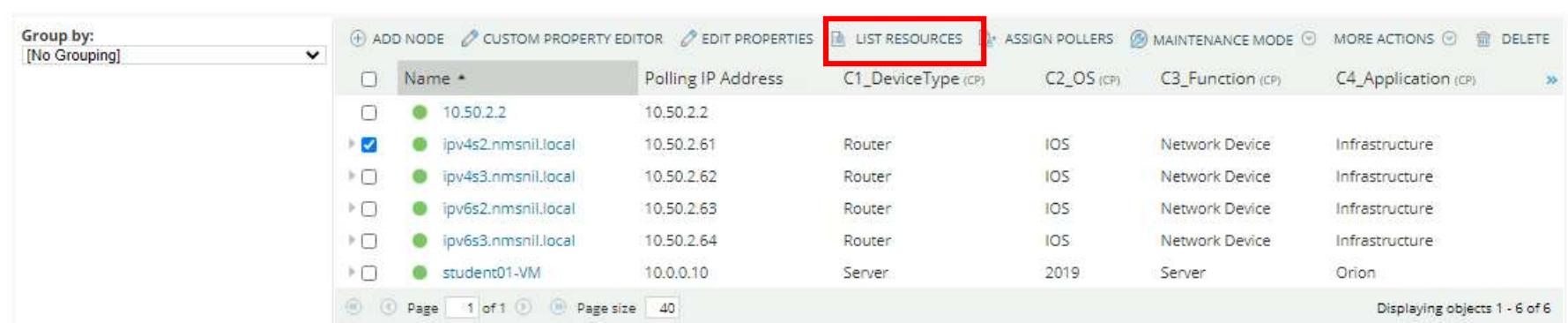
Manage Nodes

Show: Nodes

Group by: [No Grouping]

Name	Polling IP Address	C1_DeviceType (CP)	C2_OS (CP)	C3_Function (CP)	C4_Application (CP)
10.50.2.2	10.50.2.2				
<input checked="" type="checkbox"/> ipv4s2.nmsnll.local	10.50.2.61	Router	IOS	Network Device	Infrastructure
<input type="checkbox"/> ipv4s3.nmsnll.local	10.50.2.62	Router	IOS	Network Device	Infrastructure
<input type="checkbox"/> ipv6s2.nmsnll.local	10.50.2.63	Router	IOS	Network Device	Infrastructure
<input type="checkbox"/> ipv6s3.nmsnll.local	10.50.2.64	Router	IOS	Network Device	Infrastructure
<input type="checkbox"/> student01-VM	10.0.0.10	Server	2019	Server	Orion

Page 1 of 1 Page size 40 Displaying objects 1 - 6 of 6



### List Resources

The List Resources section allows you to select the interfaces and resources you are interested in managing.

Action: Select your laptop and click on 'LIST RESOURCES'.

You should see something very similar to this screen below.

### List Resources - DESKTOP-514M24G

Select resources and statistics to monitor:

Select:  ALL  NONE  ALL VOLUMES

CPU & Memory  
 Status & Response Time  
   ICMP (Ping) - Fastest  
   Status & Response Time Agent  
 Volume Utilization  
   Physical Memory  
   Virtual Memory  
   C:\ Label:OS Serial Number B6AFC208

Action: Click the 'ALL' button from the top menu and Click 'SUBMIT'.

Action: Select the Cisco Router in your network. Click the 'LIST RESOURCES' button.

Question: What do you see? Choose only the active interfaces. Does this change the overall status of the node? Yes/No

This page intentionally left blank.

## Step 7.

Manage Nodes

Show: **Nodes** SEARCH

Group by: [No Grouping]

Name	Polling IP Address	C1_DeviceType (CP)	C2_OS (CP)	C3_Function (CP)	C4_Application (CP)
10.50.2.2	10.50.2.2				
ipv4s2.nmsnil.local	10.50.2.61	Router	IOS	Network Device	Infrastructure
ipv4s3.nmsnil.local	10.50.2.62	Router	IOS	Network Device	Infrastructure
ipv6s2.nmsnil.local	10.50.2.63	Router	IOS	Network Device	Infrastructure
ipv6s3.nmsnil.local	10.50.2.64	Router	IOS	Network Device	Infrastructure
student01-VM	10.0.0.10	Server	2019	Server	Orion

ADD NODE CUSTOM PROPERTY EDITOR EDIT PROPERTIES LIST RESOURCES **ASSIGN POLLERS** MAINTENANCE MODE MORE ACTIONS DELETE

Page 1 of 1 Page size 40 Displaying objects 1 - 6 of 6

Next is the ‘ASSIGN POLLERS’ button. This button is used to assign specific device Pollers to a node in the event the information is not polled from the device natively by SolarWinds. This is often used on new Vendor devices and equipment or for some specific requirements.

Action: Select the Cisco Router then click the ‘ASSIGN POLLERS’ button on the menu bar shown above.

Action: Expand the Cisco Router Selection. Check each one of the Cisco Device Pollers and then click on ‘SUBMIT’.

Here we see many different types of pollers are already configured in our SolarWinds Web Console.

#### Nodes: Assign Pollers

What are pollers? Pollers are group of object identifiers (OIDs) that gather details for a technology like CPU & Memory. The results are automatically displayed inline with normal SolarWinds statistics. [» Manage Pollers](#)  
What are Universal Device Pollers (UnDPs)? UnDPs poll a single OID on any device in your network, like current fan state. The results are displayed in custom charts, gauges or tables. Manage UnDPs on your SolarWinds server, go to Start > All Programs > SolarWinds Orion > Network Performance Monitor > Universal Device Poller

Assign Universal Device Pollers (UnDPs) to the following selected nodes:

Nisgaa-02-sw

Example

- ciscoEnvMonFanState (The current state of the fan being instrumented.)
- ciscoEnvMonSupplyState (The current state of the power supply being instrumented.)
- ciscoEnvMonTemperatureStatusValue (The current measurement of the test point being instrumented.)
- ciscoEnvMonTemperatureStatusValueFahrenheit (The current measurement of the test point being instrumented, in ...)
- upsAdvBatteryCapacity (The remaining battery capacity expressed in percent of full capac...)
- upsAdvInputLineVoltage (The current utility line voltage in VAC.)
- upsAdvOutputLoad (The current UPS load expressed in percent of rated capacity.)
- upsBasicBatteryStatus (The status of the UPS batteries. A batteryLow(3) value indicates ...)
- vmGuestOS (Operating system running on this vm.)
- vmGuestState (Guest operating system ON or OFF.)

SUBMIT

CANCEL

## Step 8.

The screenshot shows the 'Manage Nodes' interface. A red box highlights the 'MAINTENANCE MODE' dropdown menu for a selected node. The menu includes options: MUTE ALERTS NOW, RESUME ALERTS (UNMUTE), UNMANAGE NOW, MANAGE AGAIN, and SCHEDULE... .

Name	Polling IP Address	C1_DeviceType (IP)	C2_OS (IP)	C4_Application (IP)
10.50.2.2	10.50.2.2			
ipv4s2.nmsnll.local	10.50.2.61	Router	iOS	Infrastructure
ipv4s3.nmsnll.local	10.50.2.62	Router	iOS	Infrastructure
ipv6s2.nmsnll.local	10.50.2.63	Router	iOS	Infrastructure
ipv6s3.nmsnll.local	10.50.2.64	Router	iOS	Network Device
student01-VM	10.0.0.10	Server	2019	Server

Here we have the option to place different maintenance status on our nodes. If an Authorized Service Interruption (ASI) was needed, then we would ‘Unmanage’ a node until the ASI was completed. We also can mute alerts and set a schedule of for node management. A schedule is good when there are special situations where users may close at night and turn off the equipment.

Action: Click on all other Desktop machines in your MANAGED NODES view and set them to ‘UNMANAGE NOW’. This will turn the status icon blue with a white ‘X’ in the center to notify you the node is unmanaged but still part of the database.

## Step 9.

The screenshot shows the 'Manage Nodes' section of a network management application. At the top, there's a toolbar with buttons for ADD NODE, CUSTOM PROPERTY EDITOR, EDIT PROPERTIES, LIST RESOURCES, ASSIGN POLLERS, MAINTENANCE MODE, and MORE ACTIONS. Below the toolbar is a table listing network nodes. The columns include Name, Polling IP Address, C1\_DeviceType, C2\_OS, and C3\_Function. Several nodes are listed, including 10.50.2.2, ipv4s2.nmsn1.local, ipv4s3.nmsn1.local, ipv6s2.nmsn1.local, ipv6s3.nmsn1.local, and student01-VM. A red box highlights the 'MORE ACTIONS' dropdown menu on the right side of the table, which contains 16 items: POLL NOW, REDISCOVER, USE POLLED STATUS, SHUT DOWN, ENABLE, OVERRIDE POWER LEVEL, MANAGE ENERGYWISE, UPDATE TOPOLOGY, IMPORT CUSTOM PROPERTY VALUES, EXPORT CUSTOM PROPERTY VALUES, CANCEL PLANNED UNMANAGE, ADD NODES TO NCM, REMOVE NODES FROM NCM, ENABLE LOG MONITORING, and DISABLE LOG MONITORING. The 'MORE ACTIONS' menu has a page number indicator 'Page 1 of 6' at the bottom right.

Name	Polling IP Address	C1_DeviceType	C2_OS	C3_Function
10.50.2.2	10.50.2.2			
ipv4s2.nmsn1.local	10.50.2.61	Router	iOS	Network Device
ipv4s3.nmsn1.local	10.50.2.62	Router	iOS	Network Device
ipv6s2.nmsn1.local	10.50.2.63	Router	iOS	Network Device
ipv6s3.nmsn1.local	10.50.2.64	Router	iOS	Network Device
student01-VM	10.0.0.10	Server	2019	Server

Let's take a look at some of the toolbar items here in the Manage Nodes section. Here we see different options to perform polling and administrative duties on our nodes. Notice the 'ADD NODES TO NCM' at the bottom of the list. If you should happen across a network device that should be managed under NCM, you can add it to NCM here instead of running a Network Discovery Wizard.

Action: Click on 'MORE ACTIONS'.

## Step 10.

Manage Nodes

Show: Nodes

Group by: Vendor

	Name	Polling IP Address	C1_DeviceType (CP)	C2_OS (CP)	C3_Function (CP)	C4_Application (CP)
<input checked="" type="checkbox"/> student01-VM	student01-VM	10.0.0.10	Server	2019	Server	Orion

**EDIT PROPERTIES** (highlighted with a red box and circled with a red circle)

Next is the ‘EDIT PROPERTIES’ Page. This is the location where you can set node properties, polling, and activities.

**Edit Properties**

Edit Properties of the following selected nodes:

student01-VM

Name: **student01-VM**

Polling IP Address: **10.0.0.10**   
IPv4 and IPv6 formats are both valid

Dynamic IP Address (DHCP or BOOTP)

View type used for displaying details about this node

View Type: **(default)**

Status rollup mode:

Status rollup mode: **Mixed** [What does this mean?](#)

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 element on the node but not the node itself.

**Status Only: ICMP**  
Limited data (status, response time, and packet loss) is collected using ICMP (ping). Useful for devices which do not support SNMP or WMI.

**Most Devices: SNMP and ICMP**  
Standard polling method for network devices such as switches and routers, as well as Unix/Linux servers.

**Windows Servers: WMI and ICMP**  
Recommended agentless polling method for Windows servers.

**Windows & Unix/Linux Servers: Agent**  
Optional agent useful for monitoring Windows & Unix/Linux hosts in remote or distributed environments, such as the cloud. Credentials are needed only for installing the agent. The agent does not need to be installed on the server already. [What is an agent?](#)

Agent software is installed on student01-VM.

**VMware, Hyper-V or Nutanix entities:**  
Use to monitor VMware, Hyper-V or Nutanix entities.

**Meraki Wireless: API**  
API based polling for Meraki wireless gear.

The top portion is reserved for the node name and IP address. Both can be changed if needed.

The Polling Method is used to tell SolarWinds how to poll and monitor the device. There are several different options here.

ICMP would be used for nodes which may not be underneath your authoritative control.

SNMP would be used for your networking devices or servers.

Windows Servers would use WMI/ICMP or SolarWinds Agents.

Linux Servers would use a Linux Agent.

The screenshot shows the configuration interface for managing a node. It includes three main sections:

- Polling:** Set to Node Status Polling: 120 seconds and Collect Statistics Every: 10 minutes. The Polling Engine is set to DESKTOP-514M24G (Primary). A "CHANGE POLLING ENGINE" button is available.
- Dependencies:** Shows Parent (other objects dependent) and Child (dependent on other object) fields.
- Category:** Set to Auto-detected (Other).

The bottom section here is where you can control the frequency at which you would poll your device. Do not set less than 30 seconds. The poll may not return in time for the next poll to be sent. If you have nodes that are not critical, then maybe these nodes could be polled every 5-8 minutes instead of 2 minutes.

#### Action:

For this lab we will set the following:

Your SolarWinds Server: 4 minutes

Cisco Device: 1 minute

Other Nodes: 10 minutes

Dependencies can be either automatically built with SolarWinds or manually built. Those networking devices that use a neighbor protocol or features will build dependencies automatically, but for those devices that don't like Taclanes, then a manual build will be required.

Custom Properties

C1_DeviceType:	Router	▼
What type of device is this node?		
C2_OS:	iOS	▼
What Operating System is used on this device?		
C3_Function:	Network Device	▼
What function does this device serve?		
C4_Application:	Network Device	▼
What application is the primarily on this device?		
L1_Base:	JBSA San Antonio	▼
Where is this node located?		
L2_Building:	1435	▼
What building is this node located?		
L3_Room:	1011	▼
Which rack is used to house this node?		
L4_Rack:	101	▼
Where in the rack is this node located or what unit level is the top edge of the device?		

Here we can modify the custom property settings for the node.

Web Browse Template	<input type="text" value="http://{{ HrefIPAddress }}"/>	How users will navigate to the node using http or https in the Node Details resource
SSH Port	<input type="text" value="22"/>	Port in which ssh service is running
Active Directory Domain Controller	<input type="checkbox"/> Poll to monitor Active Directory users logged in to your network	
Node Thresholds		
CPU Load	<input type="checkbox"/> Override Orion General Thresholds	
Warning:	greater than or equal to 80 %	
Critical:	greater than or equal to 90 %	
Capacity Trending	Calculate exhaustion using average daily values	
Memory Usage	<input type="checkbox"/> Override Orion General Thresholds	
Warning:	greater than or equal to 80 %	
Critical:	greater than or equal to 90 %	
Capacity Trending	Calculate exhaustion using average daily values	
Response Time	<input type="checkbox"/> Override Orion General Thresholds	
Warning:	greater than or equal to 500 ms	
Critical:	greater than or equal to 1000 ms	
Percent Packet Loss	<input type="checkbox"/> Override Orion General Thresholds	
Warning:	greater than or equal to 30 %	
Critical:	greater than or equal to 50 %	
Cisco ACI Controller Polling Settings	<input type="checkbox"/> Poll for Cisco ACI	
Palo Alto Polling Settings	<input type="checkbox"/> Poll for Palo Alto	
CLI Polling Settings:	<input type="checkbox"/> Enable CLI Polling » <a href="#">Learn More</a>	
	Enable polling for Cisco Nexus, Cisco ASA or Palo Alto firewalls and discover VPN details, security zones, high availability health, vPCs, and more.	

Above we are given the opportunity to override the default thresholds natively configured by SolarWinds.

Yes  Manage node(s) with NCM

**NCM Properties**

**Node Details**

Node Group:

Node Comments:

**Connection Profile**

Global Connection Profiles: <No Profile>

Login Credentials: Device

Username: \${GlobalUsername}  
Password:   
Enable Level: \${GlobalEnableLevel}

Enable Password:   
Execute Scripts Using: \${GlobalExecProtocol}

Request Configs Using: \${GlobalConfigRequestProtocol}

Transfer Configs Using: \${GlobalConfigTransferProtocol}

Telnet Port: \${GlobalTelnetPort}

SSH Port: \${GlobalSSHPort}

**Communication**

Device Template: Auto Determine

Allow Terminal Server Support: No

Use Keyboard Interactive Authentication: No

This is where you set the NCM settings for the node.

If you want to place the node in an NCM group, you would configure in the top portion here.

In the Connection Profile section, you would select the credential used to access the device from a drop-down menu system. Do not use personal accounts or group accounts here. This should be configured with a service account. This section will auto-populate with the settings configured in the Connection Profile section when you originally configured the account.

The Communication Section is where the Device Template to be used can be defined. By default, it is configured with Auto Determine. Best practice is to hard code this item to solidify which Device Template to use every time.

Action: Click ‘SUBMIT’ to exit.

This concludes the lab exercise.

This page intentionally left blank.

# Lab 08 - Network Atlas

Welcome to the Network Atlas lab. This lab will show you how to create maps to display on your dashboards in your SolarWinds solution.

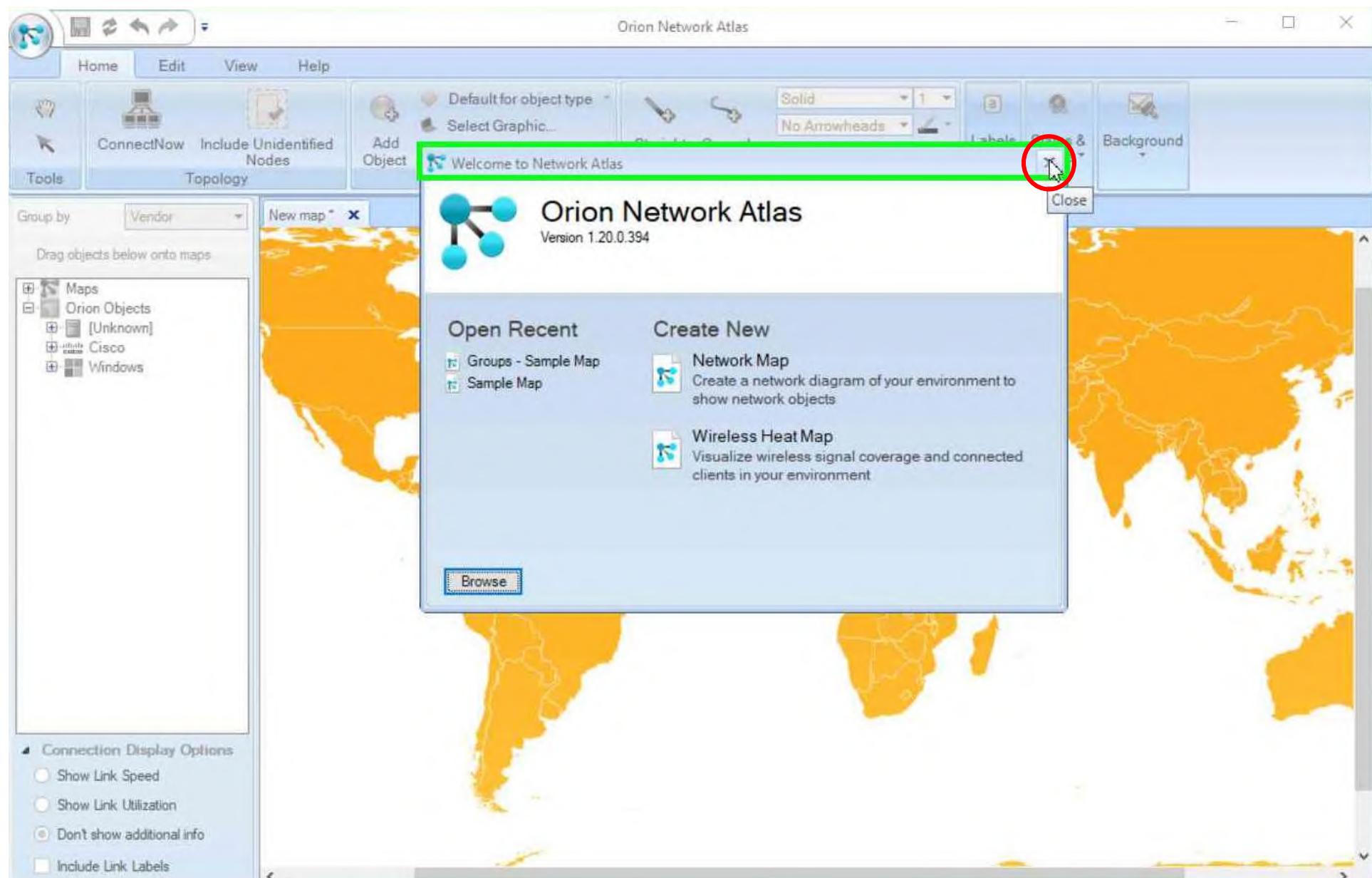
## Step 1. (Only used when not already working directly from the Orion Server)



To access the Network Atlas program, you will need to Remote Desktop Protocol into your SolarWinds Server. Network Atlas is a small executable on the SolarWinds server. Since it is an executable, Air Force IT Policies prohibit any user from running executables from their individual workstations.

Action: You will need to Remote Desktop Protocol (RDP) into your SolarWinds Server. Once logged in navigate to Start > SolarWinds > Network Atlas > Right Click 'Run as Administrator'.

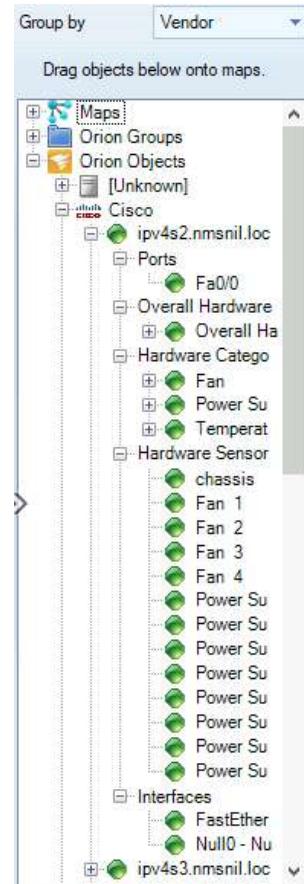
## Step 2.



Action: Click on the ‘X’ on the Product window in the middle of the screen.

Here is the front page of Network Atlas. By default, the program opens with a blank map of the world. Maps are created by drag and drop items from the left on to the palate on the right. Objects include, other Maps, Groups, Nodes, and Interfaces. A nested map is basically a map within a map.

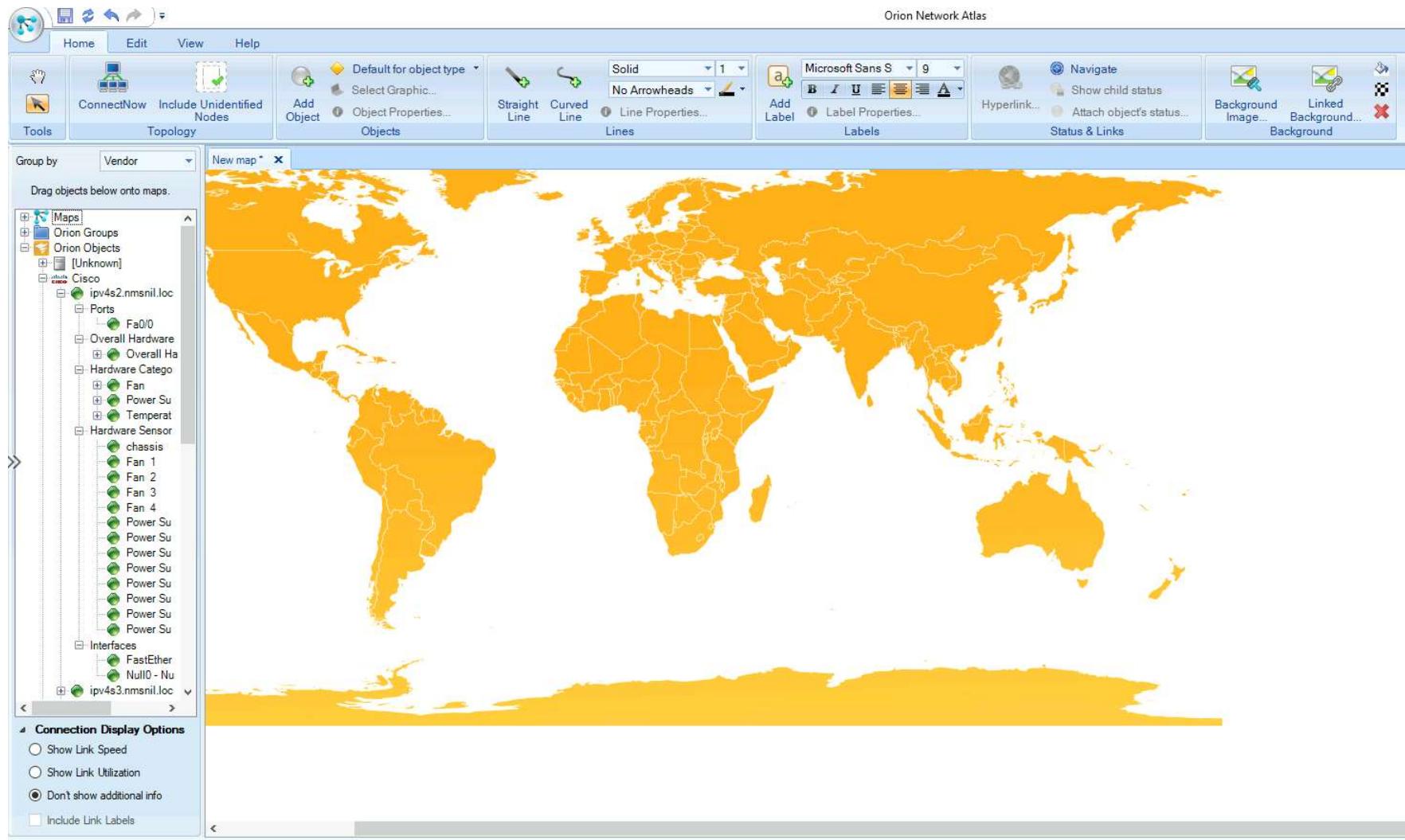
### Step 3.



On the left-hand side of the window we have the ability to add Maps, Orion Groups, and Orion Objects. If you expand these objects, we see the different elements for us to use to build our map.

Action: Time will be given for you to create a couple maps.

## Step 4.



First let take a short drive around the interface. The Edit tab on the top toolbar will allow you to do perform basic document editing tasks. Second, the View tab will provide you with some basic viewing techniques. Third, the Help tab will provide some basic help options.

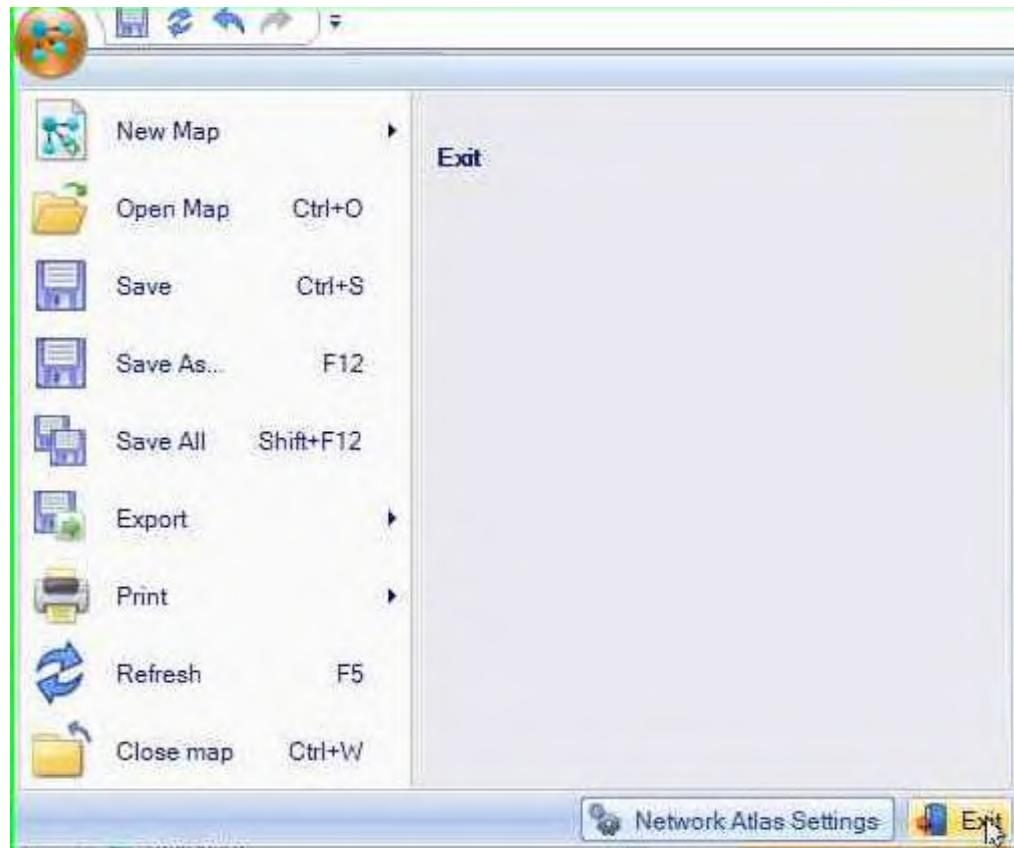
## Step 5.



We can drag and drop any of the nodes, groups, maps, objects or elements on to a background to provide the basis of a network or status map.

Action: Find the Cisco Router in your Objects Section and place all Ports onto the map.

## Step 6.



In the upper left corner of the interface you can find the File options. This will provide some basic Save, Export, New Map, and such.

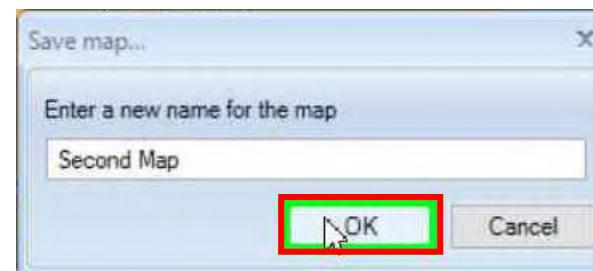
The Exit program button is located here as well.

Action: Click on 'Save' to save this map. Name the map "First Map".

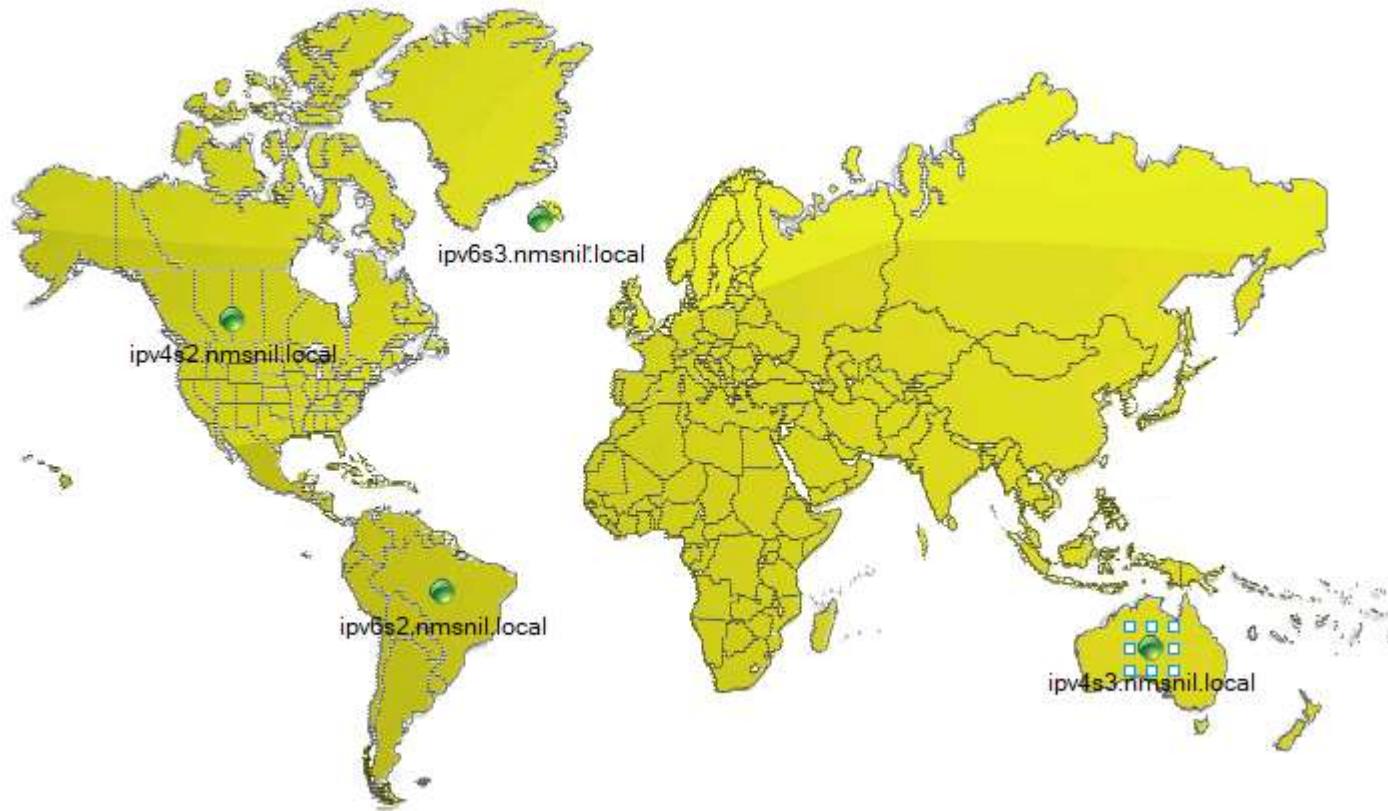
## Step 7.



Action: Create a second map and place all the workstations in your network on the map. Save this map with a name of “Second Map”



## Step 8.



Action: Create a third map. Now drag and drop the first two maps on to the palette. Save this map with a name of “Third Map”.

By placing a map icon into another map, you have just created a Nested map. If you double click on the map Icon it will take you inside that map.

This concludes the lab exercise.

# Lab 09 –Alerts

This lab will help develop alerts for your organization to act upon and resolve issues in your environment.

## Step 1.

The screenshot shows the SolarWinds Orion interface under 'Main Settings & Administration'. The top navigation bar includes 'MY DASHBOARDS', 'ALERTS & ACTIVITY', 'REPORTS', and 'SETTINGS'. The main content area is divided into sections: 'GETTING STARTED WITH ORION', 'NODE & GROUP MANAGEMENT', and 'ALERTS & REPORTS'. The 'ALERTS & REPORTS' section contains links for managing alerts, reports, SMTP servers, and ServiceNow instances. A red arrow points to the 'Manage Alerts' link.

- » Manage Alerts
- » Configure Default Send Email Action
- » Manage Reports
- » ServiceNow Instances
- » Manage SMTP Servers

SolarWinds Alerts is a powerful tool to inform you of an issue in your environment. They can be set up using a wide variety of information gathered from a node or the status of an interface.

Action: Select ‘Manage Alerts’ from the ALERTS & REPORTS menu.

## Step 2.

## Manage Alerts

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

The screenshot shows the 'Manage Alerts' page in SolarWinds. At the top, there are two tabs: 'ALERT MANAGER' (selected) and 'ACTION MANAGER'. Below the tabs, there is a dropdown menu for 'GROUP BY' set to '[No Grouping]'. A horizontal toolbar contains several buttons: '+ ADD NEW ALERT', 'EDIT ALERT', 'DUPLICATE & EDIT' (which is highlighted with a red box), 'ENABLE/DISABLE', and a refresh icon. The main area is a grid of alert entries. Each entry has a checkbox for 'Alert Name', a description, and a 'Enabled (On/Off)' switch. The descriptions include: 'Multicast routing group is down', 'Multicast routing group status is not normal', 'Multicast routing group traffic too low (bps)', 'Multicast routing group traffic too low (pps)', 'Neighbor is down', 'Network Discovery and Import complete', 'Network Discovery Failed', 'New Firmware Vulnerability Detected', 'No polling engine update in last 10 minutes', 'Node deleted', 'Node is down' (with a checked checkbox), 'Node is in a Warning or Critical State', 'Node not polled in last 10 minutes', 'Node polling failed on last 5 tries', and 'Node rebooted'. All 'Enabled (On/Off)' switches are currently set to 'OFF'.

In this lab we will be duplicating and editing an alert that comes natively with your SolarWinds software. The Alerts that come with your software have a limitation to most of them that prohibit you from modifying certain areas of the alert. Therefore, SolarWinds has decided to provide the DUPLICATE & EDIT button. This will give you full access to the alert to modify as you wish. Besides, you never want to modify the master template in the first place.

Action: Check the box next to 'Email me when a Node goes down' alert, then click on the 'DUPLICATE & EDIT' button on the top of the page.

### Step 3.

Edit Alert

PROPERTIES > TRIGGER CONDITION > RESET CONDITION > TIME OF DAY > TRIGGER ACTIONS > RESET ACTIONS > SUMMARY >

**1. Alert Properties**

Name of alert definition (required)  
502d - Node is down 

Description of alert definition  
Displayed on Manage alerts page.  
This alert will write to the SolarWinds event log when a node goes down and when a node comes back up again.

Enabled (On/Off)  
 ON

Evaluation Frequency of Alert  
Evaluate the trigger condition every  minutes ▾  
Event-based trigger conditions do not use the evaluation frequency.

Severity of alert  
 ⓘ

Alert Limitation Category  
Restrict access to this alert to user accounts with the selected alert limitation  
 ▾

First thing we want to do is to edit the name. We do not want the word ‘Copy’ anywhere on our system. This word signifies to everyone else that may use the system, that the previous user never finished setting up the alert and thus shall be deemed as trash and will be deleted.

Action: Modify the name to reflect your organizations number and name of alert definition.

Action: Enable the Alert

## Step 4.

### 1. Alert Properties

Name of alert definition (required)

502d - Node is down

Description of alert definition

Displayed on Manage alerts page.

This alert will write to the SolarWinds event log when a node goes down and when a node comes back up again.

Enabled (On/Off)

ON

Evaluation Frequency of Alert

Notice

Informational

Warning

Serious

Critical

Trigger condition every 1 minutes ▾

conditions do not use the evaluation frequency.



Alert Limitation Category

Restrict access to this alert to user accounts with the selected alert limitation

(No Limitation) ▾

Here we can change the severity of the alert.

Action: Select 'Critical'

## Step 5.

### 2. Trigger Condition

Trigger condition is simple condition or set of multiple nested conditions which must be met before the alert is triggered. »[Learn more](#)

I want to alert on:

Node

The scope of alert: [\(i\)](#)

- All objects in my environment ([Show List](#))  
 Only following set of objects

The actual trigger condition:

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

Status has changed (Node Event) - Event must occur at least 1x

and

**Node Status is equal to Down**

+

» Advanced options

[IMPORT](#) [EXPORT](#)

On the Trigger Condition Page, we can provide criteria for the purpose of alerting on conditions. You may select All, or, some of the conditions that must be met for the alert to activate. Take a moment to review some of the drop-down menus here to provide you with additional options.

Action: Click 'NEXT' at the bottom of the page.

## Step 6.

### 3. Reset Condition

When the reset condition is met the alert is removed from active alerts. »[Learn more](#)

- Reset this alert automatically after  minutes
- No reset condition - Trigger this alert each time the trigger condition is met
- No reset action - Manually remove the alert from the active alerts list
- Create a special reset condition for this alert

I want to alert on:



The scope of alert:

- All objects in my environment ([Show List](#))
- Only following set of objects

The actual trigger condition:

Trigger alert when

All child conditions must be satisfied (AND)

⋮ Status has changed (Node Event) - Event must occur at least 1x

and

⋮ Node Status is equal to

► Advanced options

[IMPORT](#) [EXPORT](#)

Reset conditions can be done through different situations. For this exercise, we will be leaving the reset condition as previously configured.

As seen above we can set a reset condition based on conditional statements and configurations.

Action: Click 'NEXT' at the bottom of the page.

## Step 7.

### 4. Time of Day

Time of Day controls when specified network objects should be monitored. This helps to avoid unwanted alerting noise during the expected outage or maintenance of your network (e.g. Your server reboot time is scheduled every Friday at 11:00 PM). [»Learn more about Time of Day usage](#)

Alert is always enabled, no schedule needed

Specify time of day schedule for this alert

BACK **NEXT** CANCEL

We can alert based on times of the day. Again, SolarWinds knew we had some users that like to turn off all equipment at the end of day. Now we can only have our alerts on during business hours.

Click 'NEXT' at the bottom of the page.

## Step 8.

### 5. Trigger Action

When the trigger condition is met the following actions in following order will be executed. You can also specify the escalation behavior if the alert is not being acknowledged in certain time.

[»Learn more about Actions and Escalation](#)

#### Message displayed when this alert is triggered

Displayed on All active alerts page/resource and on Alert details page. This message can be reused also for email action.

INSERT VARIABLE

#### Trigger Actions:

Escalation Level 1 (When the alert is triggered, all actions in this level fire.)				
ACTION TITLE		EDIT	COPY	SIMULATE
:: 502d - NetPerfMon Event Log : Node \${NodeName} is \${Status}. 				
::  502d - Send an Email/Page (ALERT: Node \${NodeName} is \${Status}) 				
<a href="#">Add Action</a> <a href="#">Assign Action(s)</a>				
<a href="#">Add Escalation Level</a>				

## Step 9.

Configure Action: Log The Alert To The NetPerfMon Event Log ×

Name of action  
502d - NetPerfMon Event Log : Node \${NodeName} is \${Status}.

▼ Log the Alert to the NetPerfMon Event Log settings

Message to send to Network Performance Monitor Event Log  
Node \${NodeName} is \${Status}.

**INSERT VARIABLE**

► Time of Day No additional schedule for this action needed

► Execution settings Execute if acknowledged already.

**SAVE CHANGES** CANCEL

Action: Modify the name of the Action as shown above. We want to remove the words “Copy of” and replace with our Unit number i.e. “502d”.

## Step 10.

Configure Action: Send An Email/Page ×

Name of action  
502d - Send an Email/Page (ALERT: Node \${NodeName} is \${Status})

▼ 1. Recipients

To  
\${DefaultEmailTo} Delete

CC  
\${DefaultEmailCC} Delete

BCC

► Sender details: (\${DefaultEmailFrom})

► 2. Message ALERT: Node \${NodeName} is \${Status}

► 3. SMTP Server 192.168.1.136

► Time of Day No additional schedule for this action needed

► Execution settings Execute if acknowledged already.

NEXT CANCEL

Again, we need to modify the name of this action.

## Step 11.

Configure Action: Send An Email/Page ×

Name of action  
502d - Send an Email/Page (ALERT: Node \${NodeName} is \${Status})

► 1. Recipients \${DefaultEmailTo}

► 2. Message ALERT: Node \${NodeName} is \${Status}

▼ 3. SMTP Server

Name of SMTP Server [What is an SMTP Server?](#) [Manage SMTP Servers](#)  
192.168.1.136

► Time of Day No additional schedule for this action needed

► Execution settings Execute if acknowledged already.

SAVE CHANGES CANCEL



Since we are sending an email to notify us of an issue, we will need to configure an email server.

Action: Use your IP Address of your workstation as the SMTP Server address. Then click ‘SAVE CHANGES’.

Trigger Actions give you the ability to provide action on alerts. This action ranges from sending emails, to playing a sound, to change node properties. Be careful, some actions are invasive ones and can lead to bigger problems.

## Step 12.

### Edit Alert - "502d - Node is down"

When reset condition of the alert is met the following actions and in following order will be executed...

ACTION TITLE	EDIT	COPY	SIMULATE	DELETE
:: 502d - NetPerfMon Event Log : Node \${NodeName} is \${Status}. ⚙				
:: ⏤ 502d - Send an Email/Page (RESET: Node \${NodeName} is \${Status}). ⚙				

Add Action   Assign Action(s)

Let's ensure the name of the actions meet our standards.

Step 13.

Configure Action: Log The Alert To The NetPerfMon Event Log ×

Name of action  
502d - NetPerfMon Event Log : Node \${NodeName} is \${Status}.

▼ Log the Alert to the NetPerfMon Event Log settings

Message to send to Network Performance Monitor Event Log  
Node \${NodeName} is \${Status}.

INSERT VARIABLE

► Time of Day No additional schedule for this action needed

→ **SAVE CHANGES** **CANCEL**

Action: Ensure the name of the action meets organizational standards.

Action: Click 'SAVE CHANGES' when complete.

## Step 14.

Configure Action: Send An Email/Page ×

Name of action  
502d - Send an Email/Page (RESET: Node \${NodeName} is \${Status}.)

► 1. Recipients \${DefaultEmailTo}

► 2. Message RESET: Node \${NodeName} is \${Status}.

▼ 3. SMTP Server

Name of SMTP Server What is an SMTP Server? [Manage SMTP Servers](#)  
192.168.1.136

► Time of Day No additional schedule for this action needed

→ SAVE CHANGES CANCEL

Action: Ensure the name of the action meets organizational standards.

Action: Ensure the IP address of your workstation is configured as the SMTP Server.

Action: Click 'SAVE CHANGES' when complete.

## Step 15.

### 7. Summary of Alert Configuration

Please review the alert configuration before saving...

**Name of alert:**

**502d - Node is down**

**Description of alert:**

This alert will write to the SolarWinds event log when a node goes down and when a node comes back up again.

**Type of Property to monitor**

Node

**Enabled(On/Off):**

ON

**Evaluation Frequency of alert:**

Every minute

**Severity of alert:**

Critical

**Alert Custom Properties: (0)**

No Alert Custom Properties defined

**Alert owner (user who created this alert):**

admin

**Alert Limitation Category**

No Limitation

**Trigger Condition:**

The actual trigger condition:  
Node - Status - is equal to - Down

---

**Reset Condition:**

Node - Status - is not equal to - Down

---

**Time of Day schedule:**

Alert is always enabled

---

**Trigger Action:**

Escalation Level 1

1. 502d - NetPerfMon Event Log : Node \${NodeName} is \${Status}.
  2. 502d - Send an Email/Page (ALERT: Node \${NodeName} is \${Status})
- 

**Reset Action:**

1. 502d - NetPerfMon Event Log : Node \${NodeName} is \${Status}.
  2. 502d - Send an Email/Page (RESET: Node \${NodeName} is \${Status}.)
- 

**» Alert Integration**

Here at the end of Alert, we have a review page. This will tell us everything about the alert we just configured/modified on a single page. Once we are satisfied with the Alert, we will submit the alert for action.

Action: Click 'NEXT'.

## Step 16.

### Manage Alerts

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

ALERT MANAGER		ACTION MANAGER		
GROUP BY:		Search...		
Alert Name	Enabled (On/Off)	Alert Description	Property to Monitor	Trigger Action(s)
502d - Node is down	ON	This alert will write to the SolarWinds event log when a nod...	Node	2 actions
502d - SolarWinds Server Utilization Status	ON	We are checking the SolarWinds Servers for utilization and ...	Node	2 actions
Alert me and trigger an NCM action	OFF		Node	3 actions
Alert me when a new MAC address appears on network	OFF	User Device Tracker alert when new MAC address is added.	New MAC Address	0 actions
Alert me when a new MAC Vendor appears on network	OFF	User Device Tracker alert when new MAC Vendor is found i...	New MAC Vendor	0 actions

Now the Alert is active and running on the system.

Move on to the next page for part 2 of this lab.

In this section of the lab we will be building an Alert from the beginning to completion.

## Step 17.

### Manage Alerts

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

The screenshot shows a software interface titled 'Manage Alerts'. At the top, there are two tabs: 'ALERT MANAGER' (which is highlighted in dark blue) and 'ACTION MANAGER'. Below the tabs is a toolbar with several buttons: 'GROUP BY' (set to '[No Grouping]'), '+ ADD NEW ALERT' (highlighted with a red box), 'EDIT ALERT', 'DUPLICATE & EDIT', 'ENABLE/DISABLE', 'ASSIGN ACTION', 'EXPORT/IMPORT', and 'DELETE'. To the right of the toolbar is a search bar labeled 'Alert Name' and two filter dropdowns: 'Enabled (On/Off)' and 'Alert Description'. The main area below the toolbar is currently empty, showing a light gray background.

Action: Click on 'ADD NEW ALERT'.

## Step 18.

### 1. Alert Properties

**Name of alert definition** (required)  
502d - SolarWinds Server Utilization Status

**Description of alert definition**  
Displayed on Manage alerts page.  
We are checking the SolarWinds Servers for utilization and status

**Enabled (On/Off)**  
 ON

**Evaluation Frequency of Alert**  
Evaluate the trigger condition every  1 minutes ▾  
Event-based trigger conditions do not use the evaluation frequency.

**Severity of alert**  
 Critical ▾ ⓘ

**Alert Limitation Category**  
Restrict access to this alert to user accounts with the selected alert limitation  
 (No Limitation) ▾

Action: Fill out form as shown above.

Action: Click 'NEXT' when done.

## Step 19.

### 2. Trigger Condition

Trigger condition is simple condition or set of multiple nested conditions which must be met before the alert is triggered. »[Learn more](#)

I want to alert on:

Node ▼

The scope of alert: (i)

- All objects in my environment ([Show List](#))  
 Only following set of objects

The actual trigger condition:

Trigger alert when

All child conditions must be satisfied (AND) (v)

must exist for more than 2 minutes (v)

Node C4\_Application is equal to Orion

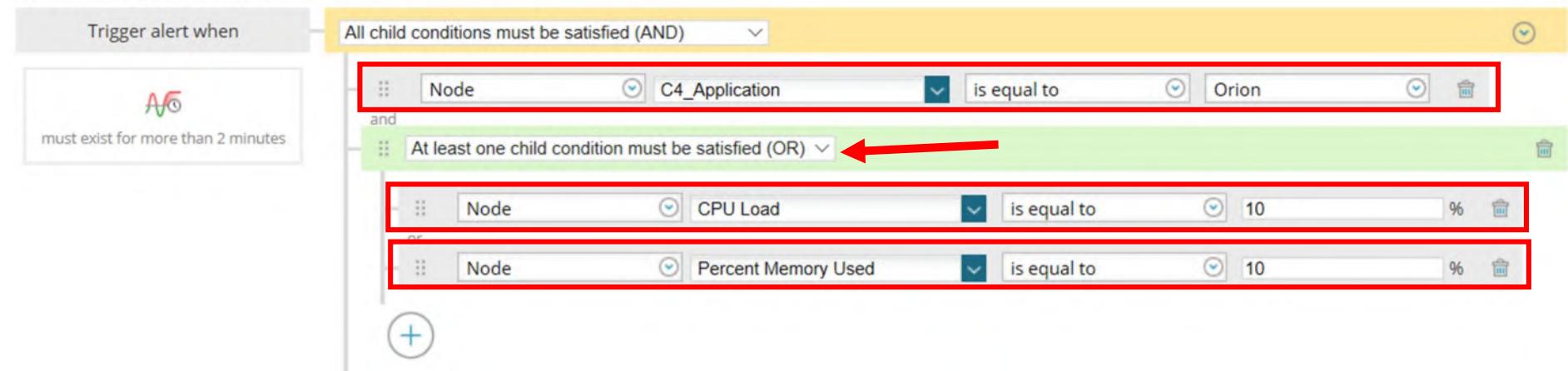
and

At least one child condition must be satisfied (OR) (v)

Node CPU Load is equal to 10 %

Node Percent Memory Used is equal to 10 %

+



Action: Fill out form as shown above.

## Step 20.

The actual trigger condition:

Trigger alert when

All child conditions must be satisfied (AND)

Node C4\_Application is equal to Orion

and

At least one child condition must be satisfied (OR)

Node CPU Load is equal to 10 %

or

Node Percent Memory Used is equal to 10 %

Condition must exist for more than 2 minutes

Advanced options

IMPORT EXPORT

This screenshot shows the configuration of a trigger condition. It starts with a main condition 'All child conditions must be satisfied (AND)' highlighted in yellow. This is followed by a 'Node' condition where 'C4\_Application' is compared to 'Orion' using the 'is equal to' operator. Below this is a 'and' connector. A nested condition 'At least one child condition must be satisfied (OR)' is shown in green, enclosed in a box. This contains two 'Node' conditions: one for 'CPU Load' set to 10% and another for 'Percent Memory Used' set to 10%. Both of these are connected by an 'or' connector. There are also '+' and '-' buttons for adding or removing conditions at the bottom of the tree structure. At the bottom left, there is a checkbox for 'Condition must exist for more than 2 minutes'. Below the main configuration area are 'Advanced options', 'IMPORT', and 'EXPORT' buttons.

Action Fill out form as shown above and then click 'NEXT'

## Step 21.

### 3. Reset Condition

When the reset condition is met the alert is removed from active alerts. »[Learn more](#)

- Reset this alert when trigger condition is no longer true (Recommended)
- Reset this alert automatically after  seconds ▾
- No reset condition - Trigger this alert each time the trigger condition is met
- No reset action - Manually remove the alert from the active alerts list
- Create a special reset condition for this alert

I want to alert on:

 ▾

The scope of alert: [\(i\)](#)

- All objects in my environment ([Show List](#))
- Only following set of objects

Action: Select ‘Create a special reset condition for this alert’.

## Step 22.

The scope of alert:  All objects in my environment ([Show List](#))  Only following set of objects

The actual trigger condition:

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

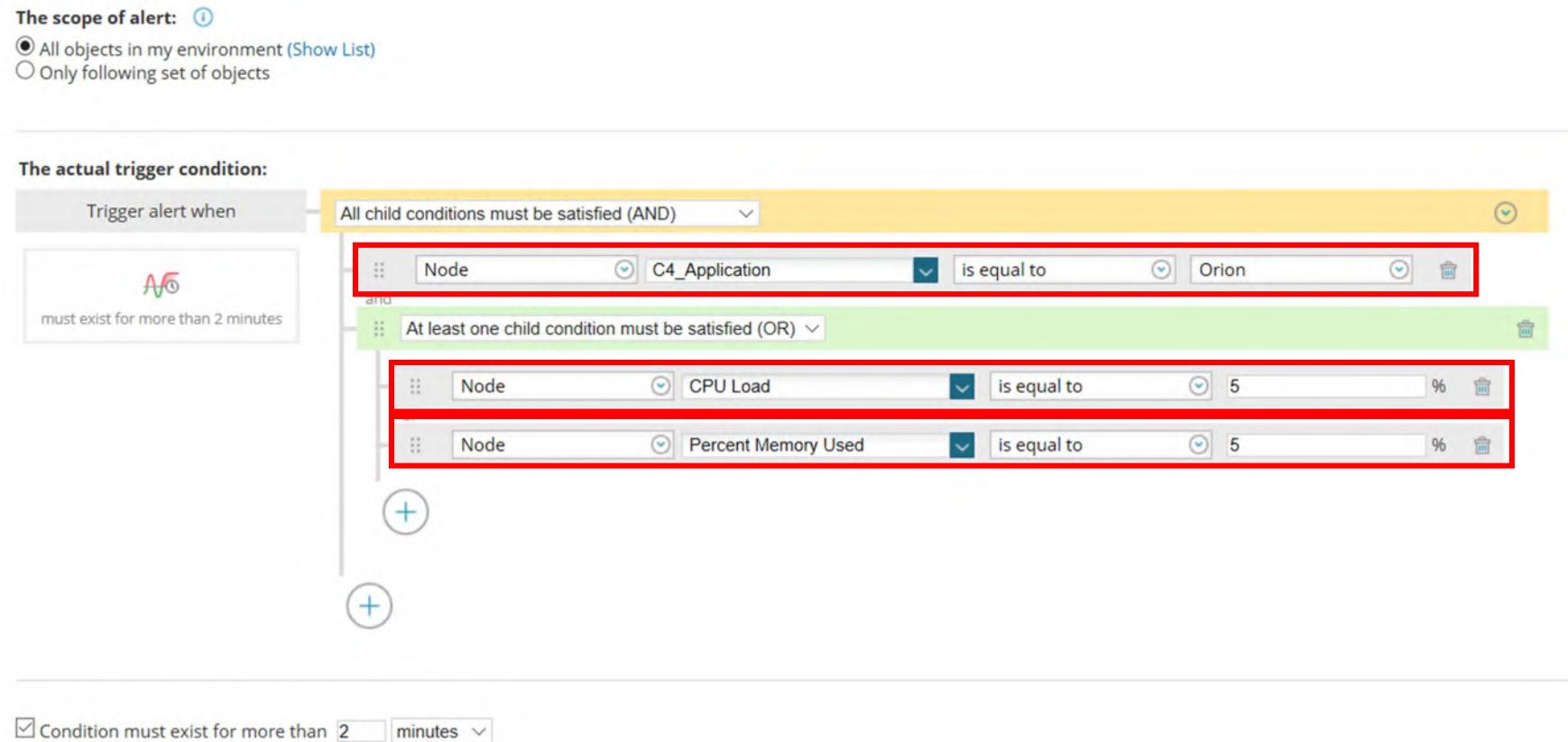
Node C4\_Application is equal to Orion

and  At least one child condition must be satisfied (OR)

Node CPU Load is equal to 5 %

Node Percent Memory Used is equal to 5 %

Condition must exist for more than 2 minutes



Action: Fill out form as shown above and then click 'NEXT' located in the lower right-hand corner.

Note: the 'NEXT' button is not shown here because it is in the very lower right-hand corner of the screen, which would make this screen hard to read for this operation.

## Step 23.

### Edit Alert - "502d - SolarWinds Server Utilization Status"

The screenshot shows the 'Edit Alert' interface for '502d - SolarWinds Server Utilization Status'. The 'TIME OF DAY' tab is active. A red circle highlights the first radio button, 'Alert is always enabled, no schedule needed'. Below it is another radio button for specifying a time of day schedule. At the bottom right are 'BACK', 'NEXT', and 'CANCEL' buttons.

Action: We want this alert to always be firing because we are looking at system level parameters.

## Step 24.

### 5. Trigger Action

When the trigger condition is met the following actions in following order will be executed. You can also specify the escalation behavior if the alert is not being acknowledged in certain time.  
»Learn more about Actions and Escalation

#### Message displayed when this alert is triggered

Displayed on All active alerts page/resource and on Alert details page. This message can be reused also for email action.

`${N=Alerting;M=AlertName} was triggered.`

INSERT VARIABLE

#### Trigger Actions:

The screenshot shows the 'Trigger Actions' section under 'Escalation Level 1'. It lists two actions: 'Send new Syslog Message to 192.168.0.136' and 'Alert for Utilization'. The first action is highlighted with a red box. At the bottom are 'Add Action' and 'Assign Action(s)' buttons. To the right are 'EDIT', 'COPY', 'SIMULATE', and 'DELETE' buttons.

Action: For the reset actions we will be to Add Action

- Send new Syslog Message to 192.168.0.136 or whatever your IP address would be.
- Alert for Utilization

We will cover these two items in the next few slides.

## Step 25.

Configure Action: Send A Syslog Message ×

Name of action  
Send new Syslog Message to 192.168.0.136

**Send a Syslog message settings**

Hostname or IP Address of Syslog Server  
**192.168.0.136**    
Multiple Syslog servers should be separated by commas.

10.23.4.10, 10.23.25.10 - Send Syslog message to multiple IP Addresses  
10.23.4.10:500 - Send Syslog message to 10.23.4.10 port 500  
Syslog.Solarwinds.Net - Send Syslog message to Syslog.Solarwinds.Net

Protocol: UDP ▼

Severity: Alert ▼      Facility: syslog message ▼

Message:  
SolarWinds Server is having an issue. Please investigate.  
INSERT VARIABLE

► Time of Day No additional schedule for this action needed

► Execution settings Do not execute if acknowledged already.

SAVE CHANGES CANCEL

Step 26.

Configure Action: Log The Alert To The NetPerfMon Event Log \*

Name of action  
Alert for Utilization

Log the Alert to the NetPerfMon Event Log settings

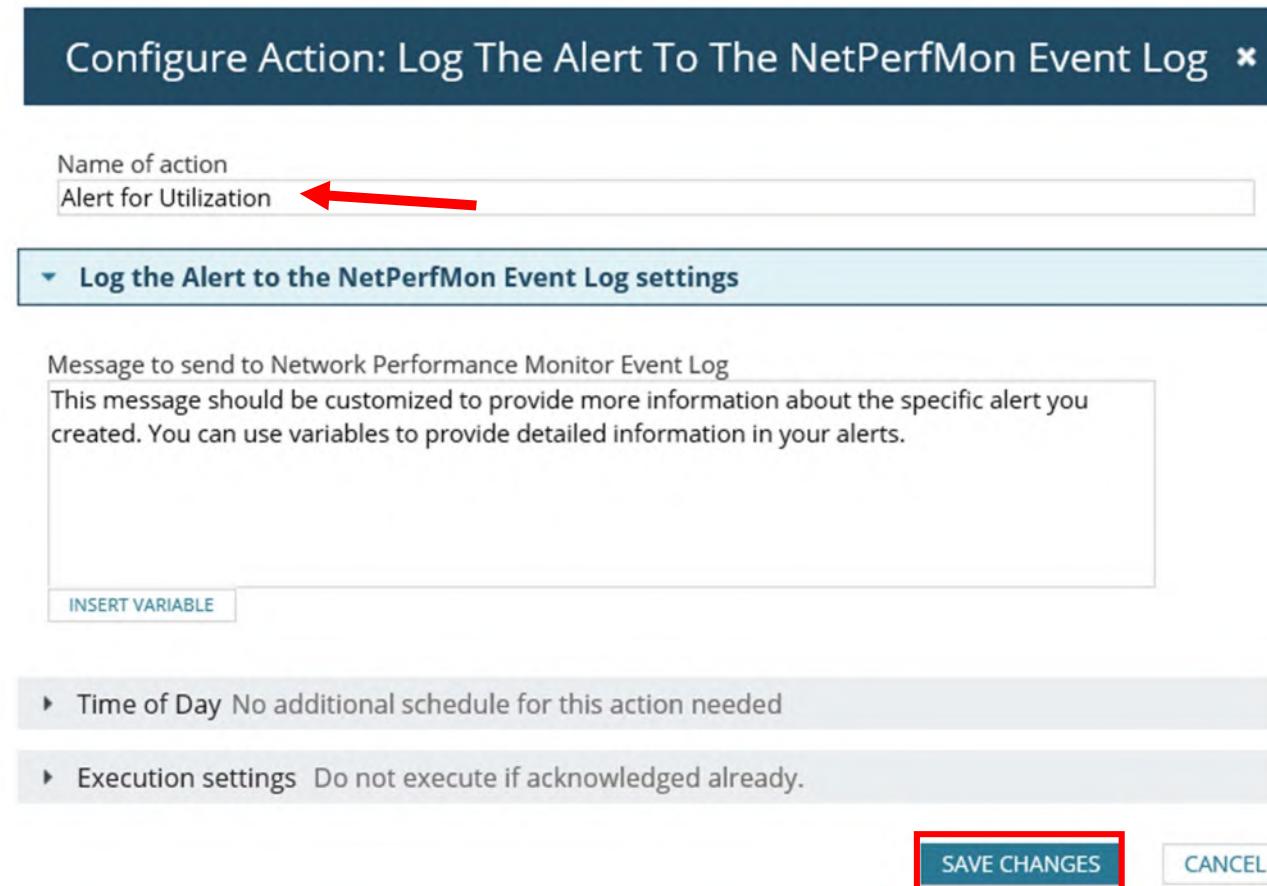
Message to send to Network Performance Monitor Event Log  
This message should be customized to provide more information about the specific alert you created. You can use variables to provide detailed information in your alerts.

INSERT VARIABLE

Time of Day No additional schedule for this action needed

Execution settings Do not execute if acknowledged already.

SAVE CHANGES CANCEL



Action: Ensure the 'Message to send to Network Performance Monitor Event Log' messages as shown above.

## Step 27.

### 6. Reset Action

When reset condition of the alert is met the following actions and in following order will be executed...

The screenshot shows a software interface for managing alert reset actions. At the top, there's a header with tabs for 'ACTION TITLE', 'EDIT', 'COPY', 'SIMULATE', and 'DELETE'. Below the header, a list displays a single action: 'Send new Syslog Message to 192.168.0.136'. Underneath this list are two buttons: 'Add Action' and 'Assign Action(s)'. At the bottom of the page, there are navigation buttons: 'BACK' and 'NEXT'. The 'NEXT' button is highlighted with a red rectangular box.

Our reset action will be to send a Syslog message to our Syslog server location which should be the IP address of your local machine.

Action: Click 'NEXT' when complete.

## Step 28.

Configure Action: Send A Syslog Message ×

Name of action  
Send new Syslog Message to 192.168.0.136

▼ **Send a Syslog message settings**

Hostname or IP Address of Syslog Server  
192.168.0.136  
Multiple Syslog servers should be separated by commas.  
10.23.4.10, 10.23.25.10 - Send Syslog message to multiple IP Addresses  
10.23.4.10:500 - Send Syslog message to 10.23.4.10 port 500  
Syslog.Solarwinds.Net - Send Syslog message to Syslog.Solarwinds.Net

Protocol: UDP

Severity: Alert Facility: syslog message

Message:  
The SolarWinds Server is having an issue.

INSERT VARIABLE

▶ Time of Day No additional schedule for this action needed

SAVE CHANGES CANCEL

Action: Verify the fields on this page are as shown above. IP Address of the Syslog Server should be the IP Address of your Workstation.

Action: Click 'SAVE CHANGES' when complete.

## 7. Summary of Alert Configuration

Please review the alert configuration before saving...

**Name of alert:**

**502d - SolarWinds Server Utilization Status**

**Description of alert:**

We are checking the SolarWinds Servers for utilization and status

**Type of Property to monitor**

Node

**Enabled(On/Off):**

ON

**Evaluation Frequency of alert:**

Every minute

**Severity of alert:**

Critical

**Alert Custom Properties: (0)**

No Alert Custom Properties defined

**Alert owner (user who created this alert):**

admin

**Alert Limitation Category**

No Limitation

**Trigger Condition:**

The actual trigger condition:

All child conditions must be satisfied (AND)

Nodes Custom Properties - C4\_Application - is equal to - Orion

At least one child condition must be satisfied (OR)

Node - CPU Load - is equal to - 10

Node - Percent Memory Used - is equal to - 10

---

**Reset Condition:**

All child conditions must be satisfied (AND)

Nodes Custom Properties - C4\_Application - is equal to - Orion

At least one child condition must be satisfied (OR)

Node - CPU Load - is equal to - 5

Node - Percent Memory Used - is equal to - 5

---

**Time of Day schedule:**

Alert is always enabled

---

**Trigger Action:**

Escalation Level 1

1.  Send new Syslog Message to 192.168.0.136 
  2.  Alert for Utilization 
- 

**Reset Action:**

1.  Send new Syslog Message to 192.168.0.136 
- 

**» Alert Integration**

Action: Click ‘SAVE CHANGES’ when complete.

## Step 30.

### Manage Alerts

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

ALERT MANAGER		ACTION MANAGER			
GROUP BY:		Search...			
[No Grouping]		+ ADD NEW ALERT   EDIT ALERT   DUPLICATE & EDIT   ENABLE/DISABLE   ASSIGN ACTION   EXPORT/IMPORT   DELETE			
<input type="checkbox"/>	Alert Name ▾	Enabled (On/Off)	Alert Description	Property to Monitor	Trigger Action(s)
<input type="checkbox"/>	502d - Node is down	ON	This alert will write to the SolarWinds event log when a nod...	Node	2 actions
<input type="checkbox"/>	502d - SolarWinds Server Utilization Status	ON	We are checking the SolarWinds Servers for utilization and ...	Node	2 actions
<input type="checkbox"/>	Alert me and trigger an NCM action	OFF		Node	3 actions
<input type="checkbox"/>	Alert me when a new MAC address appears on network	OFF	User Device Tracker alert when new MAC address is added.	New MAC Address	0 actions
<input type="checkbox"/>	Alert me when a new MAC Vendor appears on network	OFF	User Device Tracker alert when new MAC Vendor is found i...	New MAC Vendor	0 actions
<input type="checkbox"/>	Alert me when a rogue DNS name appears on network	OFF	User Device Tracker alert when rogue DNS name is detected.	Rogue DNSName	0 actions

Our new alert is now active on the system.

This concludes the lab exercise.

# Lab 10 – Reports

In this lab we will learn how to create a report from the information stored in the Orion SQL Database.

## Step 1.

The screenshot shows the Orion Platform interface. At the top left is a wrench icon next to the title "NODE & GROUP MANAGEMENT". Below it is a brief description: "Manage and delete nodes, dependencies and groups. Edit node properties." A grid of links follows:

» Manage Nodes	» Manage Virtual Devices	» Manage Dependencies
» Manage Groups	» Manage Agents	» Manage Custom Properties
» Manage Pollers	» Manage World Map	» Manage Device Templates
» Manage Hardware Sensors	» Manage Container Services	» Manage Orion Maps

---

Below this is another section titled "ALERTS & REPORTS" with a blue triangle icon. Its description is: "Create new alert / report or edit existing definitions." It contains three rows of links:

» Manage Alerts	» Manage Reports	» Manage SMTP Servers
» Configure Default Send Email Action		
	» Manage Alert Integration Instances	

A red box highlights the "» Manage Reports" link, and a cursor icon is positioned over it.

Let us start from the SETTINGS page.

Action: Scroll down to the ALERTS & REPORTS Section and click 'Manage Reports'.

## Step 2.

**Manage Reports**  
Reports may now be created in the web console. To get started, view our [training video](#) or review our [Reporting Guide](#).

**REPORT MANAGER**   **SCHEDULE MANAGER**

**GROUP BY:** Report Origin

All (367)   Web-based (333)   Report Writer (34)

**DUPLICATE & EDIT**

		Schedule assigned	Type
<input type="checkbox"/>	All Down Nodes	Displays all Nodes that are currently Down	Web-based
<input type="checkbox"/>	All Nodes	Report of all Nodes managed by NCM.	Web-based
<input type="checkbox"/>	All VMs	Show all monitored Virtual Machines	Web-based
<input type="checkbox"/>	Application Availability - Last Month		Web-based
<input type="checkbox"/>	Application Availability - This Month		Web-based
<input type="checkbox"/>	Application Availability - This Year		Web-based
<input type="checkbox"/>	ARP Tables	Shows the ARP Tables from each device. Run a...	Web-based
<input type="checkbox"/>	ASA Site-to-Site VPN Tunnel History - Last 30 D...	Displays historical info for all ASA Site-to-Site V...	Web-based
<input type="checkbox"/>	Availability - Last Month	Displays Last Month's Availability for each Node	ReportWriter
<input type="checkbox"/>	Availability - This Year	Displays the Availability for each Node for the ...	ReportWriter
<input type="checkbox"/>	Availability - Yesterday	Displays Yesterday's Availability for each Node	ReportWriter
<input type="checkbox"/>	Availability of Entire Network - Last Month	Displays the Average Availability of the Entire N...	ReportWriter
<input type="checkbox"/>	Available Space on each Volume	Displays the Space Available for each Volume	ReportWriter
<input type="checkbox"/>	Average and Peak Traffic - Last 7 Days	Display the Average and Peak Traffic rates for ...	Web-based
<input type="checkbox"/>	Average and Peak Traffic - Last Month	Display the Average and Peak Traffic rates for ...	Web-based
<input type="checkbox"/>	Average and Peak Traffic - This Month	Display the Average and Peak Traffic rates for ...	Web-based
<input type="checkbox"/>	Average and Peak Traffic - WAN Interfaces Last ...	Display the Average and Peak Traffic rates for ...	Web-based
<input type="checkbox"/>	Average CPU Utilization - This Week	Top 5 nodes with highest average CPU utilizati...	Web-based
<input type="checkbox"/>	Average Disk Performance - Last 7 Days		Web-based
<input type="checkbox"/>	Average Disk Space Used - Last 12 Months	Displays the Average and Peak Disk Space use...	Web-based

Page 2 of 19 | NUMBER OF ITEMS PER PAGE: 20

Locate the report All Down Nodes. There are many reports available to you that come with different SolarWinds products and the Orion Platform. You can also find additional report on Thwack. Since these are “Master” Reports, we do not want to edit those. SolarWinds has provided us with a DUPLICATE & EDIT button to allow us to safely edit a report without breaking the master report.

Action: Check the box to the left of the ‘All Down Nodes’ report

Action: Click the ‘DUPLICATE & EDIT’ button on the tool bar above.

### Step 3.

#### Edit Report

The screenshot shows the 'Edit Report' interface in a web-based application. At the top, there's a navigation bar with tabs: LAYOUT BUILDER (highlighted in blue), PREVIEW, PROPERTIES, SCHEDULE REPORT, and SUMMARY. Below the navigation, there's a 'Report width' input field set to 960 px, Fit to window width. The main area is divided into sections: 'Header' and 'Content'. In the Header section, there's a title '502d - All Down Nodes' and a description 'Displays all Nodes that are currently Down'. To the right of the title is a 'Logo' section with a checkbox checked, labeled 'Logo', and a 'BROWSE FOR LOGO' button. In the Content section, there's a 'Layout columns' selector set to 1, a '100%' width indicator, and a 'Page Layout' dropdown. The central content area contains a table definition for 'Down Nodes'. The table has a header row with columns for 'For' (set to 'Down Nodes') and 'Edit'. There's also an 'EDIT TABLE' button and an 'Edit' link. A red box highlights the 'EDIT TABLE' button. Below the table is a dashed box labeled 'Add Content'.

First things first, The Header. We do not want to see the word “Copy” anywhere in our system. It tells us that someone was investigating the system and has left behind some trash. We discard all our trash. Label the header with the Unit number as shown above, then the name of the report.

Action: Type ‘502d – All Down Nodes’

Second, we need to look at what is going to be pulled from the database to populate this report and how the report will look. In the content box, you will find an ‘EDIT TABLE’ button and an ‘Edit’ link.

## Step 4.

Edit Resource: Down Nodes for Down Nodes You can change this after submit.

Title: **502d - Down Nodes**

Subtitle:

Table layout: Edit column widths

VENDORICON	NODE	STATUS LED	<b>STATUS</b>	
Advanced	Advanced	Advanced	Advanced	

Database column: Node/Status Description

Display name: STATUS

Hide this column in the resulting table i

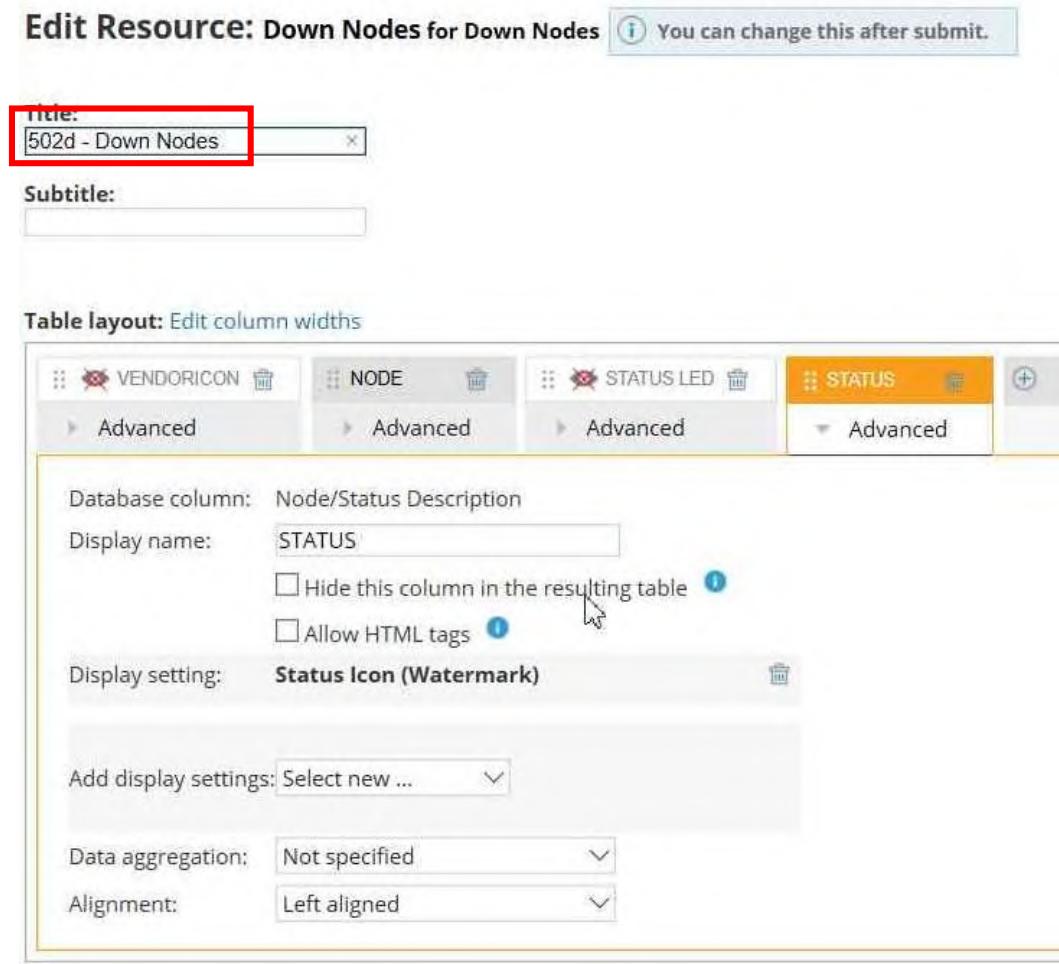
Allow HTML tags i

Display setting: Status Icon (Watermark) Edit

Add display settings: Select new ... ▼

Data aggregation: Not specified ▼

Alignment: Left aligned ▼



The EDIT TABLE button will help with the display of this report. You have the opportunity to manage the columns, how many objects to show, and sorting capabilities. We will not be changing anything here. Investigate each of the Table Columns for additional and advanced features for the column.

**Filter number of results:**

This table can include all the records retrieved, or records can be filtered.

 Show all records Show only the top  records Show only the top  % of records**Time-based settings:**

Do you only want to see data in the table above from a specific time period?  No 

**Sort results by:****Group results by:**

Here we are having the option to display the number of records to meet our needs. For our lab here we will leave the defaults.

Action: Click 'SUBMIT'.

## Step 5.

### Edit Report

The screenshot shows the 'Edit Report' interface. At the top, there's a navigation bar with tabs: LAYOUT BUILDER, PREVIEW, PROPERTIES, SCHEDULE REPORT, and SUMMARY. Below the navigation bar, the 'Report width' is set to 960 px, with an option to 'Fit to window width'. The main area is divided into sections: 'Header' and 'Content'. The 'Header' section contains the title '502d - All Down Nodes' and a description 'Displays all Nodes that are currently Down'. To the right of the header, there's a 'Logo' section with a checked checkbox labeled 'Logo' and a 'BROWSE FOR LOGO' button. The 'Content' section has a 'Layout columns' dropdown set to 1. Below this, there's a table titled '502d - Down Nodes' with an 'EDIT TABLE' button. An 'Edit' button in the table row is circled in red. A large 'Add Content' button is located at the bottom of the content area. On the right side of the content area, there are 'Page Layout' settings and a small 'x' icon.

Next, let's review the Data Source for this Report.

Action: Click the 'Edit' button to review the data source for this Report.

Add Content

1 Resource: Custom Table (Reporting)

2. Select objects you are going to report on...

**Selection method:**

Dynamic Query Builder  Basic Selector  Advanced Selector

I want to report on Node

Where At least one child condition must be satisfied (OR)

Status is equal to Unknown

Status is equal to Down

+ Add Simple Condition

Selection Name: 502d - Down Nodes

**ADD TO LAYOUT** **CANCEL**

The Edit link under the EDIT TABLE button provides you with Boolean type search parameters in order query the database for the information you want in your report. As we have seen in the Alerts lab, this operates in the same manner. This expression is telling us that we are looking for any of the conditions can match the status of a Node in the Unknown or Down state.

Action: Change the ‘Selection Name:’ to add your unit number and then click ‘ADD TO LAYOUT’.

Action: Then click ‘NEXT’.

## Step 6.

### Edit Report

LAYOUT BUILDER > PREVIEW > PROPERTIES > SCHEDULE REPORT > SUMMARY >

## 502d - All Down Nodes

Displays all Nodes that are currently Down

Summary of Orion Objects: **502d - Down Nodes**

502d - Down Nodes for 502d - Down Nodes	
NODE	STATUS
Linksys Router	● Node status is Down, Percent Packet Loss threshold is Critical.
Nisgaa-02-sw	● Node status is Down, Percent Packet Loss threshold is Critical, Hardware health monitoring is in Unknown state.
192.168.1.104	● Node status is Down, Percent Packet Loss threshold is Critical.
192.168.1.105	● Node status is Down, Percent Packet Loss threshold is Critical.
Nisgaa-01-sw	● Node status is Down, Percent Packet Loss threshold is Critical, Hardware health monitoring is in Unknown state, One or more interfaces are in an Unknown state.
192.168.0.1	● Node status is Down, Percent Packet Loss threshold is Critical.

Created on 2/15/2020. 502d Network Operations Group - CourtesyIT, LLC for additional support.

This is a preview of a sample report to ensure the data is displayed correctly.

Action: Click 'NEXT' when complete.

Note: The 'NEXT' button is buried in the lower right-hand corner and not shown above.

Step 7.

## Edit Report

LAYOUT BUILDER > PREVIEW > **PROPERTIES** > SCHEDULE REPORT > SUMMARY

 My Favorite Reports  
Reports marked as favorite are made easily available for frequent access,

**Report description:**  
Displays all Nodes that are currently Down

**Report category:**  
Used for group by purposes in View/Manage reports page  
Current Node Status

▶ **Report Limitation**  
User accounts that are assigned a specific report limitation category may only view reports in the specified report limitation category.

The next section will define the properties of the report. Again, we have the description field here. **ALWAYS PUT A DESCRIPTION!** It is easier to get into the habit then spending time trying to figure out what does what.

Action: Mark this report as a ‘Favorite’ then click ‘NEXT’ at the bottom of the page.

Step 8.

## Edit Report

The screenshot shows a navigation bar with tabs: LAYOUT BUILDER, PREVIEW, PROPERTIES, SCHEDULE REPORT, and SUMMARY. The SCHEDULE REPORT tab is highlighted in blue. Below the tabs, the title 'Schedule Report' is displayed in bold. A descriptive text follows: 'Report can be created regularly and be emailed to particular recipient, saved to disk or printed out.' Underneath, there are two radio button options: one selected ('No schedule needed') and one unselected ('Schedule this report to run regularly').

In the Schedule Report section, we have the capability to schedule and deliver these reports. Unfortunately, due to the nature of DoD computing, this feature is not allowed.

Action: We will select 'No schedule needed'.

Action: Click 'NEXT' at the bottom of the page.

Note: The 'NEXT' button is buried in the lower right-hand corner and not shown above.

## Step 9.

### Edit Report

LAYOUT BUILDER > PREVIEW > PROPERTIES > SCHEDULE REPORT > **SUMMARY**

#### Summary of report configuration

Please review the report configuration before saving...

##### ★ 502d - All Down Nodes

Displays all Nodes that are currently Down

**Description:**

Displays all Nodes that are currently Down

**Report Category:**

Current Node Status

**Custom properties assigned:**

**Report Limitation applied:**

Default

**Summary of Orion Objects used:**

502d - Down Nodes

**Summary of Time Periods used:**

**Resources used:**

502d - Down Nodes

**Report Schedule assigned:**

**Orion account to be used to generate scheduled report:**  
admin

**PREVIEW REPORT**

Show created report after saving

Here we have an opportunity to review our report for the features and criteria we desire.

Action: Click 'SUBMIT'.

Note: The 'SUBMIT' button is buried in the lower right-hand corner and not shown above.

## Step 10.

### Manage Reports

Reports may now be created in the web console. To get started, view our [training video](#) or review our [Reporting Guide](#).

The screenshot shows a web-based reporting interface. At the top, there are two tabs: "REPORT MANAGER" (which is selected) and "SCHEDULE MANAGER". Below the tabs, a "GROUP BY:" dropdown menu is set to "Report Origin". Underneath this, there are two buttons: "All (267)" and "Web-based (267)", with "Web-based (267)" being highlighted. A toolbar at the top right includes buttons for "CREATE NEW REPORT", "EDIT REPORT", "DUPLICATE & EDIT", "VIEW REPORT", "SCHEDULE REPORT", "EXPORT/IMPORT", and "DELETE". The main area displays a list of reports. The first report in the list is selected, indicated by a checked checkbox and a blue star icon. The report details are as follows:

Report Title	Description	Schedule assigned
502d - All Down Nodes	Displays all Nodes that are currently Down	
502d - Cisco Nodes	for all of our cisco nodes	
90/95/99th Percentile Traffic Rate - Last 7 Da...	Displays the 90/95/99th percentile traffic rat...	
90/95/99th Percentile Traffic Rate - Last Mon...	Displays the 90/95/99th percentile traffic rat...	

Here is our report.

Action: Select the report you just created/modified and click on the name to run the report.

What is the result?

[Continue to next section for an additional lab in building a report.](#)

## Step 11.

From the Reports Screen, click on ‘CREATE NEW REPORT’. The screen shot you see below is a navigational aide into the process of building a report from scratch. Click ‘GET STARTED’ to move forward with the lab.

What's New With Web-Based Reports? ×

**Creating Reports from the web console is brand new! A few tips:**

Watch this [training video](#), or read our [quick start guide](#) to get going quickly.  
You can still use the Orion Report Writer application on your SolarWinds server if you prefer. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Report Writer**.

**Add content**

- Select a resource, any resource or widget available in the web console can now be added to reports! (e.g. "Custom table" and "Custom chart" are fully customizable for reporting purposes).
- Choose a datasource (e.g. All Cisco nodes).

**Edit resource**

- Tweak the data in the resource (e.g. sort columns, group data, limit result to the top 10, etc.).

**Customize report layout**

- A single report can now contain multiple charts, tables and gauges!

**Preview report**

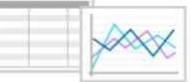
- Double-check that the report shows the needed data.

**Define properties**

- These properties will help you find this report later (e.g. mark this report as your favorite so it always appears at the top of the list)

**Schedule Report**

- Assign an existing schedule or create a new one (e.g. email your boss the "Network Health" report every Friday at 5pm)

**1**  **2**  **3**  **4**  **5**  **6** 

Add multiple resources (tables/charts) to single report and place them side-by-side if desirable!

Don't show this again

**GET STARTED!**

Getting Started with reports is very much like building Alerts. The functionality and “look and feel” is the same. Let’s get started!

## Step 12.

The screenshot shows a search interface for available resources. On the left, a sidebar lists options like Type, Alerts, Charts, etc. The main area has a 'GROUP BY:' dropdown set to 'Type'. A table lists resources: 'Custom Chart' under Category 'Reporting' and 'Custom Table' under Category 'Reporting'. A red circle highlights the radio button next to 'Custom Table', indicating it is selected. A search bar at the top right contains the placeholder 'Search all resources ...' and a 'SEARCH' button.

Resource name	Category
Custom Chart	Reporting
Custom Table	Reporting

Select the Type of report you would like to display. Take a moment to explore the other types of reports offered by SolarWinds. For our purpose here we will be selecting Custom Table.

Action: Select the radio button next to ‘Custom Table’.

Action: Click ‘SELECT AND CONTINUE’.

## Step 13.

Add Content

1. Resource: **Custom Table** (Reporting)

2. Select objects you are going to report on...

**Selection method:**

Dynamic Query Builder  Use DQB for selections such as 'All cisco nodes' where object selection may change over time. [Learn More](#)

Basic Selector  Advanced Selector

I want to report on **Node** ▼ ▼

+ Add Condition ▼

All Nodes are selected.

Selection Name: All Nodes

**ADD TO LAYOUT** **CANCEL**

The screenshot shows the 'Add Content' dialog box for creating a report. It's titled 'Add Content' and has a dark header bar. Below the header, there are two steps listed: '1. Resource: Custom Table (Reporting)' and '2. Select objects you are going to report on...'. The second step is highlighted with a light blue background. Under 'Selection method:', there is a 'Dynamic Query Builder' checkbox which is checked, followed by a note about using DQB for selections like 'All cisco nodes'. There are two radio buttons: 'Basic Selector' (which is selected) and 'Advanced Selector'. Below this, there is a dropdown menu set to 'Node'. To the right of the dropdown, a yellow box says 'All Nodes are selected.' with a small info icon. At the bottom left, there is a button labeled '+ Add Condition' with a red border around it. At the very bottom, there is a 'Selection Name:' field containing 'All Nodes' and two buttons on the right: 'ADD TO LAYOUT' and 'CANCEL'.

To start building the report you will need to add conditional statements to the report to allow SolarWinds to automatically manage the report data.

Click 'Add Condition'.

## Step 14.

The screenshot shows the 'Add Content' dialog box with the following steps:

1. Resource: Custom Table (Reporting)
2. Select objects you are going to report on...

**Selection method:**

Dynamic Query Builder  Use DQB for selections such as 'All cisco nodes' where object selection may change over time. [Learn More](#)

Basic Selector  Advanced Selector

I want to report on Node

Where All child conditions must be satisfied (AND)

**Vendor is equal to Cisco**

+ Add Simple Condition

Selection Name: Datasource 1

**ADD TO LAYOUT**

A red box highlights the condition "Vendor is equal to Cisco". A second red box highlights the "ADD TO LAYOUT" button.

Now we are in a familiar place. Does it not look just like an alert condition? Here we have the option to change from the Caption to another type of data field to build the report for the data we are seeking.

Action: After you have added the conditional statement, proceed to drop down labeled ‘Select field...’ and navigate the menu screen to select ‘Vendor’.

Action: Type the word “Cisco” in the corresponding box to finish the conditional statement.

## Step 15.

Edit Resource: Custom Table for Datasource 1

*(i) You can change this after submit.*

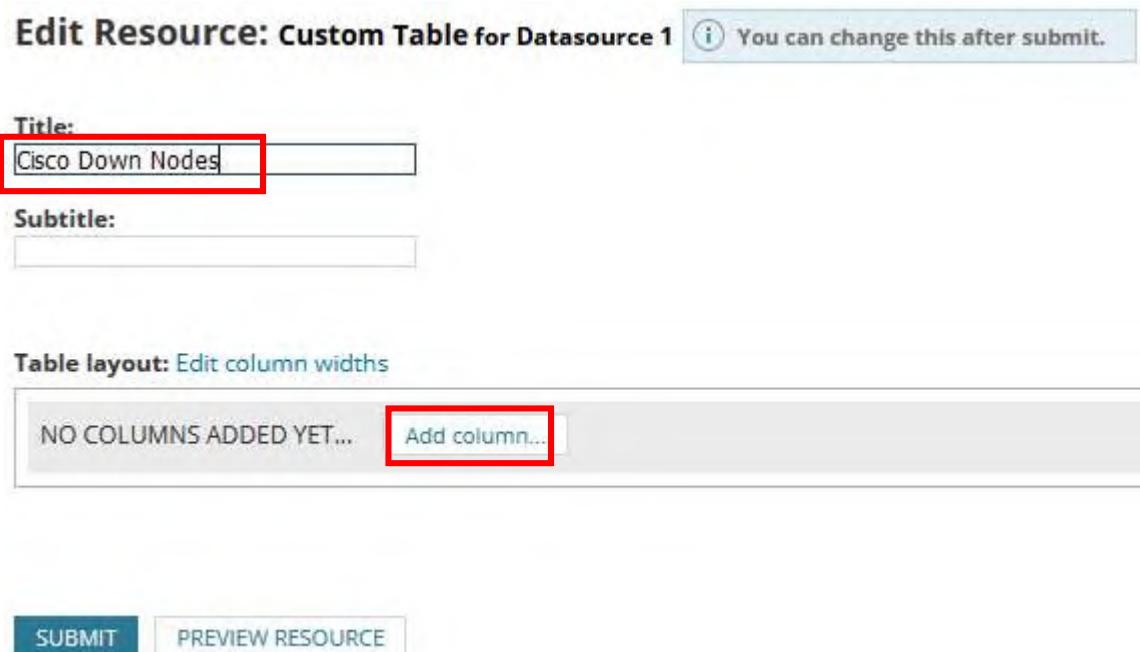
**Title:**  
Cisco Down Nodes

**Subtitle:**

**Table layout: Edit column widths**

NO COLUMNS ADDED YET... [Add column...](#)

[SUBMIT](#) [PREVIEW RESOURCE](#)



From here we will begin building the column in the report.

Click in the 'Add Column ...' box.

## Step 16.

The screenshot shows the 'Add Column' dialog box. On the left, there's a tree view of 'ORION OBJECTS' including 'Node', 'GROUP BY', 'Nodes', 'Application', 'Asset Inventory', and 'Drivers'. The 'Caption' and 'ID' columns are highlighted with red circles. The 'Caption' column is currently selected, indicated by a blue border. The 'Selected columns' section on the right is empty. At the bottom are 'ADD COLUMN' and 'CANCEL' buttons.

SolarWinds will give us the ability to select many different types information for our report. This data you see here is actually located in the database on the SQL Server.

Action: Select the following choices:

- Caption
- IP Address
- Status
- Vendor

When the selection has been identified, click the 'ADD COLUMN' button.

## Step 17.

Edit Resource: Cisco Down Nodes for Datasource 1 i You can change this after submit.

Title: Cisco Down Nodes

Subtitle:

Table layout: Edit column widths  

... CAPTION ...	... IP ADDRESS ...	... STATUS ...	... VENDOR ...	+ ...
▶ Advanced	▶ Advanced	▶ Advanced	▶ Advanced	

Filter number of results:  
This table can include all the records retrieved, or records can be filtered.

Show all records  
 Show only the top  records  
 Show only the top  % of records

Time-based settings:  
Do you only want to see data in the table above from a specific time period? No  i

Sort results by:

Group results by:

SUBMIT PREVIEW RESOURCE

Action: Click 'Edit column widths.'

## Step 18.

The screenshot shows the 'Resource Preview' dialog for 'Cisco Down Nodes for Datasource 1'. At the top, it says 'Column width settings:  Automatic  Custom'. A red circle highlights the 'Custom' radio button. Below this, a tip states: 'TIP: The width of column can be adjusted by dragging the orange line.' The main area displays a table with three columns: 'CAPTION', 'IP ADDRESS', and 'STATUS'. The 'STATUS' column contains the text 'No activity to report.' In the bottom right corner of the dialog, there are two buttons: 'SAVE COLUMN WIDTHS' (highlighted with a red box) and 'CANCEL'.

SolarWinds will auto-size the columns for you. This may affect the way the data is presented. Always make sure you custom sizing the columns so they display the data appropriately.

Action: Adjust the column widths. Click on 'SAVE COLUMN WIDTHS'.

## Step 19.

**Filter number of results:**  
This table can include all the records retrieved, or records can be filtered.

Show all records  
 Show only the top 10  records  
 Show only the top 10  % of records

**Time-based settings:**  
Do you only want to see data in the table above from a specific time period?  No  

**Sort results by:**

**Group results by:**



Prior to submitting and building your report, SolarWinds provides the option to show various amounts of records. For our lab here today, we will not be modifying any of these numbers.

Action: Click 'SUBMIT'.

## Step 20.

### Add Report

The screenshot shows the SolarWinds Layout Builder interface. At the top, there's a navigation bar with tabs: LAYOUT BUILDER (highlighted in blue), PREVIEW, PROPERTIES, SCHEDULE REPORT, and SUMMARY. Below the navigation is a 'Report width' input field set to 960 px, with a 'Fit to window width' button. A 'Header' section contains the title '502d - Cisco Nodes' and a subtitle input field. To the right of the title is a 'Logo' section with a checked checkbox, a 'BROWSE FOR LOGO' button, and the SolarWinds logo. A 'Content' section below has a 'Layout columns' input set to 1, a '100%' width input, and a table component. The table has a header row with '502d - Cisco Nodes' and 'EDIT TABLE' buttons. It also includes a dropdown for 'For' and an 'Edit' button. At the bottom of the content area is a dashed box labeled 'Add Content'. On the right side of the content area, there are 'Page Layout' settings with a dropdown menu.

Now the basis of our report is built.

Action: Click 'NEXT' at the bottom right of the page (not shown here).

Note: The 'NEXT' button is buried in the lower right-hand corner and not shown above.

## Step 21.

Steps Recorder - Recording Now

4 products in evaluation.

REPORTS SETTINGS ADMIN (LOGOUT) HELP

What's New

Add Report

LAYOUT BUILDER > PREVIEW > PROPERTIES > SCHEDULE REPORT > SUMMARY >

## 502d - Cisco Nodes

Summary of Orion Objects: Cisco\_Nodes

CAPTION	IP ADDRESS	MACHINE TYPE	POLLING METHOD	SNMP VERSION	STATUS	CHASSIS SERIAL NUMBER
Nisgaa-02-sw	192.168.1.110	Cisco Catalyst 3560-8PC	SNMP	2	● Down	FOC1521V0EQ
Nisgaa-01-sw	192.168.0.110	Cisco Catalyst 3560-8PC	SNMP	3	● Down	

Created on 2/14/2020. 502d Network Operations Group - Nisgaa Data Systems for additional support.

BACK NEXT CANCEL

solarwinds

Orion Platform HF2, NCM HF1, NPM, NTA, UDT: 2019.4 © 1999-2020 SolarWinds Worldwide, LLC. All Rights Reserved.

Type here to search

5:27 PM 2/14/2020

This is a preview of our report.

Action: Click 'NEXT'.

## Step 22.

### Add Report

The screenshot shows the 'Add Report' interface with the 'PROPERTIES' tab selected. At the top, there are tabs for LAYOUT BUILDER, PREVIEW, PROPERTIES (which is highlighted in blue), SCHEDULE REPORT, and SUMMARY. Below the tabs, there is a section titled 'My Favorite Reports' with a checkbox labeled 'My Favorite Reports'. A red circle highlights this checkbox. A tooltip below it states: 'Reports marked as favorite are made easily available for frequent access.' Further down, there is a 'Report description:' field containing the text 'for all of our cisco nodes'. Under 'Report category:', there is a dropdown menu set to 'Custom'. At the bottom left, there is a section titled 'Report Limitation' with a note: 'User accounts that are assigned a specific report limitation category may only view reports in the specified report limitation category.'

If you create a report, always mark it as a favorite. This will help you find your report faster instead of hunting through the list to locate it.

Also, do not forget to provide a description. Provide some useful text so others will understand the reports purpose and scope.

Action: Click 'My Favorite Reports' and provide a description. Click 'NEXT'.

Note: The 'NEXT' button is buried in the lower right-hand corner and not shown above.

## Step 23.

### Add Report

The screenshot shows a navigation bar with tabs: LAYOUT BUILDER, PREVIEW, PROPERTIES, SCHEDULE REPORT, and SUMMARY. The SCHEDULE REPORT tab is highlighted in dark blue. Below the tabs, the title "Schedule Report" is displayed, followed by the sub-instruction: "Report can be created regularly and be emailed to particular recipient, saved to disk or printed out." Two radio buttons are present: one labeled "No schedule needed" (which is checked) and another labeled "Schedule this report to run regularly". A red circle highlights the "No schedule needed" radio button.

Many reports will not have a schedule. If a schedule report is required, it will usually involve an email delivery to be configured.

Action: Click 'NEXT'.

Note: The 'NEXT' button is buried in the lower right-hand corner and not shown above.

## Step 24.

### Add Report

LAYOUT BUILDER > PREVIEW > PROPERTIES > SCHEDULE REPORT > **SUMMARY**

#### Summary of report configuration

Please review the report configuration before saving...

#### ★ 502d - Cisco Nodes

**Description:**

for all of our cisco nodes

**Report Category:**

Custom

**Custom properties assigned:**

**Report Limitation applied:**

Default

---

**Summary of Orion Objects used:**

Cisco\_Nodes

**Summary of Time Periods used:**

**Resources used:**

502d - Cisco Nodes

---

**Report Schedule assigned:**

**Orion account to be used to generate scheduled report:**

admin

[PREVIEW REPORT](#)

Show created report after saving

---

Summary of our report and options selected.

Action: Click 'NEXT'.

Note: The 'NEXT' button is buried in the lower right-hand corner and not shown above.

## Step 25.

< BACK TO MANAGE REPORTS

Edit Report Export to Excel Print

# 502d - Cisco Nodes

Summary of Orion Objects: [Cisco\\_Nodes](#)

**502d - Cisco Nodes for Cisco\_Nodes**

CAPTION	IP ADDRESS	MACHINE TYPE	POLLING METHOD	SNMP VERSION	STATUS	CHASSIS SERIAL NUMBER
Nisgaa-02-sw	192.168.1.110	Cisco Catalyst 3560-8PC	SNMP	2	<span style="color:red;">●</span> Down	FOC1521V0EQ
Nisgaa-01-sw	192.168.0.110	Cisco Catalyst 3560-8PC	SNMP	3	<span style="color:red;">●</span> Down	

Created on 2/14/2020, 502d Network Operations Group - Nisgaa Data Systems for additional support



Here is an example of our Report. You may not have any data displayed in your report because all your nodes should currently be in the up status.

This concludes the lab exercise.

# Lab 11 – Script Management

This lab will show the student how to develop scripts which can be used to upload configuration and manage your networking devices.

## Step 1.

The screenshot shows the Orion NPM dashboard. At the top, there are four navigation tabs: MY DASHBOARDS, ALERTS & ACTIVITY, REPORTS, and SETTINGS. Below these are four main category sections: HOME, NETWORK, NETWORK CONFIGURATION, and NETFLOW. The HOME section contains links like Summary, Groups, Quality of Experience, Orion Maps, Environment, Performance Analysis, Top 10, thwack Community, Custom Summary, Training, and Virtualization. The NETWORK section contains links like NPM Summary, Network Top 10, Wireless, NetPath Services, VSANs, Load Balancing, Overview, and CFP Dashboard. The NETWORK CONFIGURATION section, which is expanded, contains links for Configuration Management, Config Summary, Config Change Templates, Compliance, Jobs, End of Support, Firmware Upgrades, CFP Dashboard, ToS, BGP, Flow Sources, and CBQoS Polling. The NETFLOW section contains links for NTA Summary, Apps, Conversations, Countries, Endpoints, Receivers, Transmitters, IP Groups, Protocols, ToS, BGP, Flow Sources, and CBQoS Polling. A red box highlights the 'Configuration Management' link under the NETWORK CONFIGURATION section, and a mouse cursor is positioned over it.

Action: Select from MY DASHBOARDS > NETWORK CONFIGURATION > Configuration Management.

## Step 2.

### Configuration Management

The screenshot shows the Configuration Management Dashboard with the 'SCRIPT MANAGEMENT' tab highlighted by a red box. The dashboard includes tabs for CONFIG MANAGEMENT, TRANSFER STATUS, INVENTORY STATUS, SCRIPT MANAGEMENT (highlighted), and BASELINE MANAGEMENT. A toolbar at the top provides options like DOWNLOAD, COMPILE NODE(S) CONFIGS, UPLOAD, EXECUTE SCRIPT, EDIT PROPERTIES, and UPDATE INVENTORY. On the left, a sidebar allows grouping by Vendor (Cisco 4, Unknown 1, Windows 1). The main area displays a table of nodes with columns for Name, IP Address, Baselines, and Last. There are four nodes listed: ipv4s2.nmsnll.local (IP 10.50.2.61), ipv4s3.nmsnll.local (IP 10.50.2.62), ipv6s2.nmsnll.local (IP 10.50.2.63), and ipv6s3.nmsnll.local (IP 10.50.2.64). All nodes have 'No baseline set'.

Name	IP Address	Baselines	Last
ipv4s2.nmsnll.local	10.50.2.61	No baseline set	
ipv4s3.nmsnll.local	10.50.2.62	No baseline set	
ipv6s2.nmsnll.local	10.50.2.63	No baseline set	
ipv6s3.nmsnll.local	10.50.2.64	No baseline set	

On the Configuration Management Dashboard, navigate to the Script Management tab

Action: Click 'SCRIPT MANAGEMENT' tab on the tool bar.

### Step 3.

#### Script Management

The screenshot shows the 'SCRIPT MANAGEMENT' tab selected in a navigation bar. Below it, a message states: '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 or a group, or in editing an existing config file.' A tooltip says: 'Arrange your scripts by Name, Creation Time, or Modified Time (when script was last changed.)'. At the bottom, there are buttons for 'ADD NEW SCRIPT' (highlighted with a red box and a cursor), 'EDIT SCRIPT', and 'DELETE'. There is also a search bar labeled 'Script name' and columns for 'Creation Time', 'Modified Time', and 'Comments'.

We are going to add a new script.

Action: Click 'ADD NEW SCRIPT'.

## Step 4.

ADD NEW SCRIPT

Script Name:  Banner

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19

Comments:

SAVE CANCEL

We are going to use this lab to develop a script for configuring the banner on a Cisco Router. This page is basically a notepad interface for use to type freely without formatting issues.

Action: Name the script “Banner”.

## Step 5.

ADD NEW SCRIPT

Script Name: Banner

```
17 Counterintelligence (CI) Investigations.  
18 -At any time, the USG may inspect and seize data stored on this IS.  
19 -Communications using, or data stored on, this IS are not private, are subject to  
20 routine monitoring, interception, and search, and may be disclosed or used for any  
21 USG-authorized purpose.  
22 -This IS includes security measures (e.g., authentication and access controls) to  
23 protect USG interests--not for your personal benefit or privacy.  
24 -Notwithstanding the above, using this IS does not constitute consent to PM, LE  
25 or CI investigative searching or monitoring of the content of privileged  
26 communications, or work product, related to personal representation or services  
27 by attorneys, psychotherapists, or clergy, and their assistants. Such  
28 communications and work product are private and confidential. See User Agreement  
29 for details.  
30  
31 !!!!  
32 !!!!  
33 !!!! Banner Version 2020-0130  
34 !!!!  
35 ^  
36
```

Comments:

**SAVE** **CANCEL**

Next, we need to supply the script with Cisco CLI commands.

Action: Copy the Cisco CLI text below and paste into the Script Text box as shown above.

Action: Click ‘SAVE’ when complete.

## **Cisco CLI Command**

```
config t  
no banner motd  
no banner exec  
banner login ^
```

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

```
!!  
!!  
!!..Banner Version 2020-1030  
!!  
!!
```

## Step 6.

### Script Management

The screenshot shows the 'SCRIPT MANAGEMENT' tab selected in a navigation bar. A tooltip message says: '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 or a group, or in editing an existing config file.' Below this, a note says: 'Arrange your scripts by Name, Creation Time, or Modified Time (when script was last changed.).' There are buttons for 'ADD NEW SCRIPT', 'EDIT SCRIPT', and 'DELETE'. A table lists one script entry:

Script name	Creation Time	Modified Time	Comments
502nd - Banner	10/14/2020 06:07 pm	10/14/2020 06:07 pm	

As we see our configuration listed above, we want to return to Config Management  
Action: Click 'CONFIG MANAGEMENT'.

## Step 7.

### Configuration Management

The screenshot shows the Configuration Management interface with the 'CONFIG MANAGEMENT' tab selected. The left sidebar allows grouping by Vendor (Cisco, Unknown, Windows) or No grouping. The main pane lists 4 selected nodes, each with a checked checkbox (circled in red), IP Address, Baselines (No baseline set), and Last. The toolbar at the top includes options for DOWNLOAD, COMPARISON, UPLOAD, EXECUTE SCRIPT, EDIT PROPERTIES, and UPDATE INVENTORY.

	Name	IP Address	Baselines	Last
<input checked="" type="checkbox"/>	ipv4s2.nmsnil.local	10.50.2.61	No baseline set	
<input checked="" type="checkbox"/>	ipv4s3.nmsnil.local	10.50.2.62	No baseline set	
<input checked="" type="checkbox"/>	ipv6s2.nmsnil.local	10.50.2.63	No baseline set	
<input checked="" type="checkbox"/>	ipv6s3.nmsnil.local	10.50.2.64	No baseline set	

Now we need to select a device to apply the script.

Action: Locate your Cisco device from the list in the NCM Device Window located to the left of the screen. And click the box to the left of your device.

Action: Click on 'EXECUTE SCRIPT' on the tool bar.

## Step 8.

### Execute Script

Wednesday, October 14, 2020 6:09:40 PM

▶ Applies to 4 node(s)

Select Script

VIEW BY NAME:

[502nd - Banner](#)

```
!#####
!##### Banner #####
!#####
config t
no banner motd
no banner exec
banner login ^

You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you
consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for
purposes including, but not limited to, penetration testing, COMSEC
monitoring, network operations and defense, personnel misconduct (PM),
law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are
subject to routine monitoring, interception, and search, and may be
disclosed or used for any USG-authorized purpose.
```

Save script

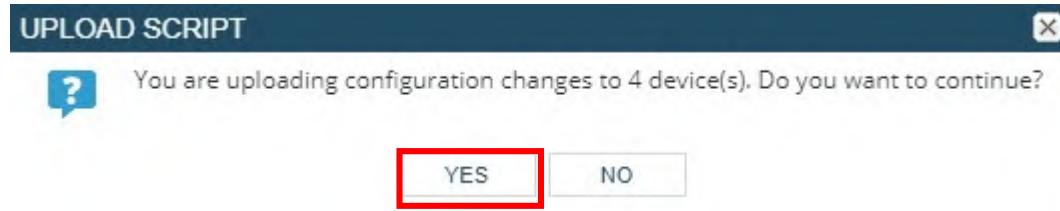
Execute Script in Config Mode » Help me understand what config mode means

Reboot Device

Here we are going to select the script on the left, which will display the parameters on the right.

Action: Navigate to the bottom of the page and check the box “Execute Script in Config Mode” then click ‘EXECUTE’.

## Step 9.



This is a confirmation screen to make sure you want to perform this action.

Action: Click 'YES'.

## Step 10.

### Transfer Status

CONFIG MANAGEMENT	TRANSFER STATUS	INVENTORY STATUS	SCRIPT MANAGEMENT	BASELINE MANAGEMENT
<a href="#">CANCEL ALL</a>   <a href="#">CLEAR ALL</a>   <a href="#">CLEAR COMPLETE</a>   <a href="#">CLEAR FAILED</a>   <a href="#">RE-EXECUTE</a>   <a href="#">SHOW SCRIPT RESULTS</a>				
	Date Time	Action	Node Name	IP Address
	10/14/2020 06:11 pm	Upload	ipv4s3.nmsnll.local	10.50.2.62
	10/14/2020 06:11 pm	Upload	ipv6s3.nmsnll.local	10.50.2.64
	10/14/2020 06:11 pm	Upload	ipv4s2.nmsnll.local	10.50.2.61
	10/14/2020 06:11 pm	Upload	ipv6s2.nmsnll.local	10.50.2.63

Once you confirm the execution of the script, SolarWinds will bring you out to the Configuration Management Page. We can watch the status of our script execution under the 'Status/Details' column. If the script is running successfully, a date will be displayed. If there was a problem, an error would be displayed.

To continue with this lab, create a Script for each of the following by using your Cisco Configuration file in your Class Documents folder:

1. Services
2. NTP
3. Logging
4. SNMP

This concludes the lab exercise.

# Lab 12 – NCM Settings

This lab will assist in learning about some of the settings NCM has to offer.

## Step 1.



### PRODUCT SPECIFIC SETTINGS

Global and product specific settings such as session timeout, page refresh, site logo, chart settings etc.

- |  |  |                                 |
|--|--|---------------------------------|
| » Web Console Settings                     | » SRM Settings                         | » WPM Settings                  |
| » NCM Settings                             | » QoE Settings                         | » Database Performance Analyzer |
| » Cloud Infrastructure Monitoring Settings | » SAM Settings                         | » Virtualization Settings       |
| » Orion Service Manager                    | » NTA Settings                         | » Agent Settings                |
| » Proxy Settings                           | » High Availability Deployment Summary | » High Availability Settings    |
| » Application Connection Settings          | » APM Deployment Summary               | » CLI Settings                  |

Starting from the SETTINGS > All Settings page we will want scrolled slightly to the PRODUCT SPECIFIC SETTINGS section.

Action: Click “NCM Settings”.

## Step 2.

### NCM Settings

**NCM NODE MANAGEMENT**  
Add and remove NCM nodes. Select node details to be added to the database. Review licensing details.

» Add or Manage Nodes      » Node Licensing      » Node Inventory

---

**CONFIG SETTINGS**  
Adjust config types, config transfer, comparisons and manage archive settings.

» Config Settings      » Comparison Criteria

» Config Archive Folder Locations      » Config Types      » Binary Config Storage Settings

The NCM Settings page is full of options to customize your NCM product. We are only going to view a couple of these setting in the exercise. To review all settings here will take another full week of class time. Let's review some of the more important ones.

Action: Click on 'Config Types' in the CONFIG SETTINGS section.

### Step 3.

#### Config Types

Admin ▶ NCM Settings ▶ Config Types

Some configs are monitored by default and they cannot be removed. Add new custom config types to track.

##### Config Types

Running	 EDIT
Startup	 EDIT
Device State	 EDIT
NTP	 EDIT  REMOVE
SNMP User	 EDIT  REMOVE
Interface Brief	 EDIT  REMOVE
<input type="text"/>	
 ADD NEW	

The Config Types section will allow us to configure different types of configurations from our devices. These configurations are pulled from the device template assigned to your devices in the Edit Properties section of Manage Nodes.

Action: Type 'NTP' in the box then click the 'ADD NEW' button to the right.

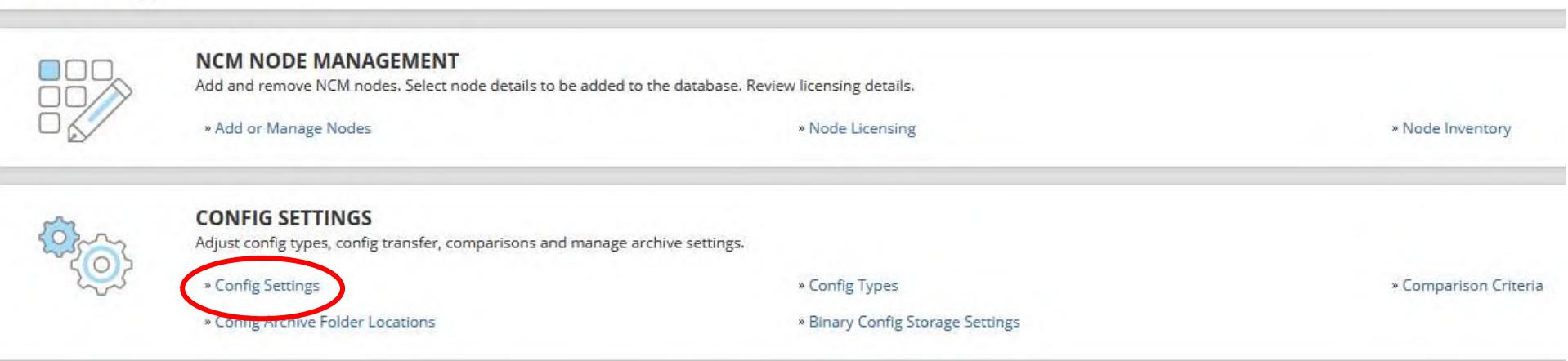
Action: Type SNMP User in the box then click the 'ADD NEW' button to the right.

Action: Type Interface Brief in the box then click the 'ADD NEW' button to the right.

Action: Click on 'NCM Settings' in the upper left-hand corner as seen in the picture above.

## Step 4.

### NCM Settings



**NCM NODE MANAGEMENT**  
Add and remove NCM nodes. Select node details to be added to the database. Review licensing details.

» Add or Manage Nodes      » Node Licensing      » Node Inventory

---

**CONFIG SETTINGS**  
Adjust config types, config transfer, comparisons and manage archive settings.

» Config Settings (circled in red)      » Config Types      » Comparison Criteria  
» Config Archive Folder Locations      » Binary Config Storage Settings

Next let's look at Config Settings.

Action: Click on 'Config Settings'.

## Step 5.

### Config Settings

#### Config Transfer

Simultaneous Downloads/Uploads	<input type="text" value="25"/>	25 sessions	Default: 25 sessions
SNMP Config Transfer Timeout	<input type="text" value="4"/>	4 minutes	Default: 4 minutes
Config Min Length	<input type="text" value="1"/>	1 lines	Default: 11 lines

#### Config Comparisons

These settings affect how the Compare Configs page displays.

Comparison Output Width	<input type="text" value="250"/>
<input type="radio"/> Display the full side-by-side comparison	<input checked="" type="radio"/> Display the number of lines

#### Config Archive

Save a copy of each config into the archive directory, as it is downloaded

When configs are edited, only retain the last version

Enter a path for the archive directory on this main or additional polling engine NCM server:

E:\ProgramData\SolarWinds\NCM\Config-Archive



Specify a template that should be used for naming config files:

Here we see various options for our configuration actions.

1. Simultaneous Downloads/Uploads – Default is 25. Do not change, you may go fewer if you like but do not increase. You may bog down the system and cause other errors.
2. SNMP Config Transfer Timeout – If you are using SNMP for transfer protocol you may need to increase on those higher latency links.
3. Config Min Length – Default says 11 lines, but we are going to move it down to 1 line. Some of our Config Types may only have one line to download.
4. Enter a path for the archive directory on this main or additional polling engine NCM server: We will set this to the E:\ProgramData\SolarWinds\NCM\Config-Archive path in order to reduce further burden on the C:\. Use the ‘VALIDATE’ button to ensure such a path exists on your NCM Server.

Action: Configure ‘Config Min Length’ for 2 lines. Click on “NCM Settings” in upper left corner.

## Step 6.

---



### COMPLIANCE POLICY REPORT MANAGEMENT

Manage compliance policy reports (HIPAA, SOX, CISP and Cisco Security Audit), rules, and policies. » Learn more

» Manage Policy Reports

» Manage Policies

» Manage Rules

» Manage Violation Levels



Action: Click on 'Manage Violation Levels' in the COMPLIANCE POLICY REPORT MANAGEMENT section.

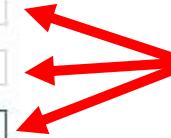
Step 7.

## Manage Violation Levels

**Customize Policy Rule Violation Levels**

<span style="color: blue;">i</span> Violation Level 1:	CAT III
<span style="color: yellow;">!</span> Violation Level 2:	CAT II
<span style="color: red;">!</span> Violation Level 3:	CAT I

**SUBMIT**   **CANCEL**



The default settings are Informational for Level 1, Warning for Level 2, and Critical for Level 3. We are going to change them for DoD purposes.

Action: Change Level 1 to CAT III, Level 2 to CAT II, and Level 3 to CAT I.

Action: Click 'SUBMIT' when complete.

## Step 8.



### GLOBAL DEVICE DEFAULTS

Review and edit default settings for device logins, communication transfer protocol and transfer ports.

» Global Device Defaults

» Connection Profiles

Action: Click on ‘Connection Profiles’ in the GLOBAL DEVICE DEFAULTS section.

## Step 9.

### Manage Connection Profiles

The screenshot shows a user interface for managing connection profiles. At the top, there are four buttons: 'CREATE NEW' (highlighted with a red box), 'EDIT', 'DELETE', and 'ASSIGN TO NODES'. Below these buttons are two input fields: 'Profile Name' (with a dropdown arrow) and 'Use for auto-detect' (with a checkbox). The background is light gray, and the overall layout is clean and organized.

Connection Profiles are profiles you provide to SolarWinds to allow for device configuration backup, upload, and administrative actions. This should be a service account within your network management group.

Action: Click ‘CREATE NEW’.

## Step 10.

Profile Name  
Admin Cisco

CLI Login/User Name  
Admin

CLI Password:  
\*\*\*\*\*

Enable Level: ?  
<No Enable Login>

Enable Password

Execute Commands and Scripts  
SSH2

Config Request  
SSH2

Transfer Configs  
SSH2

Telnet Port  
23

SSH Port  
22

Automatically test this profile against monitored nodes that allowed it. ?

**SUBMIT** **CANCEL**

Here we have our connection profile.

Action:

Profile Name: **Admin Cisco** – Give it a readable name:

CLI Login/Username: **Admin** – The username needs for the device to recognize as an actual account:

CLI Password: **P@ssw0rd!1** - Password for access

Enable: Cisco devices will need to be enabled. Other vendors may as well but consult vendor documentation. We will not be using this feature here.

Enable Password: not needed in this example.

Execute Commands and Scripts: SSH2, no Telnet allowed

Config Request: SSH2, no Telnet allowed

Click ‘SUBMIT’ when complete.

## Step 11.

### Manage Connection Profiles

<input type="button"/> CREATE NEW	<input type="button"/> EDIT	<input type="button"/> DELETE
<input type="button"/> ASSIGN TO NODES		
<input type="checkbox"/>	Profile Name	Use for auto-detect
<input type="checkbox"/>	Admin Cisco	No
<input type="checkbox"/>	Fortinet	No
<input type="checkbox"/>	Nisgaa	No
<input type="checkbox"/>	Palo Alto - Admin	No
<input type="checkbox"/>	Palo Alto - Solarwinds	Yes

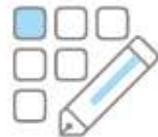
Here we have configured our new connection profile. The other connection profiles located here provide further examples of various profiles your organization may require.

This concludes the lab exercise.

# Lab 13 - Device Templates

In this lab we will work on Device Templates. Device Templates are used to communicate with a networking device on which commands to issue to return the correct action. These commands are often used to download/upload configuration files and software upgrades.

## Step 1.



### NODE & GROUP MANAGEMENT

Manage and delete nodes, dependencies and groups. Edit node properties.

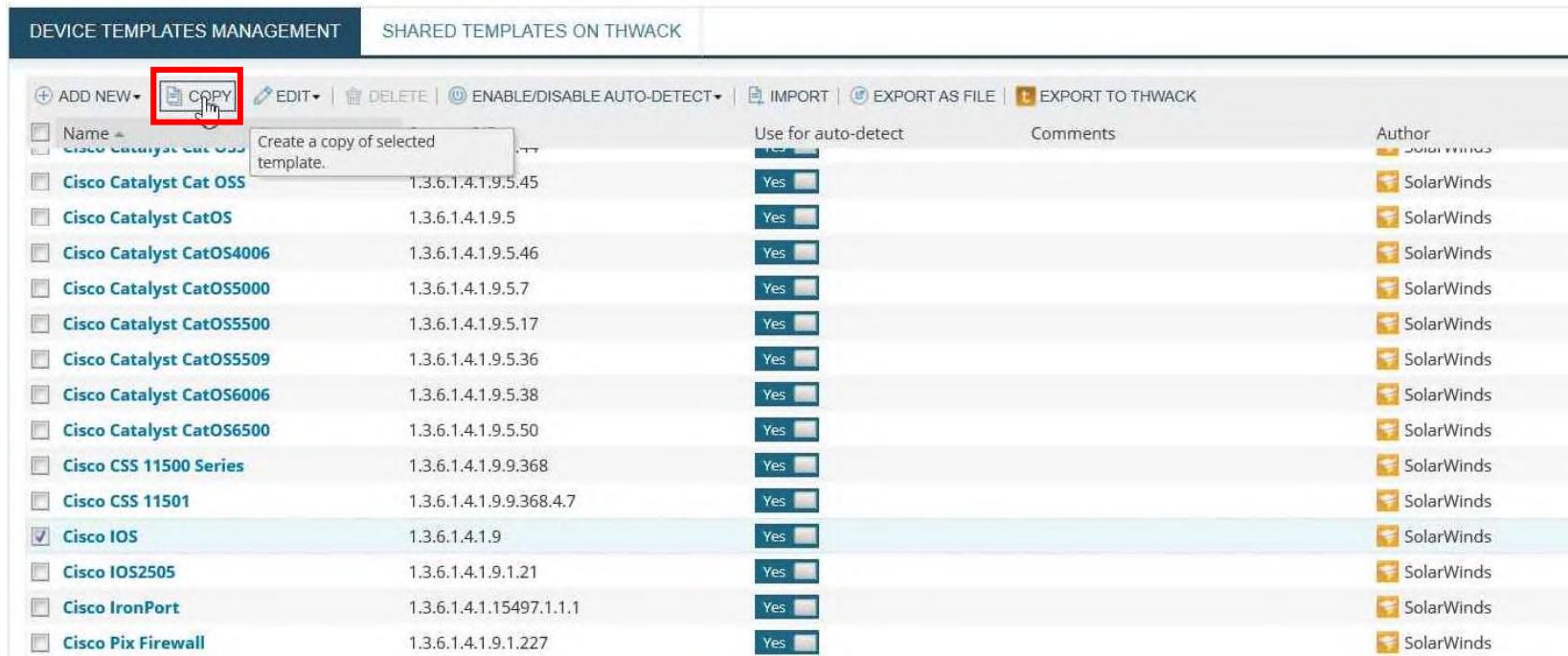
- » [Manage Nodes](#)
- » [Manage Groups](#)
- » [Add Discovered Scopes](#)
- » [Manage DHCP Servers](#)
- » [Manage Pollers](#)
- » [Manage Hardware Sensors](#)
- » [Manage API Pollers](#)
- » [Manage Virtual Devices](#)
- » [Manage Agents](#)
- » [Manage Orphaned IPs](#)
- » [Manage Scopes](#)
- » [Manage World Map](#)
- » [Manage Orion Maps](#)
- » [Manage Dependencies](#)
- » [Manage Custom Properties](#)
- » [Manage Subnets & IPs](#)
- » [Manage Storage Objects](#)
- » [Manage Device Templates](#)
- » [Manage Container Services](#)

Starting from the Setting page we will go to the Device Templates section.

Action: Click on ‘Manage Device Templates’ in the NODE & GROUP MANAGEMENT section.

## Step 2.

### Device Templates Management



The screenshot shows a list of device templates. A red box highlights the 'COPY' button in the top navigation bar. A tooltip 'Create a copy of selected template.' is visible over the 'COPY' button. The table lists various Cisco device templates with their names, version numbers, auto-detect settings, comments, and authors.

Name	Version	Use for auto-detect	Comments	Author
Cisco Catalyst Cat OSS	1.3.6.1.4.1.9.5.45	Yes		SolarWinds
Cisco Catalyst CatOS	1.3.6.1.4.1.9.5	Yes		SolarWinds
Cisco Catalyst CatOS4006	1.3.6.1.4.1.9.5.46	Yes		SolarWinds
Cisco Catalyst CatOS5000	1.3.6.1.4.1.9.5.7	Yes		SolarWinds
Cisco Catalyst CatOS5500	1.3.6.1.4.1.9.5.17	Yes		SolarWinds
Cisco Catalyst CatOS5509	1.3.6.1.4.1.9.5.36	Yes		SolarWinds
Cisco Catalyst CatOS6006	1.3.6.1.4.1.9.5.38	Yes		SolarWinds
Cisco Catalyst CatOS6500	1.3.6.1.4.1.9.5.50	Yes		SolarWinds
Cisco CSS 11500 Series	1.3.6.1.4.1.9.9.368	Yes		SolarWinds
Cisco CSS 11501	1.3.6.1.4.1.9.9.368.4.7	Yes		SolarWinds
<input checked="" type="checkbox"/> Cisco IOS	1.3.6.1.4.1.9	Yes		SolarWinds
Cisco IOS2505	1.3.6.1.4.1.9.1.21	Yes		SolarWinds
Cisco IronPort	1.3.6.1.4.1.15497.1.1.1	Yes		SolarWinds
Cisco Pix Firewall	1.3.6.1.4.1.9.1.227	Yes		SolarWinds

We are going to edit a Cisco IOS device template to include commands for NTP configuration save.

Action: Select 'Cisco IOS' from the list by checking the box to the left of the name. Then select 'COPY'. Again, we do not want to modify the master file.

Action: Select 'EDIT' and on the drop-down menu, select 'XML Editor'.

### Step 3.

COPY DEVICE TEMPLATE

Template Name:	502d - Cisco IOS
System OID:	1.3.6.1.4.1.9
System Description Pattern:	Type System Description Pattern
Use for auto-detect:	Yes <input checked="" type="radio"/> <input type="radio"/> Match by System Description
Comments:	   

Template XML:

```
<!-- edited with XML Spy v4.4 U (http://www.xmlspy.com) by () -->
<!--SolarWinds Network Management Tools-->
<!--Copyright 2005 SolarWinds.Net All rights reserved-->
<Configuration-Management Device="Cisco Devices" SystemOID="1.3.6.1.4.1.9">
    <Commands>
        <Command Name="RESET" Value="terminal width 0${CRLF}terminal length 0"/>
        <Command Name="Reboot" Value="reload${CRLF}y${CRLF}y"/>
        <Command Name="EnterConfigMode" Value="config terminal"/>
        <Command Name="ExitConfigMode" Value="end"/>
        <Command Name="Startup" Value="startup"/>
        <Command Name="Running" Value="running"/>
        <Command Name="DownloadConfig" Value="Show ${ConfigType}"/>
        <Command Name="UploadConfig" Value="${EnterConfigMode}${CRLF}${ConfigText}${CRLF}${ExitConfigMode}"/>
        <Command Name="DownloadConfigIndirect" Value="copy ${ConfigType}
${TransferProtocol}://${StorageAddress}/${StorageFilename}${CRLF}${CRLF}"/>
        <Command Name="UploadConfigIndirect" Value="copy ${TransferProtocol}://${StorageAddress}/${StorageFilename}"/>
```

**COPY DEVICE TEMPLATE**

Template Name:	502d Cisco IOS
System OID:	1.3.6.1.4.1.9
System Description Pattern:	Type System Description Pattern
Use for auto-detect:	Yes <input type="button" value="▼"/>
<input checked="" type="radio"/> Match by System OID <input type="radio"/> Match by System Description	
Comments:	
<b>Template XML:</b> <pre>&lt;!-- edited with XML Spy v4.4 U (http://www.xmlspy.com) by () --&gt; &lt;!--SolarWinds Network Management Tools--&gt; &lt;!--Copyright 2005 SolarWinds.Net All rights reserved--&gt; &lt;Configuration-Management Device="Cisco Devices" SystemOID=" 1.3.6.1.4.1.9"&gt;   &lt;Commands&gt;     &lt;Command Name="RESET" Value="terminal width 0\${CRLF}terminal length 0"/&gt;     &lt;Command Name="Reboot" Value="reload\${CRLF}y\${CRLF}y"/&gt;     &lt;Command Name="EnterConfigMode" Value="config terminal"/&gt;     &lt;Command Name="ExitConfigMode" Value="end"/&gt;     &lt;Command Name="Startup" Value="startup"/&gt;     &lt;Command Name="Running" Value="running"/&gt;     &lt;Command Name="DownloadConfig" Value="Show \${ConfigType}"/&gt;     &lt;Command Name="UploadConfig" Value="\${EnterConfigMode}\${CRLF}\${ConfigText}\${CRLF}\${ExitConfigMode}"/&gt;     &lt;Command Name="DownloadConfigIndirect" Value="copy \${ConfigType} \${TransferProtocol}://\${StorageAddress} /\${StorageFilename}\${CRLF}\${CRLF}\${CRLF}"/&gt;     &lt;Command Name="UploadConfigIndirect" Value="copy \${TransferProtocol}://\${StorageAddress}/\${StorageFilename} \${ConfigType}\${CRLF}\${CRLF}"/&gt;     &lt;Command Name="DownloadConfigIndirectSCP" Value="copy \${ConfigType} \${TransferProtocol}://\${SCPServerUserName}@\${SCPStorageAddress} /\${StorageFilename}\${CRLF}\${CRLF}\${CRLF} \${SCPServerPassword}"/&gt;     &lt;Command Name="UploadConfigIndirectSCP" Value="copy \${TransferProtocol}://\${SCPServerUserName}@\${SCPStorageAddress}/\${StorageFilename} \${ConfigType}\${CRLF}\${CRLF} \${SCPServerPassword}"/&gt;     &lt;Command Name="EraseConfig" Value="write erase\${CRLF}Y"/&gt;     &lt;Command Name="SaveConfig" Value="write memory"/&gt;     &lt;Command Name="Version" Value="show version"/&gt;</pre>	
<input style="border: 2px solid red; border-radius: 50%; padding: 5px; margin-right: 10px;" type="button" value="SAVE"/> <input type="button" value="CANCEL"/>	

This is a device template. As you can see it uses command line interface wording to gather the requested documents.

Action: Click 'SAVE'.

#### Step 4.

## Device Templates Management

DEVICE TEMPLATES MANAGEMENT		SHARED TEMPLATES ON THWACK		
<a href="#">+ ADD NEW</a>   <a href="#">COPY</a>   <a href="#">EDIT</a>   <a href="#">DELETE</a>   <a href="#">ENABLE/DISABLE AUTO-DETECT</a>   <a href="#">IMPORT</a>   <a href="#">EXPORT AS FILE</a>   <a href="#">EXPORT TO THWACK</a>				
Name	OID	Use for auto-detect	Comments	Author
<input type="checkbox"/> 3Com	Using Interactive Wizard	<input checked="" type="checkbox"/>		SolarWinds
<input checked="" type="checkbox"/> 502d Cisco IOS	Using Xml Editor	<input checked="" type="checkbox"/>		admin
<input type="checkbox"/> Adtran	1.3.6.1.4.1.9	<input checked="" type="checkbox"/>		SolarWinds
<input type="checkbox"/> Alaxala AX3630S and AX2530	1.3.6.1.4.1.664	<input checked="" type="checkbox"/>		SolarWinds
<input type="checkbox"/> Allied-Telesis	1.3.6.1.4.1.207.1.14.109	<input checked="" type="checkbox"/>		SolarWinds
<input type="checkbox"/> Apresia 3424GT and 13200	1.3.6.1.4.1.278.1.27	<input checked="" type="checkbox"/>		SolarWinds
<input type="checkbox"/> Arris	1.3.6.1.4.1.4998	<input checked="" type="checkbox"/>		SolarWinds
<input type="checkbox"/> Aruba	1.3.6.1.4.1.14823	<input checked="" type="checkbox"/>		SolarWinds
<input type="checkbox"/> Business Policy Switch 2000	1.3.6.1.4.1.45.3.40	<input checked="" type="checkbox"/>		SolarWinds
<input type="checkbox"/> Cisco Adaptive Security Appliance	1.3.6.1.4.1.9.1.669	<input checked="" type="checkbox"/>		SolarWinds
<input type="checkbox"/> Cisco Catalyst 1900	1.3.6.1.4.1.9.5.175	<input checked="" type="checkbox"/>		SolarWinds
<input type="checkbox"/> Cisco Catalyst Cat OSS	1.3.6.1.4.1.9.5.44	<input checked="" type="checkbox"/>		SolarWinds
<input type="checkbox"/> Cisco Catalyst Cat OSS	1.3.6.1.4.1.9.5.45	<input checked="" type="checkbox"/>		SolarWinds
<input type="checkbox"/> Cisco Catalyst CatOS	1.3.6.1.4.1.9.5	<input checked="" type="checkbox"/>		SolarWinds
<input type="checkbox"/> Cisco Catalyst CatOS4006	1.3.6.1.4.1.9.5.46	<input checked="" type="checkbox"/>		SolarWinds
<input type="checkbox"/> Cisco Catalyst CatOS5000	1.3.6.1.4.1.9.5.7	<input checked="" type="checkbox"/>		SolarWinds
<input type="checkbox"/> Cisco Catalyst CatOS5500	1.3.6.1.4.1.9.5.17	<input checked="" type="checkbox"/>		SolarWinds

Now with our new Device Template, we can assign it to our Cisco devices for action.

Action: Drop the 'EDIT' button down and select 'Using Interactive Wizard'

## Step 5.

### Edit device template 502nd - Cisco IOS

The screenshot shows the 'Edit device template' interface with the title 'Edit device template 502nd - Cisco IOS'. The top navigation bar includes 'SELECT NODE', 'CHOOSE OPERATION', 'GENERAL DEVICE ACCESS', 'CONFIG DOWNLOAD', and 'SAVE DEVICE TEMPLATE'. The main section is titled 'Select Node' with the sub-instruction: 'NCM uses the selected node to test operations as you build the template. You can assign the finished device template to nodes as a final step in the process.' Below this, there is a search bar with 'Level: 1' and 'Group by: Vendor'. The node list is organized by vendor: Cisco, Unknown, and Windows. The Cisco section is expanded, showing four nodes: 'ipv4s2.nmsnil.local', 'ipv4s3.nmsnil.local', 'ipv6s2.nmsnil.local', and 'ipv6s3.nmsnil.local'. The Windows section shows one node: 'student01-VM'. The Windows section has an expand/collapse arrow. A red box highlights the Cisco vendor node, and a red arrow points to the 'NEXT' button at the bottom right.

Here we are going to select our node.

Action: Expand the Cisco Vendor Icon. Check the box for one of the nodes for now.

Action: Click 'NEXT'.

## Step 6.

Edit device template 502nd - Cisco IOS for ipv4s2.nmsnil.local

SELECT NODE > CHOOSE OPERATION > GENERAL DEVICE ACCESS > CONFIG DOWNLOAD > SAVE DEVICE TEMPLATE >

**Choose Operation**

I want to be able to:

Execute scripts only  
 Execute scripts and download config from the device  
 Execute scripts, download config from the device and upload config to the device  
[» Help me choose](#)

You will be able to test the operations in the next steps.  
Changes made in this wizard will be saved after you complete the last step.

BAC **NEXT** CANCEL

Choose how you want to use this Device Template. When in doubt go with default settings. This default is set to ‘Execute scripts and download config from the device’.

Action: Click ‘NEXT’.

## Step 7.

### General Device Access

#### Connection Profile

Global Connection Profile: Admin Cisco

Login Credentials: Device

Username: Admin

Password: \*\*\*\*\*

Enable Level: enable

Enable Password: \*\*\*\*\*

Execute Scripts Using: SSH2

Request Configs Using: SSH2

Transfer Configs Using: SSH2

Telnet Port: 23

SSH Port: 22

#### Device Template

Reset Terminal Size Command: terminal width 0\${CRLF}terminal length 0  
Enter command to turn off paging (more prompt) on device. Multiple commands can be separated by \${CRLF} macro

Show Version Command: show version  
Multiple commands can be separated by \${CRLF} macro  
▶ Show advanced options

Test Device Access:  » What does this test validate?

Here is where we will assign the Network Service account mentioned in earlier labs. This is a simple drop down and select.

Action: In the Global Connection Profile line use the drop-down menu to select our Admin Cisco account from the drop down to access our Cisco devices.

Action: Click 'NEXT' at the bottom right of the page.

## Step 8.

### Config Download

#### Download Command

Enter the command for downloading a config from this device.

Download Config Command: `Show ${ConfigType}`

[SHOW MACRO VALUES](#)

For example: `show ${ConfigType}`

Available Macros:  
\${ConfigType} - determine type of config to download

[Manage Config Types](#)

#### Config Types

Enter a name for each type of config file type than NCM should be able to download from this device.

Running Config File Name: `running`

Is binary config

Startup Config File Name: `startup`

Is binary config

NTP Config File Name: `ntp status`

Is binary config

SNMP User Config File Name: `snmp user`

Is binary config

Interface Brief Config File Name: `ip interface brief`

Is binary config

In the Config Types section on this page. If in the blank spaces with the proper Cisco Command. There is no need to put a show in front of our commands because the show is inherently provided by the Download Config Command seen above.

NTP Config File name: `ntp status`

SNMP User Config File Name: `snmp user`

Interface Brief Config File Name: `ip interface brief`

Action: Click 'NEXT' when complete.

## Step 9.

### Config Upload

#### Upload Options

Enter Config Mode Command: config terminal

Exit Config Mode Command: end

Write to NVRAM Command: write memory

Reboot Command: reload\${CRLF}y\${CRLF}y

#### Upload Command

Upload Config Command: \${EnterConfigMode}\${CRLF}\${ConfigText}\${CRLF}\${ExitConfigMode}

For example: \${EnterConfigMode}\${CRLF}\${ConfigText}\${CRLF}\${ExitConfigMode}

 **Available Macros:**

\${ConfigText} - text of config to upload

\${EnterConfigMode} - command to enter into config mode

\${ExitConfigMode} - command to exit from config mode

-\${CRLF} - use to separate multiple commands or simulate Enter key press

There is no action to be taken here. We are going to stay with the default settings.

Click the 'NEXT' button on the bottom right of the page.

## Step 10.

Save Device Template

Save Device Template: 502nd - Cisco IOS  
System OID: 1.3.6.1.4.1.9  
System Description Pattern:  
Use for auto-detect: Yes  
 Match by System OID  
 Match by System Description

Comments:

» Help me understand how device templates are assigned to nodes

Assign Device Template

This device template and connection profile will be assigned to the following node: [ipv4s2.nmsn1.local](#)

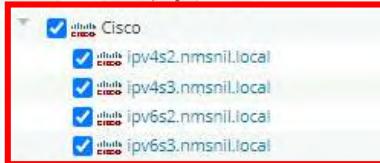
Select additional nodes to assign device template to:

Level: 1 Group by: Vendor   Select All

Cisco  
 ipv4s2.nmsn1.local  
 ipv4s3.nmsn1.local  
 ipv6s2.nmsn1.local  
 ipv6s3.nmsn1.local

Unknown  
 Windows

Assign the same connection profile to selected nodes



Here we can assign our new device template to our Cisco Devices.

Action: Select the 'FINISH' button at the bottom right of the page when complete.

## Step 11.

### Device Templates Management

DEVICE TEMPLATES MANAGEMENT					SHARED TEMPLATES ON THWACK
<a href="#">ADD NEW</a>   <a href="#">COPY</a>   <a href="#">EDIT</a>   <a href="#">DELETE</a>   <a href="#">ENABLE/DISABLE AUTO-DETECT</a>					<a href="#">IMPORT</a>   <a href="#">EXPORT AS FILE</a>   <a href="#">EXPORT TO THWACK</a>
Name	System OID	Use for auto-detect	Comments	Author	
3Com	1.3.6.1.4.1.43.1.16.4	<input checked="" type="checkbox"/>		SolarWinds	
502d - Cisco IOS	1.3.6.1.4.1.9	<input checked="" type="checkbox"/>		admin	
Adtran	1.3.6.1.4.1.664	<input checked="" type="checkbox"/>		SolarWinds	
Alaxala AX3630S and AX2530	1.3.6.1.4.1.21839.1.2	<input checked="" type="checkbox"/>		SolarWinds	
Allied-Telesis	1.3.6.1.4.1.207.1.14.109	<input checked="" type="checkbox"/>		SolarWinds	
Apresia 3424GT and 13200	1.3.6.1.4.1.278.1.27	<input checked="" type="checkbox"/>		SolarWinds	
Arris	1.3.6.1.4.1.4998	<input checked="" type="checkbox"/>		SolarWinds	
Aruba	1.3.6.1.4.1.14823	<input checked="" type="checkbox"/>		SolarWinds	
Business Policy Switch 2000	1.3.6.1.4.1.45.3.40	<input checked="" type="checkbox"/>		SolarWinds	
Cisco Adaptive Security Appliance	1.3.6.1.4.1.9.1.669	<input checked="" type="checkbox"/>		SolarWinds	
Cisco Catalyst 1900	1.3.6.1.4.1.9.5.175	<input checked="" type="checkbox"/>		SolarWinds	
Cisco Catalyst Cat OSS	1.3.6.1.4.1.9.5.44	<input checked="" type="checkbox"/>		SolarWinds	
Cisco Catalyst Cat OSS	1.3.6.1.4.1.9.5.45	<input checked="" type="checkbox"/>		SolarWinds	
Cisco Catalyst CatOS	1.3.6.1.4.1.9.5	<input checked="" type="checkbox"/>		SolarWinds	

There is our newly modified Device Template.

## Step 12.

A screenshot of the Cisco Network Configuration Management interface. At the top, there is a navigation bar with links: DOWNLOAD, COMPARISON, UPLOAD, EXECUTE SCRIPT, EDIT PROPERTIES, and UPDATE INVENTORY. A red arrow points to the DOWNLOAD link. Below the navigation bar is a sidebar with options: Download config (Running, Startup), Custom config types (NTP Status, SNMP User, Interface Brief), and a status indicator for ipv6s3.nmsnil.local. The main area is a table listing device configurations. The columns are: IP Address, Baselines, Last, Last action date, and Error details. The table contains four rows, each corresponding to a custom config type listed in the sidebar. The first three rows have a red border around them.

	IP Address	Baselines	Last	Last action date	Error details
NTP Status	snil.local	10.50.2.61	No baseline set		10/14/2020 06:11:17 pm
SNMP User	snil.local	10.50.2.62	No baseline set		10/14/2020 06:11:17 pm
Interface Brief	snil.local	10.50.2.63	No baseline set		10/14/2020 06:11:17 pm
ipv6s3.nmsnil.local	10.50.2.64	No baseline set		10/14/2020 06:11:17 pm	

Action:

- A. Navigate to My Dashboards > Network Configuration > Configuration Management.
- B. Select your Cisco Device.
- C. Navigate to the download menu item above.
- D. Download each of the Custom Config Types you have configured.

Did you get the expect results for each of the different configs?

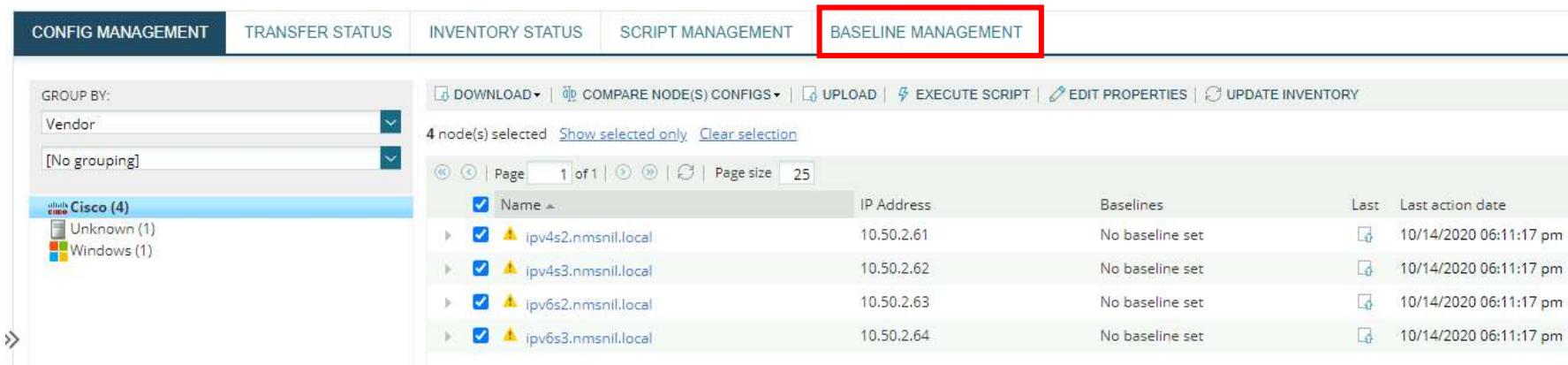
This concludes this lab exercise.

# Lab 14 – Baseline Management

This lab will provide the student the ability to set baseline configurations for their networking devices.

## Step 1.

### Configuration Management



The screenshot shows the Configuration Management interface. The top navigation bar has tabs: CONFIG MANAGEMENT, TRANSFER STATUS, INVENTORY STATUS, SCRIPT MANAGEMENT, and BASELINE MANAGEMENT. The BASELINE MANAGEMENT tab is highlighted with a red box. On the left, there's a sidebar for 'GROUP BY' with dropdowns for 'Vendor' (Cisco) and 'No grouping'. Below that is a tree view showing 'Cisco (4)', 'Unknown (1)', and 'Windows (1)'. The main area displays a table of nodes. The table columns are: Name, IP Address, Baselines, Last, and Last action date. There are four rows, each with a yellow warning icon and a checkmark in the first column. The rows are: 'ipv4s2.nmsnil.local' (IP 10.50.2.61), 'ipv4s3.nmsnil.local' (IP 10.50.2.62), 'ipv6s2.nmsnil.local' (IP 10.50.2.63), and 'ipv6s3.nmsnil.local' (IP 10.50.2.64). All rows show 'No baseline set' under 'Baselines' and '10/14/2020 06:11:17 pm' under 'Last action date'.

Name	IP Address	Baselines	Last	Last action date
ipv4s2.nmsnil.local	10.50.2.61	No baseline set		10/14/2020 06:11:17 pm
ipv4s3.nmsnil.local	10.50.2.62	No baseline set		10/14/2020 06:11:17 pm
ipv6s2.nmsnil.local	10.50.2.63	No baseline set		10/14/2020 06:11:17 pm
ipv6s3.nmsnil.local	10.50.2.64	No baseline set		10/14/2020 06:11:17 pm

From the Configuration Management Page, we are going to look at Baseline Management. Baseline Management is the ability to set a baseline configuration for your networking devices and be able to identify any configuration that falls outside of the set baseline.

Action: Click ‘BASELINE MANAGEMENT’.

## Step 2.

### Baseline Management



Here we see there are already two different types of baselines set. We are going to configure a new one in the lab.

Action: Click 'NEW BASELINE' as shown above.

### Step 3.

#### New Baseline Config

##### Baseline Name

502nd - Router Baseline

##### Description

Baseline configuration for a router

##### This baseline is:

- A complete config file (should **exactly match** any configs it is compared to)
- A snippet of a config file (compared configs should **contain** all of this snippet)

##### File to use as baseline

PASTE

BROWSE

No file selected yet.

#### CONFIGURE

As always, we will need to give this baseline a name and description.

Move to next step.

## Step 4.

### New Baseline Config

Baseline Name  
502nd - Router Baseline

Description  
Baseline Router Configuration

This baseline is:

A complete config file (should **exactly match** any configs it is compared to)

A snippet of a config file (compared configs should **contain** all of this snippet)

File to use as baseline

**PASTE**  

**BROWSE** No file selected yet.

---

**CONFIGURE**

Action: Type in the Name Field “Services”.

Action: Type in the Description Field “All services we need on a cisco router”.

Action: Click ‘PASTE’ as show above.

## Step 5.

Paste Baseline

Paste the config file you want to use as a baseline in the text box below.

```
no ip bootp server
no ip domain lookup
ip domain name nmsnil.local
login on-failure log
login on-success log
```

SAVE CANCEL

Here is where we will input the services of a Cisco Router that are supposed to be part of the baseline configuration for our devices. We are only going to use three, but we understand there are many more.

## Step 6.

### CONFIGURE

- no ip bootp server
- no ip domain lookup
- ip domain name nmsn1.local
- login on-failure log
- login on-success log

Action: Type in the three-commands seen in the picture above.

ASSIGN TO NODES (0) **SAVE** CANCEL

Action: Click 'SAVE' in the lower right-hand corner when done.

## Step 7.

### New Baseline Config

#### Baseline Name

502nd - Router Baseline

#### Description

Baseline Router Configuration

#### This baseline is:

- A complete config file (should **exactly match** any configs it is compared to)
- A snippet of a config file (compared configs should **contain** all of this snippet)

#### File to use as baseline

PASTE

BROWSE

No file selected yet.

#### CONFIGURE

- no ip bootp server
- no ip domain lookup
- ip domain name nmsn11.local
- login on-failure log
- login on-success log

Our baseline is now configured.

Action: Click ‘SUBMIT’ at the bottom of the screen.

Step 8.

## Baseline Management

The screenshot shows the 'Baseline Management' section of a software interface. At the top, there is a navigation bar with tabs: 'CONFIG MANAGEMENT', 'TRANSFER STATUS', 'INVENTORY STATUS', 'SCRIPT MANAGEMENT', and 'BASELINE MANAGEMENT'. The 'BASELINE MANAGEMENT' tab is currently selected. Below the navigation bar is a toolbar with several buttons: '+ NEW BASELINE', 'EDIT', 'APPLY/REMOVE' (which is highlighted with a red box), 'ENABLE', 'DISABLE', 'UPDATE', and 'DELETE'. To the left of the toolbar are two dropdown menus and a search bar labeled 'Name'. Below the toolbar, a list displays a single baseline entry: '502nd - Router Baseline' with a checked checkbox next to it. This entry is also highlighted with a red box. To the right of the entry is the text 'Baseline Router Configuration'. At the bottom of the list area, there are navigation controls: '< 1 >' and '1-1 of 1'.

For the baseline to be active we need to enable it.

Action: Select the Baseline, then click 'APPLY/REMOVE' in the Baseline tool bar above.

## Step 9.

### APPLY/REMOVE

Set the **502nd - Router Baseline** baseline to the following nodes:

The screenshot shows a configuration interface for applying a baseline to network nodes. On the left, there's a sidebar with 'FILTERS' expanded, showing 'Machine Type (3)', 'Status (2)', and 'Vendor (3)' sections. Under 'Vendor', 'Cisco' is selected. In the center, a table lists four routers: 'ipv4s2.nmsnil.local', 'ipv4s3.nmsnil.local', 'ipv6s2.nmsnil.local', and 'ipv6s3.nmsnil.local', all of which have a checkmark in the 'Selected' column. To the right, an 'APPLY TO' section has 'Running' checked. A 'SELECTED' list on the far right shows the four router names again, each with a delete icon.

FILTERS: (1)	Node / Vendor	Cisco	Clear All
<b>FILTERS</b>			
Machine Type (3)			
Status (2)			
<b>Vendor (3)</b>			
Cisco	<input checked="" type="checkbox"/>		
Unknown	<input type="checkbox"/>		
Windows	<input type="checkbox"/>		

Caption	Search...	Q
ipv4s2.nmsnil.local		
ipv4s3.nmsnil.local		
ipv6s2.nmsnil.local		
ipv6s3.nmsnil.local		

APPLY TO
<input type="checkbox"/> Interface Brief
<input type="checkbox"/> NTP Status
<input checked="" type="checkbox"/> Running
<input type="checkbox"/> SNMP User

SELECTED: (4) <span style="float: right;">CLEAR ALL</span>
ipv4s2.nmsnil.local <span style="float: right;">X</span>
ipv4s3.nmsnil.local <span style="float: right;">X</span>
ipv6s2.nmsnil.local <span style="float: right;">X</span>
ipv6s3.nmsnil.local <span style="float: right;">X</span>

Action: Under the 'Filters' column select the vendor drop-down option and check the box next to 'Cisco'

Action: In the center column, Select all four routers

Action: Under the 'APPLY TO' column select 'Running' config type.

Action: Click 'SAVE' at the bottom right-hand corner of the window.

## Step 10.

### Baseline Management

The screenshot shows the 'BASELINE MANAGEMENT' tab selected in a navigation bar. Below it is a toolbar with buttons for 'NEW BASELINE', 'EDIT', 'APPLY/REMOVE', 'ENABLE', 'DISABLE', 'UPDATE', and 'DELETE'. A search bar with dropdown menus for 'Name' and 'Status' is present. The main area displays a table with one row: '502nd - Router Baseline' under 'Name', 'Baseline Router Configuration' under 'Type', and 'Updating...' with a progress bar and '4 nodes Applied to' status.

Once the baseline is applied to the devices an audit will be performed.

The screenshot shows an audit results page for the '502nd - Router Baseline'. It includes a header with a close button, sorting and filtering options ('Sort' and 'Show'), and a search bar. The main table lists four devices: 'ipv4s2.nmsn11.local' (Running, No issues), 'ipv6s2.nmsn11.local' (Running, Mismatched lines), 'ipv4s3.nmsn11.local' (Running, Mismatched lines), and 'ipv6s3.nmsn11.local' (Running, Mismatched lines). At the bottom, there are navigation links for pages 1-4 of 4.

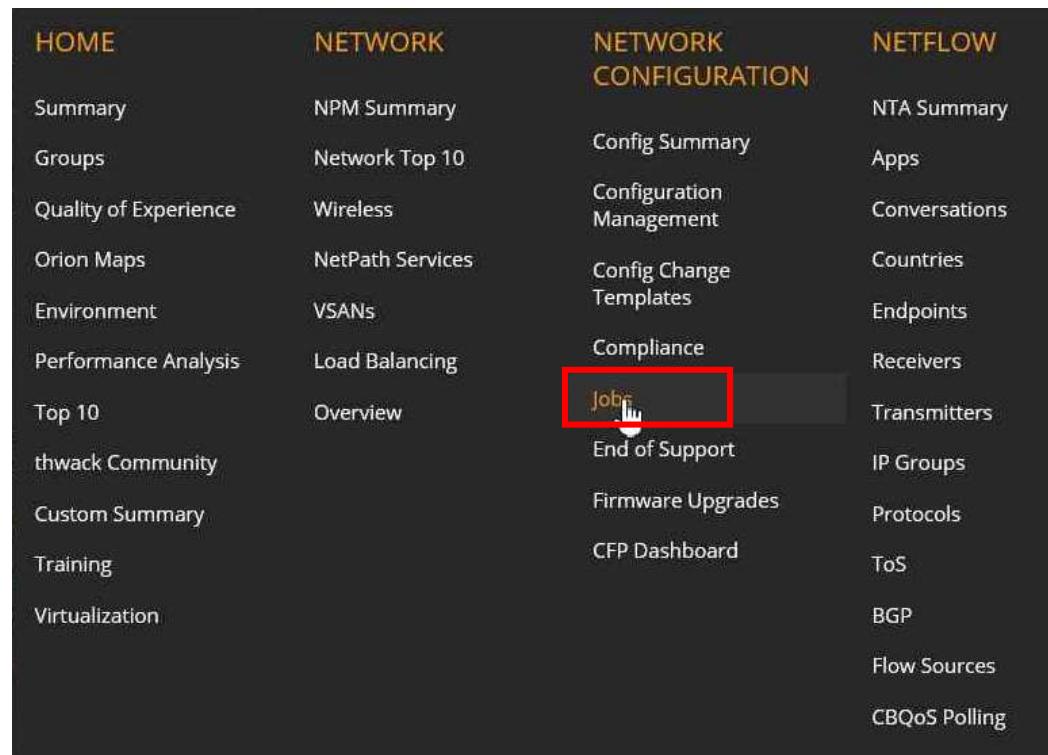
The baseline is evaluated every night at 11:45pm and a notification will be shown once the process has completed. We already see the other two baselines have devices that are outside the standard configuration.

This concludes the lab exercise.

# Lab 15 – NCM Jobs

This lab will teach the student on how to configure a SolarWinds NCM Job. Jobs are helpful in performing duties in management the SolarWinds System and the network. Today we are going to work on backing up our network device configurations.

## Step 1.

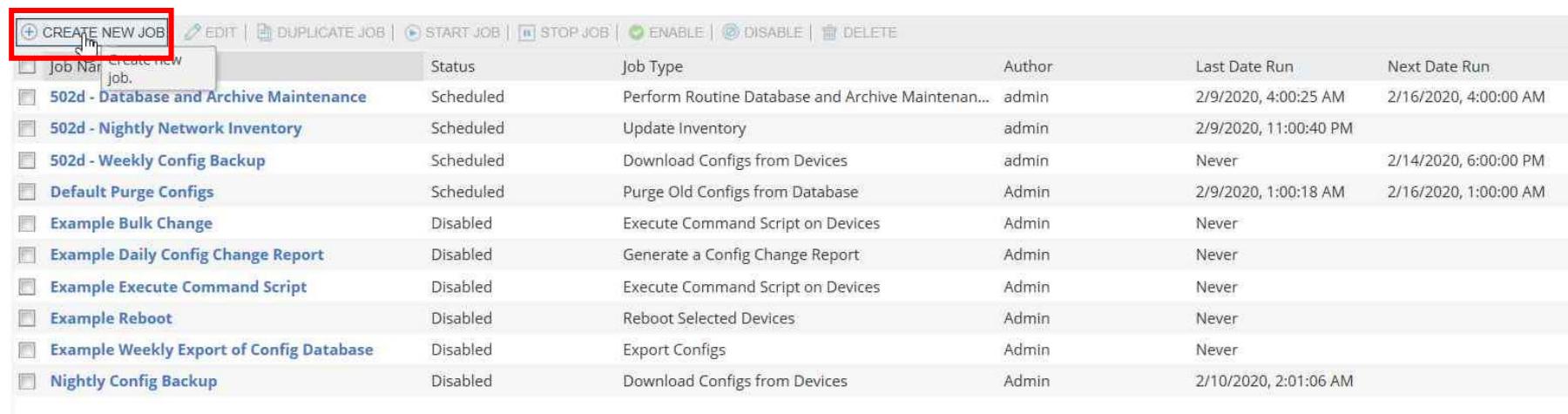


From the MY DASHBOARDS > NETWORK CONFIGURATION > Jobs Menu we will go to the Jobs Page.

Action: Navigate to MY DASHBOARDS > NETWORK CONFIGURATION > Jobs.

## Step 2.

### Jobs List



The screenshot shows a table titled 'Jobs List' with various job entries. At the top, there is a toolbar with buttons for CREATE NEW JOB, EDIT, DUPLICATE JOB, START JOB, STOP JOB, ENABLE, DISABLE, and DELETE. A red box highlights the 'CREATE NEW JOB' button. The table has columns for Job Name, Status, Job Type, Author, Last Date Run, and Next Date Run. The data includes:

Job Name	Status	Job Type	Author	Last Date Run	Next Date Run
502d - Database and Archive Maintenance	Scheduled	Perform Routine Database and Archive Maintenance	admin	2/9/2020, 4:00:25 AM	2/16/2020, 4:00:00 AM
502d - Nightly Network Inventory	Scheduled	Update Inventory	admin	2/9/2020, 11:00:40 PM	
502d - Weekly Config Backup	Scheduled	Download Configs from Devices	admin	Never	2/14/2020, 6:00:00 PM
Default Purge Configs	Scheduled	Purge Old Configs from Database	Admin	2/9/2020, 1:00:18 AM	2/16/2020, 1:00:00 AM
Example Bulk Change	Disabled	Execute Command Script on Devices	Admin	Never	
Example Daily Config Change Report	Disabled	Generate a Config Change Report	Admin	Never	
Example Execute Command Script	Disabled	Execute Command Script on Devices	Admin	Never	
Example Reboot	Disabled	Reboot Selected Devices	Admin	Never	
Example Weekly Export of Config Database	Disabled	Export Configs	Admin	Never	
Nightly Config Backup	Disabled	Download Configs from Devices	Admin	2/10/2020, 2:01:06 AM	

Here we are going to create a new job to save our device configurations.

Action: Click 'CREATE NEW JOB' button.

### Step 3.

#### Create New Job

CREATE JOB > CHOOSE NODES > ENTER NOTIFICATION DETAILS > ADD JOB SPECIFIC DETAILS > REVIEW >

New Job Details

Name of Job: 502d - Weekly Save Configuration

Job Type: Execute Command Script on Devices

Schedule Type: Basic

ONCE DAILY WEEKLY MONTHLY

EVERY 1 day(s)

EVERY WEEK DAY

Start time: 17:00 Enter time values from 00:00 through 24:00. Use HH:MM format (NCM Server time: 10:29 UTC -6)

Starting On: 2/13/2020 Ending On: 2/13/2030

First, we need to give the job a name, define what type of job we are going to create, then decide on a schedule.

Name of Job: [Unit Number] – Weekly Save Configuration

Job Type: Execute Command Script on Devices

Schedule: Basic Every Weekday to start at 17:00

## Step 4.

### Create New Job

CREATE JOB > CHOOSE NODES > ENTER NOTIFICATION DETAILS > ADD JOB SPECIFIC DETAILS > REVIEW >

#### Choose Nodes

Select the nodes that are required for the job:

Select Nodes     All Nodes     Dynamic Selection (Choose nodes that meet certain criteria)

Vendor is Cisco

Wildcard matching may be used.  
Examples of wildcard matching:

- Match values beginning with 'AX3-'  
Use AX3-\*
- Match values ending in '-TX'  
Use \*-TX



We are going to use look for all Cisco Devices.

Action: Select 'Dynamic Selection'. Then drop down the Node ID box down and select Vendor in the list. Next type 'Cisco' into the box as shown above.

## Step 5.

### Create New Job

CREATE JOB > CHOOSE NODES > **ENTER NOTIFICATION DETAILS** > ADD JOB SPECIFIC DETAILS > REVIEW >

Save Job Log  
 Save Results To File  
 Email Results     Do Not Email Results

BACK NEXT CANCEL

We will not be selecting or changing any items here.

Action: Click the 'NEXT' button

## Step 6.

### Create New Job

CREATE JOB > CHOOSE NODES > ENTER NOTIFICATION DETAILS > **ADD JOB SPECIFIC DETAILS** > REVIEW >

#### Execute Script Job



```
Load Saved Script | Load Script from File | Save Script to File  
wr mem  
copy run start
```

Filter results that match a pattern:  » Learn more about patterns

Show commands in output

Here in the text box field we will enter the two different commands Cisco uses to save a configuration to NVRAM.

In the Text box type as shown above. Be sure to add the several lines (Carriage Returns) between each command as some Cisco Operating Systems will ask for filenames.

## Step 7.

### Review New Job

CREATE JOB > CHOOSE NODES > ENTER NOTIFICATION DETAILS > ADD JOB SPECIFIC DETAILS > REVIEW

Confirm the information you entered to create this job. To make changes, go back by selecting the back button at the bottom of the page

**Job Name:** 502d - Weekly Save Configuration

**Job Type:** Execute Command Script on Devices

**Frequency of Job:** Daily, every day

**Job Run Time:** 5:00 PM

**Comments:** Issuing a copy running start command to all Cisco Devices

**Nodes Selected:** 2 Nodes Selected

**Email Notification:** Disabled

This tab in the wizard will give us a summary of our new job.

Action: Select ‘FINISH’ to create the job.

## Step 8.

### Jobs List

CREATE NEW JOB	EDIT	DUPLICATE JOB	START JOB	STOP JOB	ENABLE	DISABLE	DELETE
Job Name	Status	Job Type	Author	Last Date Run	Next Date Run		
502d - Database and Archive Maintenance	Scheduled	Perform Routine Database and Archive Maintenan...	admin	2/9/2020, 4:00:25 AM	2/16/2020, 4:00:00 AM		
502d - Nightly Network Inventory	Scheduled	Update Inventory	admin	2/9/2020, 11:00:40 PM			
502d - Weekly Config Backup	Scheduled	Download Configs from Devices	admin	Never	2/14/2020, 6:00:00 PM		
502d - Weekly Save Configuration	Scheduled	Execute Command Script on Devices	admin	Never			
Default Purge Configs	Scheduled	Purge Old Configs from Database	Admin	2/9/2020, 1:00:18 AM	2/16/2020, 1:00:00 AM		
Example Bulk Change	Disabled	Execute Command Script on Devices	Admin	Never			
Example Daily Config Change Report	Disabled	Generate a Config Change Report	Admin	Never			
Example Execute Command Script	Disabled	Execute Command Script on Devices	Admin	Never			
Example Reboot	Disabled	Reboot Selected Devices	Admin	Never			
Example Weekly Export of Config Database	Disabled	Export Configs	Admin	Never			
Nightly Config Backup	Disabled	Download Configs from Devices	Admin	2/10/2020, 2:01:06 AM			

You have completed building a new job.

Continue to next step to develop your NCM Jobs.

## Step 9.

To continue with this lab and setting up our jobs. Perform the following Actions.

### Database and Archive Maintenance Job

- Change the name of the job to incorporate the new naming standards.
- Change day of the week to: Sunday
- Change time of day to: 0400
- Update description

### Nightly Network Inventory

- Change the name of the job to incorporate the new naming standards
- Change day of the week to: Every Weekday
- Change time of day to: 2000
- Update description
- Use dynamic selection to only run this job on Cisco Nodes

### Weekly Config Backup

- Change the name of the job to incorporate the new naming standards
- Change day of the week to: Monday, Wednesday, Friday, & Sunday
- Change time of day to: 1800
- Update description
- Use dynamic query to selection only Cisco Routers running IOS operating systems

### Other tasks

- Ensure all Jobs modified or created thus far are listed as ‘Scheduled’
- All other Jobs shall be listed as ‘Disabled’

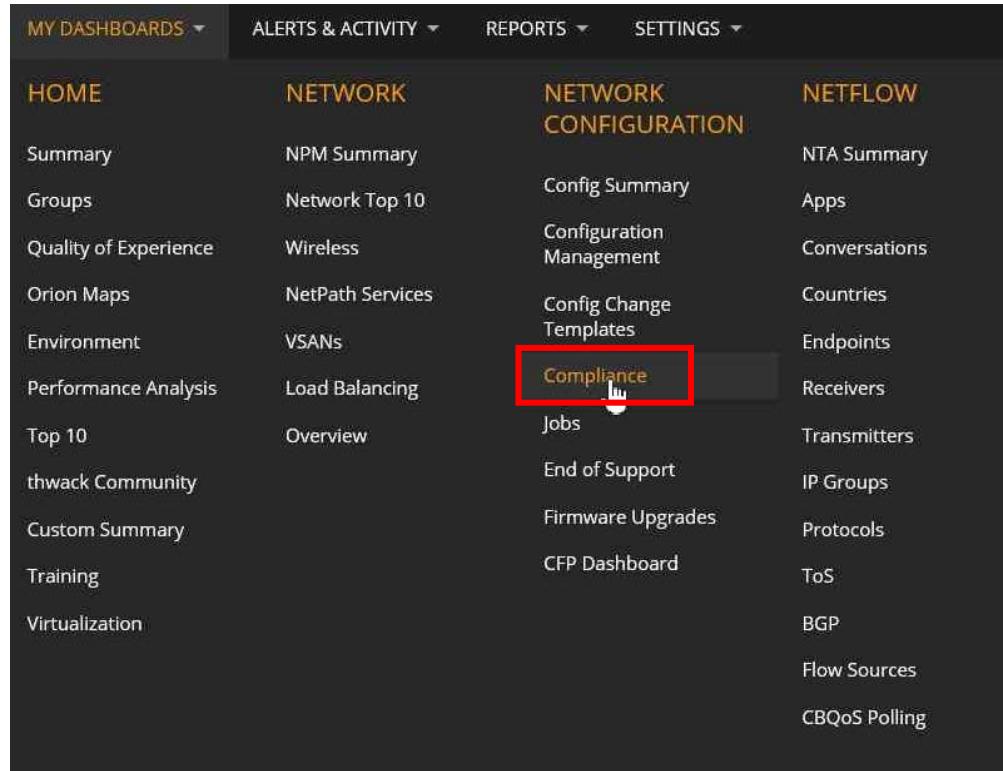
This concludes the lab exercise.

This page intentionally left blank.

# Lab 16 - Compliance

This lab will provide the student with the capability to apply the DISA STIGs for networking devices to the network audit every night.

## Step 1.



The screenshot shows the NCM (Cisco Network Manager) Settings page. The top navigation bar includes 'MY DASHBOARDS', 'ALERTS & ACTIVITY', 'REPORTS', and 'SETTINGS'. Under 'SETTINGS', there are four main categories: 'HOME', 'NETWORK', 'NETWORK CONFIGURATION', and 'NETFLOW'. The 'NETWORK CONFIGURATION' category is expanded, showing sub-options like 'Config Summary', 'Configuration Management', 'Config Change Templates', 'Compliance' (which is highlighted with a red box), 'Jobs', 'End of Support', 'Firmware Upgrades', 'CFP Dashboard', 'Protocols', 'ToS', 'BGP', 'Flow Sources', and 'CBQoS Polling'. Other sections like 'NETFLOW' also have their own sub-options.

From the Settings page we will go into the compliance section of the NCM and begin our lab.

Action: Navigate to MY DASHBOARDS > NETWORK CONFIGURATION > Compliance.

## Step 2

### Manage Policy Reports

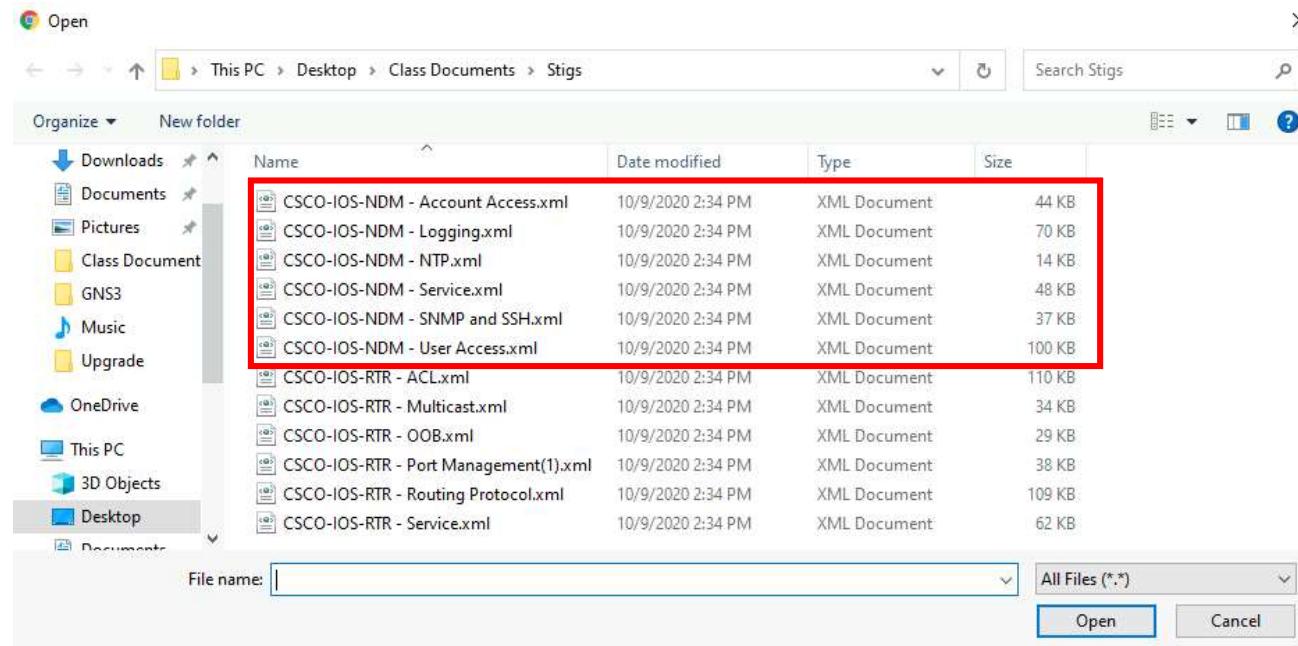
The screenshot shows a web-based management interface for policy reports. At the top, there's a yellow banner with a question mark icon and the text "How do I set up a Report? Create a rule. Add that rule to a policy. Add that policy to a report. » Learn more". Below the banner is a navigation bar with four tabs: "MANAGE REPORTS" (which is selected and highlighted in dark blue), "MANAGE POLICIES", "MANAGE RULES", and "SHARED ON THWACK". Underneath the navigation bar is a toolbar with various icons: "+ ADD NEW REPORT", "EDIT", "VIEW REPORT", "UPDATE ALL", "ENABLE", "DISABLE", "IMPORT" (which is highlighted with a red box), "EXPORT AS FILE", "EXPORT TO THWACK", and "DELETE". The main area has a search bar with "All (0)" selected and a dropdown menu for "Name". Below the search bar are three columns: "Last Update", "Folder", and "Description".

We are going straight into the rules and start from the bottom and work our way up to the report as seen in the lecture. You may see some of the native reports SolarWinds installs when the Configuration Wizard is executed. Here we want to work from a clean slate.

Action: Delete all Reports, Policies, and Rules.

Next: We are going to import a Report download from Thwack. Click on 'IMPORT' in the menu bar located above.

### Step 3.



We are looking for the downloaded file.

Action: Locate the file ‘CSCO-IOS-NDM’ file in our Software folder located on your desktop. Select this file.

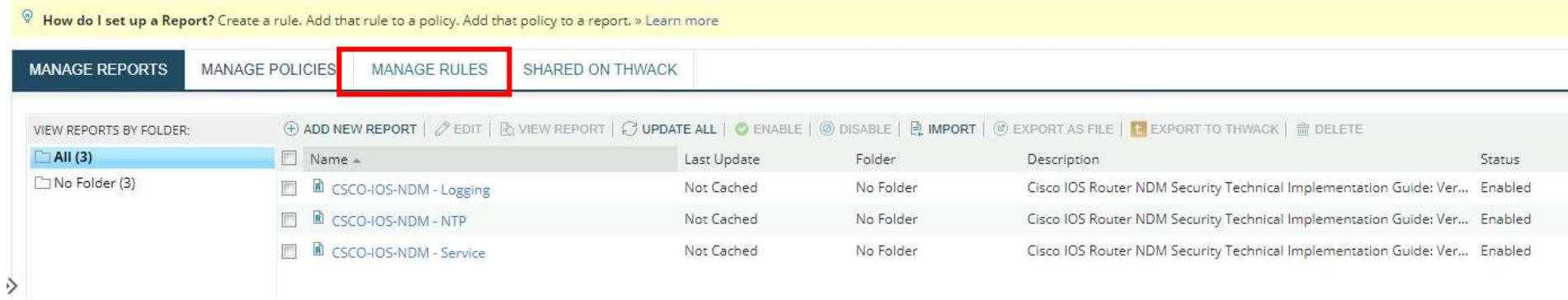
### Import Policy Report

Choose File CSCO-IOS-NDM - NTP.xml

**SUBMIT** **CANCEL**

## Step 4.

### Manage Policy Reports



The screenshot shows the 'Manage Policy Reports' page. At the top, there are four tabs: 'MANAGE REPORTS', 'MANAGE POLICIES', 'MANAGE RULES' (which is highlighted with a red box), and 'SHARED ON THWACK'. Below the tabs is a yellow banner with the text: 'How do I set up a Report? Create a rule. Add that rule to a policy. Add that policy to a report. » Learn more'. The main area is titled 'VIEW REPORTS BY FOLDER:' and shows a folder structure. Under 'All (3)', there are three items: 'CSCO-IOS-NDM - Logging', 'CSCO-IOS-NDM - NTP', and 'CSCO-IOS-NDM - Service'. Each item has columns for Name, Last Update, Folder, Description, and Status. A toolbar at the top of this section includes buttons for 'ADD NEW REPORT', 'EDIT', 'VIEW REPORT', 'UPDATE ALL', 'ENABLE', 'DISABLE', 'IMPORT', 'EXPORT AS FILE', 'EXPORT TO THWACK', and 'DELETE'.

Name	Last Update	Folder	Description	Status
CSCO-IOS-NDM - Logging	Not Cached	No Folder	Cisco IOS Router NDM Security Technical Implementation Guide: Ver...	Enabled
CSCO-IOS-NDM - NTP	Not Cached	No Folder	Cisco IOS Router NDM Security Technical Implementation Guide: Ver...	Enabled
CSCO-IOS-NDM - Service	Not Cached	No Folder	Cisco IOS Router NDM Security Technical Implementation Guide: Ver...	Enabled

Once the Report has been imported into your SolarWinds Server you will have the ability to start modifying the rules, policies and reports to meet your organization's needs.

Action: Navigate to 'MANAGE RULES' section.

## Step 5.

The screenshot shows a user interface for managing rules. At the top, there are four tabs: 'MANAGE REPORTS', 'MANAGE POLICIES', 'MANAGE RULES' (which is the active tab), and 'SHARED ON THWACK'. Below the tabs is a toolbar with buttons for 'ADD NEW RULE', 'EDIT' (circled in red), 'COPY', and 'DELETE'. A dropdown menu labeled 'GROUP BY' is set to '[No Grouping]'. The main area is a table listing rules, with columns for 'Rule Name', 'Last Modified', and 'Folder'. A red arrow points to the row for 'CSCO-IOS-NDM-CISC-ND-001030 - NTP', which has a checked checkbox in the first column. The table includes pagination at the bottom, showing '1 of 2' pages with a page size of 25.

Rule Name	Last Modified	Folder
CSCO-IOS-NDM-CISC-ND-000470 - Service	10/14/2020 07:58 pm	CSCO-IOS-NDM
CSCO-IOS-NDM-CISC-ND-000620 - Service	10/14/2020 07:58 pm	CSCO-IOS-NDM
CSCO-IOS-NDM-CISC-ND-000720 - Service	10/14/2020 07:58 pm	CSCO-IOS-NDM
CSCO-IOS-NDM-CISC-ND-000810 - Service	10/14/2020 07:58 pm	CSCO-IOS-NDM
CSCO-IOS-NDM-CISC-ND-000880 - Logging	10/14/2020 07:57 pm	CSCO-IOS-NDM
CSCO-IOS-NDM-CISC-ND-000900 - Service	10/14/2020 07:58 pm	CSCO-IOS-NDM
CSCO-IOS-NDM-CISC-ND-000940 - Logging	10/14/2020 07:57 pm	CSCO-IOS-NDM
CSCO-IOS-NDM-CISC-ND-000980 - Logging	10/14/2020 07:57 pm	CSCO-IOS-NDM
CSCO-IOS-NDM-CISC-ND-000990 - Logging	10/14/2020 07:57 pm	CSCO-IOS-NDM
CSCO-IOS-NDM-CISC-ND-001000 - Logging	10/14/2020 07:57 pm	CSCO-IOS-NDM
<input checked="" type="checkbox"/> CSCO-IOS-NDM-CISC-ND-001030 - NTP	10/14/2020 07:59 pm	CSCO-IOS-NDM
CSCO-IOS-NDM-CISC-ND-001040 - NTP	10/14/2020 07:57 pm	CSCO-IOS-NDM
CSCO-IOS-NDM-CISC-ND-001050 - NTP	10/14/2020 07:57 pm	CSCO-IOS-NDM

Action: Navigate to the rule named 'CSCO-IOS-NDM-CISC-ND-001030 – NTP' and select then click 'EDIT'.

## Edit CSCO-IOS-NDM-CISC-ND-001030 - NTP

Rules describe what is to be found (or not found) in configuration files. If the rule is not met, the rule violation will appear with the error level set below in the policy report.

### IDENTIFY THIS RULE

Rule name: CSCO-IOS-NDM-CISC-ND-001030 - NTP

Description: The Cisco router must be configured to synchronize its clock with the primary and secondary time sources using redundant authoritative time sources.

Alert level:  ⓘ Informational  ⚠ Warning  ⚡ Critical

Save in folder: CSCO-IOS-NDM

### STRING MATCHING

Alert on the rule below if  String is found  String is NOT found

Advanced Config Search(block search and/or search)

AND/OR	PARENS (OPTIONAL)	MUST/MUST NOT CONTAIN	STRING TYPE	STRING	PARENS (OPTIONAL)
		Config File	must contain	Find string	ntp server x.x.x.x
and		Config File	must contain	Find string	ntp server y.y.y.y

[ADD ANOTHER STRING](#)

[CHECK PARENTHESIS](#)

Check parenthesis in conditional statement. This does not check any parenthesis in a regular expression.

The Rule Name is the name of the rule with a standardized format.

- CSCO – Cisco
- IOS - IOS
- RTR – Router
- NDM – Network Device Management

The Description is the Group Title which comes directly from the STIG Guide itself.

Alert Level - We have previously set them to be CAT III, CAT II, CAT I in NCM Settings Lab.

Folder – This is the folder where this Rule is contained.

#### String Matching

Here we have to conditions set. The text in the String boxes are CLI commands and configurations within a Cisco Devices. The rules ask, does the configuration match exactly what is configured in the String boxes? If so, then the rule is not in violation. If it does not, then the rule is in violation and you will receive a color icon in your Policy Report.

Action: Configure the String Boxes to meet the require for the NTP configuration in the Cisco devices.

- A. The first box should read: **ntp server10.50.2.100 key 1 prefer**
- B. The second cox should read: **ntp server 10.50.2.200 key 2**

## Step 6.

SEARCH CONFIG FILE/BLOCK

Search in  Entire config file  Config block

REMEDIATION

Remediation script:

[Load Saved Script](#) | [Load Script from File](#) | [Save Script to File](#)

Check Content:  
Review the router or switch configuration and verify that two NTP servers have been defined to synchronize time similar to the following example:

```
ntp update-calendar
ntp server 129.237.32.6
ntp server 129.237.32.7
```

Some platforms have a battery-powered hardware clock, referred to in the command-line interface (CLI) as the "calendar," in addition to the software based system clock. The hardware clock runs continuously, even if the router is powered off or rebooted. If the software clock is synchronized to an outside time source via NTP, it is a good practice to periodically update the hardware clock with the time learned from NTP. Otherwise, the hardware clock will tend to gradually lose or gain time (drift) and the software clock and hardware clock may become out of synchronization with each other. The `ntp update-calendar` command will enable the hardware clock to be periodically updated with the time specified by the NTP source. The hardware clock will be updated only if NTP has synchronized to an authoritative time server. To force a single update of the hardware clock from the software clock, use the `clock update-calendar` command in user EXEC mode.

Note: Lower end router models (i.e., 2500 series) and access switches (i.e., 2950, 2970, etc) do not have hardware clocks, so this command is not available on those platforms.

Any NTP-enabled device that receives and accepts time from a stratum-n server can become a stratum-n+1 server. However, an NTP-enabled device will not accept time updates from an NTP server at a higher stratum; thereby enforcing a tree-level hierarchy of client-server relationships and preventing time synchronization loops. To increase availability, NTP peering can be enabled.

When a rule violation is found, you will have the option of running this script. [More about remediation](#).

Remediate Script type:

CLI

Automatically execute this script when violation is found

Execute Script in Config Mode

Config Change Template

**SUBMIT** CANCEL TEST

In the bottom of the rule, there is a remediation section. This can contain CLI commands which will correct any violation, or it can be used as a Notes section. It is very dangerous to let your Network Management System configure your network without you there!

Action: Click 'SUBMIT'.

## Step 7.

### Manage Policy Report Policies

The screenshot shows a web-based application interface titled "Manage Policy Report Policies". At the top, there are four tabs: "MANAGE REPORTS", "MANAGE POLICIES" (which is highlighted with a red box), "MANAGE RULES", and "SHARED ON THWACK". Below the tabs is a table with the following columns: "GROUP BY" (set to "Folder"), "Policy Name", "Last Modified", "Folder", "Appears in Report", and "Contains Rule". There is also a header row with icons for "ADD NEW POLICY", "EDIT", "COPY", and "DELETE". The table contains three entries under the "CSCO-IOS-NDM (3)" folder:

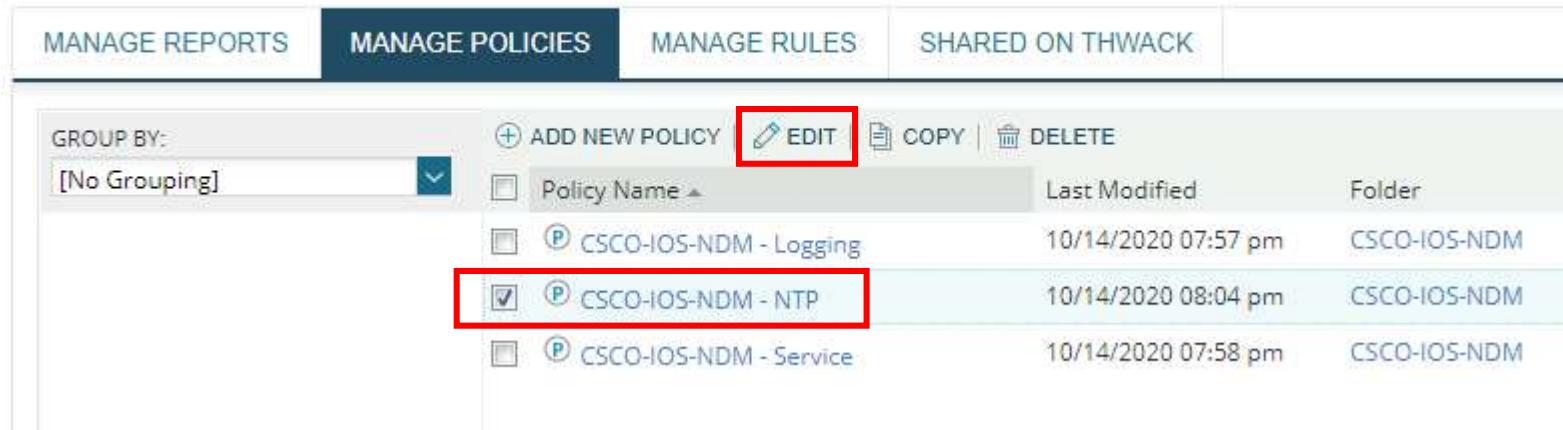
GROUP BY	Policy Name	Last Modified	Folder	Appears in Report	Contains Rule
CSCO-IOS-NDM (3)	(P) CSCO-IOS-NDM - Logging	10/14/2020 07:57 pm	CSCO-IOS-NDM	CSCO-IOS-NDM - Logging	CSCO-IOS-NDM-CISC-ND-000210 - Logging, CSCO-I...
	(P) CSCO-IOS-NDM - NTP	10/14/2020 07:57 pm	CSCO-IOS-NDM	CSCO-IOS-NDM - NTP	CSCO-IOS-NDM-CISC-ND-001030 - NTP, CSCO-IOS-...
	(P) CSCO-IOS-NDM - Service	10/14/2020 07:58 pm	CSCO-IOS-NDM	CSCO-IOS-NDM - Service	CSCO-IOS-NDM-CISC-ND-000810 - Service, CSCO-I...

Let's move over to the Policy Tab.

Action: Click 'MANAGE POLICIES'.

Step 8.

## Manage Policy Report Policies



The screenshot shows a web-based management interface for policy reports. At the top, there are four tabs: 'MANAGE REPORTS', 'MANAGE POLICIES' (which is selected and highlighted in dark blue), 'MANAGE RULES', and 'SHARED ON THWACK'. Below the tabs is a toolbar with buttons for 'ADD NEW POLICY', 'EDIT' (which has a red box around it), 'COPY', and 'DELETE'. A dropdown menu labeled 'GROUP BY:' is set to '[No Grouping]'. The main area displays a table of policies:

Policy Name	Last Modified	Folder
CSCO-IOS-NDM - Logging	10/14/2020 07:57 pm	CSCO-IOS-NDM
CSCO-ISO-NDM - NTP	10/14/2020 08:04 pm	CSCO-IOS-NDM
CSCO-IOS-NDM - Service	10/14/2020 07:58 pm	CSCO-IOS-NDM

Here we will be adding a new policy to support our Router Network Device Management Compliance STIGs for NTP and Logging audits.

Action: Select the 'CSCO-ISO-NDM – NTP' Policy and click 'EDIT'.

## Step 9.

Edit CSCO-IOS-NDM - NTP

Policy name: CSCO-IOS-NDM - NTP

Description:

Save in folder: CSCO-IOS-NDM

Select nodes:

All nodes  
 Select nodes  
 Dynamic selection

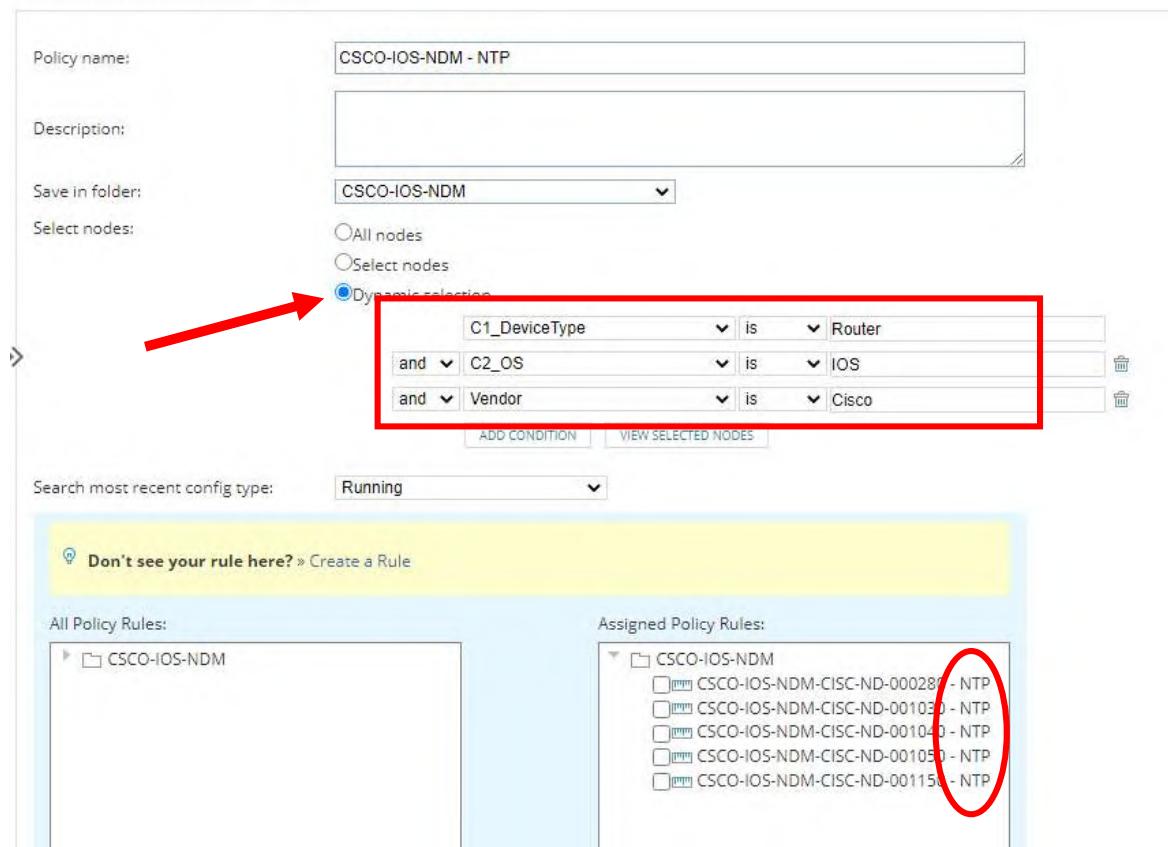
C1\_DeviceType is Router  
and C2\_OS is IOS  
and Vendor is Cisco

Search most recent config type: Running

Don't see your rule here? » Create a Rule

All Policy Rules: CSCO-IOS-NDM

Assigned Policy Rules: CSCO-IOS-NDM  
CSCO-IOS-NDM-CISC-ND-00128 - NTP  
CSCO-IOS-NDM-CISC-ND-00103 - NTP  
CSCO-IOS-NDM-CISC-ND-00104 - NTP  
CSCO-IOS-NDM-CISC-ND-00105 - NTP  
CSCO-IOS-NDM-CISC-ND-00115 - NTP



To configure the Policy, review the above configurations. Once we click on the ‘Dynamic selection’, SolarWinds will provide a list of all the Standard Properties and Custom Properties.

Action: Scroll down and select C1\_DeviceType. We are going to use the operand ‘is’ for our conditional statement. Then in the last field we will enter the Router.

- A. Policy Name: CSCO-IOS-RTR-NDM - NTP and Logging
- B. New Folder Name: CSCO-IOS-NDM
- C. Select Nodes:
  - a. Dynamic Selection
    - i. C1\_DeviceType is Router
    - ii. C2\_OS is IOS
    - iii. Vendor is Cisco
- D. Select all rules that have NTP or Logging at the end of the rule name as show above.

## Step 10.

### Edit CSCO-IOS-NDM - NTP

Policy name: CSCO-IOS-NDM - NTP

Description:

Save in folder: CSCO-IOS-NDM

Select nodes:

All nodes  
 Select nodes  
 Dynamic selection

C1\_DeviceType is Router  
and C2\_OS is IOS  
and Vendor is Cisco

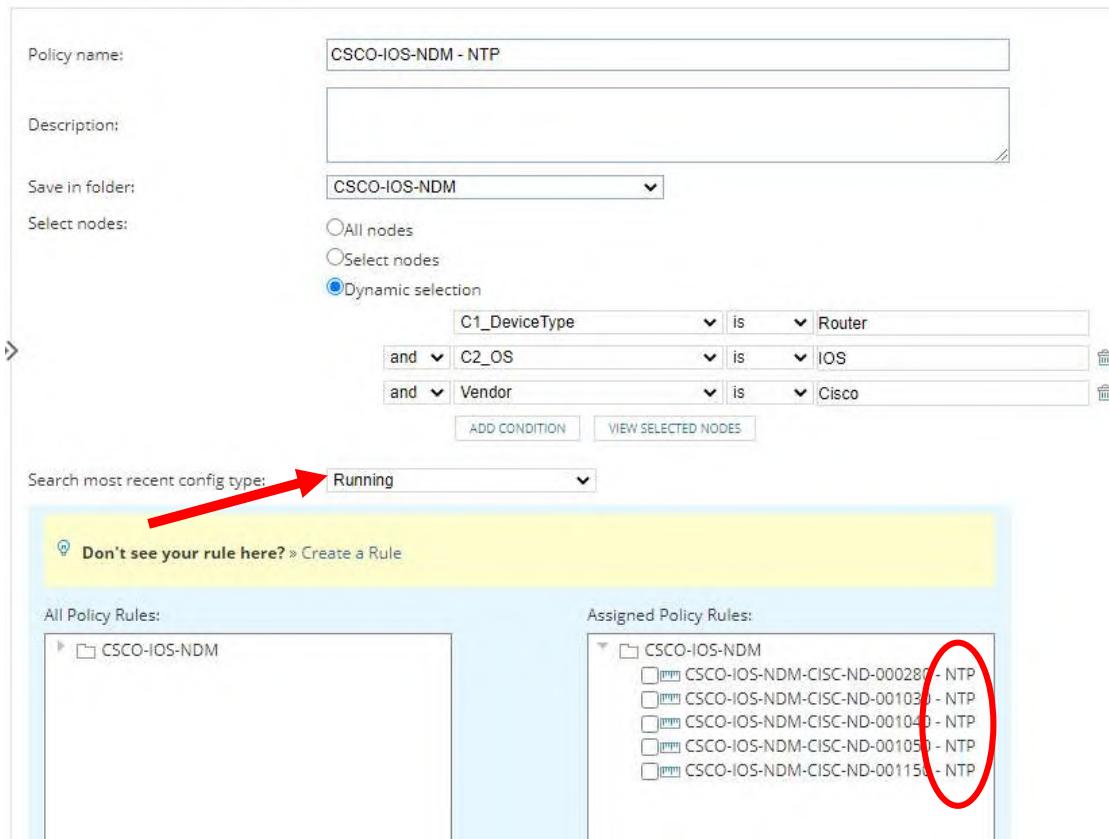
ADD CONDITION    VIEW SELECTED NODES

Search most recent config type: Running

Don't see your rule here? » Create a Rule

All Policy Rules: CSCO-IOS-NDM

Assigned Policy Rules: CSCO-IOS-NDM (circled)  
CSCO-IOS-NDM-CISC-ND-000287 - NTP  
CSCO-IOS-NDM-CISC-ND-001030 - NTP  
CSCO-IOS-NDM-CISC-ND-001040 - NTP  
CSCO-IOS-NDM-CISC-ND-001050 - NTP  
CSCO-IOS-NDM-CISC-ND-001151 - NTP



Action:

- A. Select the most recent config type: Running
- B. Select the following rules as you see above. We are looking for all the rules with NTP in the Name.

## Step 11.

Manage Policy Report Policies

Policy Name	Last Modified	Folder	Appears in Report	Contains Rule
CSCO-IOS-NDM - Logging	10/14/2020 07:57 pm	CSCO-IOS-NDM	CSCO-IOS-NDM - Logging	CSCO-IOS-NDM-CISC-ND-000210 - Logging, CSCO-I...
CSCO-IOS-NDM - NTP	10/14/2020 08:09 pm	CSCO-IOS-NDM	CSCO-IOS-NDM - NTP	CSCO-IOS-NDM-CISC-ND-001030 - NTP, CSCO-IO...
CSCO-IOS-NDM - Service	10/14/2020 07:58 pm	CSCO-IOS-NDM	CSCO-IOS-NDM - Service	CSCO-IOS-NDM-CISC-ND-000810 - Service, CSCO-I...

Once we have our policy configured, we will move on to the report.

Action: Select 'MANAGE REPORTS' in the menu bar above.

## Step 12.

### Manage Policy Reports



The screenshot shows a web-based management interface for policy reports. At the top, there are tabs: 'MANAGE REPORTS' (which is selected), 'MANAGE POLICIES', 'MANAGE RULES', and 'SHARED ON THWACK'. Below the tabs is a yellow banner with a question mark icon and the text: 'How do I set up a Report? Create a rule. Add that rule to a policy. Add that policy to a report.' followed by a link '» Learn more'. The main area is titled 'VIEW REPORTS BY FOLDER:' and shows a list of reports. There are two sections: 'All (3)' and 'No Folder (3)'. Under 'All (3)', there are three items: 'CSCO-IOS-NDM - Logging', 'CSCO-IOS-NDM - NTP' (which has a checked checkbox and is highlighted with a red box), and 'CSCO-IOS-NDM - Service'. Under 'No Folder (3)', there are no items. To the right of the list are columns for 'Last Update', 'Folder', 'Description', and 'Status'. At the top of the list area, there are several buttons: '+ ADD NEW REPORT', 'EDIT' (which is highlighted with a red box), 'VIEW REPORT', 'UPDATE SELECTED', 'ENABLE' (with a green checkmark), 'DISABLE' (with a grey circle), 'IMPORT', 'EXPORT AS FILE', 'EXPORT TO THWACK' (with a blue icon), and 'DELETE'. A vertical scrollbar is visible on the left side of the list area.

Name	Last Update	Folder	Description	Status
CSCO-IOS-NDM - Logging	Not Cached	No Folder	Cisco IOS Router NDM Security Technical Implementation Guide: Ver...	Enabled
<input checked="" type="checkbox"/> CSCO-IOS-NDM - NTP	Not Cached	No Folder	Cisco IOS Router NDM Security Technical Implementation Guide: Ver...	Enabled
CSCO-IOS-NDM - Service	Not Cached	No Folder	Cisco IOS Router NDM Security Technical Implementation Guide: Ver...	Enabled

Action: Select the 'CSCO-IOS-NDM – NTP' and click on 'Edit'.

## Step 13.

### Edit CSCO-IOS-NDM - NTP

Policy report name: CSCO-IOS-NDM - NTP

Description: Cisco IOS Router NDM Security Technical Implementation Guide: Version: 1; Release: 2; 24 Jan 2020

Save in folder: New folder

Display settings:

Include report summary

Show rules without violation

Don't see your policy here? [Create a Policy](#)

All Policies: CSCO-IOS-NDM

Assigned Policies: CSCO-IOS-NDM CSCO-IOS-NDM - NTP

SUBMIT CANCEL

Here we will provide the following information to configure the report.

Policy Report Name: CSCO-IOS-NDM – NTP

Description: Provide the current STIG in which this report was derived.

Folder: Place the report into the folder of other like reports based on Device Type.

Policies in the Report: Select the correct policy for this report.

## Step 14.

### Manage Policy Reports

The screenshot shows a web-based management interface for policy reports. At the top, there's a yellow banner with a link to 'How do I set up a Report?'. Below it is a navigation bar with tabs: 'MANAGE REPORTS' (which is selected and highlighted in dark blue), 'MANAGE POLICIES', 'MANAGE RULES', and 'SHARED ON THWACK'. The main content area has a title 'VIEW REPORTS BY FOLDER:' followed by a dropdown menu set to 'All (3)'. There are three reports listed:

Name	Last Update	Folder	Description	Status
CSCO-IOS-NDM - Logging	Waiting	No Folder	Cisco IOS Router NDM Security Technical Implementation Guide: Ver...	Enabled
CSCO-IOS-NDM - NTP	Waiting	No Folder	Cisco IOS Router NDM Security Technical Implementation Guide: Ver...	Enabled
CSCO-IOS-NDM - Service	Waiting	No Folder	Cisco IOS Router NDM Security Technical Implementation Guide: Ver...	Enabled

A red box highlights the 'UPDATE ALL' button in the toolbar above the table. A red arrow points from the bottom of the 'UPDATE ALL' button towards the 'Waiting' status of the first report in the list.

Once you have created the report, you will need to update by selecting either ‘UPDATE ALL’ or ‘UPDATE SELECTED’ in order for SolarWinds Compliance and the Configuration of the device to be compiled and audited. It will take 15 seconds to audit the last downloaded config. The system will continue to audit every report every 15 seconds until complete.

## Step 15.

### CSCO-IOS-NDM - NTP

Last updated Wednesday, November 4, 2020 07:12:27 PM

REPORT DETAILS		CSCO-IOS-NDM - NTP (searched 20 configs)				
Node Name	IP Address	CSCO-IOS-NDM-CISC-ND-000280 - NTP (0 violations)	CSCO-IOS-NDM-CISC-ND-001030 - NTP (0 violations)	CSCO-IOS-NDM-CISC-ND-001040 - NTP (0 violations)	CSCO-IOS-NDM-CISC-ND-001050 - NTP (0 violations)	CSCO-IOS-NDM-CISC-ND-001150 - NTP (0 violations)
ipv4s2.nmsnil.local	10.50.2.61	✓	✓	✓	✓	✓
ipv4s3.nmsnil.local	10.50.2.62	✓	✓	✓	✓	✓
ipv6s2.nmsnil.local	10.50.2.63	✓	✓	✓	✓	✓
ipv6s3.nmsnil.local	10.50.2.64	✓	✓	✓	✓	✓

Once the update has been completed, you will be able to review the results. Here we have four CAT III findings and one CAT II finding. In order to remediate these issues, you will need to review the SolarWinds Compliance Rule and/or adjust the device configuration to satisfy the finding.

## Step 16.

To continue with this lab, create the following reports, policies, and remediate each of the findings.

Import all the Reports in your Class Documents > STIG folder and remediate findings.

This concludes the lab exercise.

# Appendix A – Comprehensive Review

Purpose: Give the students the ability to test their knowledge of the material covered so far in the course.

Duration: estimated 8.0 hours

1. Turn off Windows Firewall and User Access Control Settings
2. Set system time to current locale and time zone
3. Install SolarWinds NPM2020.2 Software.
  - a. Install NPM, NTA, NCM, UDT on the E:\
4. Discovery
  - a. Discover all devices residing inside the 10.50.20/24 subnet.
    - i. Cisco Devices will be 10.50.2.61-64
    - ii. Orion Server will be 10.50.2.1
    - iii. Discover local subnets: 10.0.0.0/24 & 10.2.0.0/24
    - iv. Others may be discovered
  - b. Create SNMPv3 Credentials from the Cisco Configuration File
  - c. Create a Connection Profile from the README File
5. Custom Properties
  - a. Configure the following Custom Properties with assigned variables using the BITI BAN Custom Properties Worksheet.
6. Groups
  - a. Modify and Create the following Groups and place your unit number in front of the Name of the group.
    - i. Example 502d – C1\_DeviceType - Routers
  - b. Configure a group for all Windows Devices using a Dynamic Query
  - c. Configure a group for all Cisco Devices using a Dynamic Query
  - d. Configure a group for all Unknown Desktop devices using a Dynamic Query
7. Create a View
  - a. This view will be named “502d - Site Audit”
    - i. Add Custom Object Resource Widget to Column 1

1. Name Widget “Average Response Time”
    2. Select all routers
    3. Report for the last 24 hours
    4. Every Minute
  - ii. Add Policy Violations Widget to Column 2
  - b. Place this new view in the Network Configuration Menu Bar
8. Create a User Account
- a. Create an Admin user named nisgaa
    - i. NCM Administrator rights
  - b. Create a Read-only Account using your name
    - i. NCM with WebUploader permissions
9. Manage Nodes
- a. Node Database must be 100% complete
  - b. Windows identified machines will be polled at 5 minutes
  - c. Cisco identified devices will be polled at 3 minutes
  - d. Unknown devices will be polled at 10 minutes
10. Create a Connection Profile
- a. Be sure to place your unit in front of the name.
  - b. This profile will be used for the Cisco Router using Telnet
11. Device Templates
- a. Configure Config Types with the following Names
    - i. NTP Status
    - ii. SNMP User
    - iii. Interface Brief
  - b. Using the interactive Wizard editor
  - c. Modify your Cisco IOS device template
    - i. Name the new command NTP
    - ii. run a *show ntp status* command
  - d. Modify your Cisco IOS device template
    - i. Name the new command Brief

- ii. run a *show ip interface brief* command
  - e. Modify your Cisco IOS device template
    - i. Name the new command Brief
    - ii. run a *show snmp user* command
  - f. Statically assign it to your Cisco Router Device
12. Configure NCM Config types to download NTP and Brief commands
- a. Download an NTP Configuration
  - b. Download an Interface Brief Configuration
  - c. Download a SNMP User Configuration
13. Script Management
- a. Be sure to append your unit number in front of the name of each script
  - b. Develop Script Management for the following with all commands required to:
    - i. NTP Configuration to support STIG Compliance
    - ii. Services Configuration to support STIG Services
14. Compliance
- a. Remove all Compliance Reports, Policies and Procedures
  - b. Modify the Violation Levels
    - i. Critical to CAT I
    - ii. Warning to CAT II
    - iii. Informational to CAT III
  - c. Import the following Reports
    - i. Logging
    - ii. NTP
    - iii. Services
    - iv. SSH and SNMP
  - d. Remediate for all reports
  - e. Rename all rules with unit number in front
  - f. Rename all policies with unit number in front
  - g. Rename all Reports with unit number in front
15. Baseline Management

- a. Be sure to append your unit number in front of the name of each baseline
- b. Develop Baseline management to support the following
  - i. NTP Configuration
    1. Server 1 is your IP which is preferred, key is 444
    2. Server 2 is your default gateway IP, Key is 555
  - ii. Banner Configuration
  - iii. Services configuration

## 16. Jobs

- a. Create a job to run a script using the following commands
  - i. *write memory*
  - ii. *copy running start*
  - iii. This job will run every Monday, Wednesday, Friday at 8:00pm.
- b. Modify the Weekly Configuration Backup
  - i. This job will run every Tuesday, Thursday, Saturday at 8:30pm.

## Appendix B: Custom Properties

L1_Base	L2_Building	L3_Room	L4_Rack
Use Base USAF Geo-Location Code. 4 digits	Use number of the building. 4 digits	Use Room Number. 4 Digits	Use Rack number or location identifier
MPLS	1435	0020	101
TYMX	1814	0100	103
CATD	1712	101B	435C
C1_DeviceType	C2_OS	C3_Function	C4_Application
Router	IOS	Network Device	Sharepoint
Switch	NXOS	Server	SQL
Server	IOS-XE	Firewall	ADDC
Workstation	2016	Workstation	Web Server
	2019		Application Server
	2010		Orion