

SolarWinds Network Management Guide



● ● ● SMART BUSINESS ARCHITECTURE

February 2013 Series

Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in February 2013 is the “February Series”.

You can find the most recent series of SBA guides at the following sites:

Customer access: <http://www.cisco.com/go/sba>

Partner access: <http://www.cisco.com/go/sbachannel>

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100  
100 100 100
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64  
ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

If you would like to comment on a guide or ask questions, please use the [SBA feedback form](#).

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

Table of Contents

What's In This SBA Guide	1
Cisco SBA Borderless Networks	1
Route to Success	1
About This Guide	1
Introduction	2
Business Overview	2
Technology Overview	2
Deployment Details	4
Day 0—Set Up Network Management System/Assess and Configure Network Devices	4
Day 1—Baseline the Network and Start Monitoring	4
Day 2+—Optimize and Maintain the Health of the Network Prerequisites	4
Setting Up Network Management System (Day 0)	5
Assessing and Configuring Network Devices (Day 0)	9
Baselining the Network and Start Monitoring (Day 1)	12
Optimizing and Maintaining Network Health (Day 2+)	16

Appendix A: Network Details	18
Appendix B: SolarWinds Contact Information	19
End Users	19
Resellers	19

What's In This SBA Guide

Cisco SBA Borderless Networks

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Borderless Networks is a comprehensive network design targeted at organizations with up to 10,000 connected users. The SBA Borderless Network architecture incorporates wired and wireless local area network (LAN) access, wide-area network (WAN) connectivity, WAN application optimization, and Internet edge security infrastructure.

Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

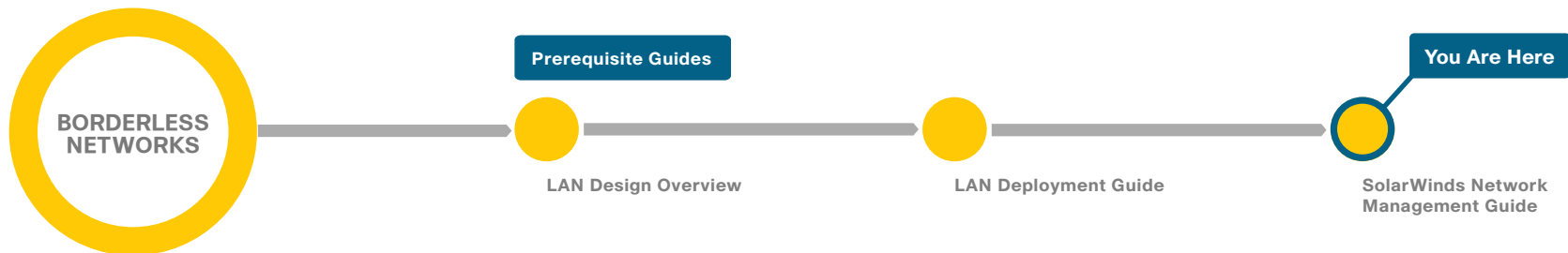
About This Guide

This *ecosystem partner guide* presents solutions, products, or services—provided by a Cisco SBA ecosystem partner—that are compatible with and complementary to SBA.

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: <http://www.cisco.com/go/sba>

Partner access: <http://www.cisco.com/go/sbachannel>



Introduction

Business Overview

The complexity and challenges of managing the network are ever increasing. IT staff is tasked with maintaining operational efficiency of the network. The abilities to monitor, isolate, and fix network performance issues are critical to minimizing network disruption and downtime. These abilities fall into different use cases, such as network configuration, deployment, monitoring, and troubleshooting. An IT staff's top concern is to have a unified network management application that can help them address these needs, thus increasing the staff's productivity. This guide is focused on our partnership with SolarWinds and their products that meet Cisco's goal to deliver affordable, easy-to-use network configuration, monitoring, and change management.

Technology Overview

Deploying the configuration modules outlined in the Cisco Smart Business Architecture (SBA) deployment guides in an efficient manner, while simultaneously maintaining the availability and performance of the network infrastructure when everything is constantly changing, is not an easy challenge to solve without the right tools. Network management systems can help by allowing you to automate configuration tasks and monitor network health, giving you the visibility required to quickly troubleshoot issues. In keeping with the blueprint theme of Cisco SBA, this guide describes the SolarWinds' Orion family of network management products, which are designed with an out-of-the-box deployment that is simple, fast, affordable, scalable, and flexible. Additionally, the Orion family of products has been tested and validated with the components described in the Cisco SBA deployment guides.

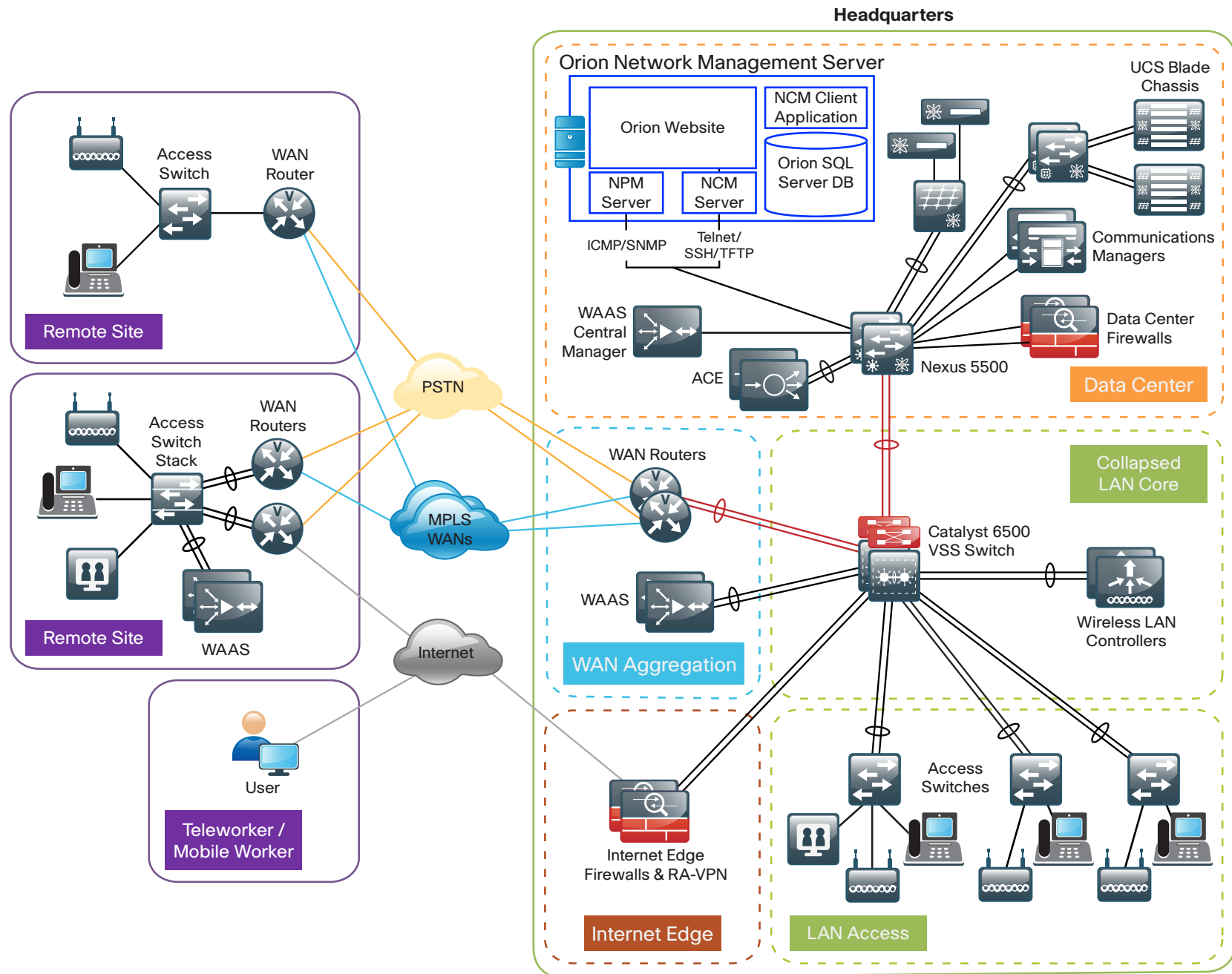
This guide is comprised of two SolarWinds Orion products:

- **Orion Network Configuration Manager (NCM)**—Used for managing and monitoring network configuration changes. Config management operations are performed using Secure Shell (SSH) Protocol, Telnet, Trivial File Transfer Protocol (TFTP), Secure File Transfer Protocol (SFTP), or Secure Copy (SCP).
- **Orion Network Performance Monitor (NPM)**—Used for quickly detecting, diagnosing, and resolving network performance problems and outages. Availability and performance statistics are polled using Internet Control Message Protocol (ICMP), Simple Network Management Protocol (SNMP), and Windows Management Instrumentation (WMI).

You can download a free trial of NPM and NCM from

http://www.solarwinds.com/Cisco_Orion

Figure 1 - Architectural overview of NPM and NCM in Cisco SBA



Deployment Details

For clarity, this document organizes the network management deployment process around the various tasks you'll complete on Day 0, Day 1, and Day 2+ in your Cisco SBA network deployment process. The actual setup of the Orion products should take about an hour.

Day 0—Set Up Network Management System/ Assess and Configure Network Devices

The Day 0 section guides you through the initial setup of the Orion network management system and how to use the system to assess and manage the device configurations for your Cisco SBA network. Perform the steps in this section immediately following the universal and global settings procedures, outlined in the *Cisco SBA—Borderless Networks LAN Deployment Guide*. This enables you to use Orion NCM to inventory the existing network, assess the differences in the network device configurations from Cisco baseline configurations, and push the configuration changes required for subsequent module deployments.

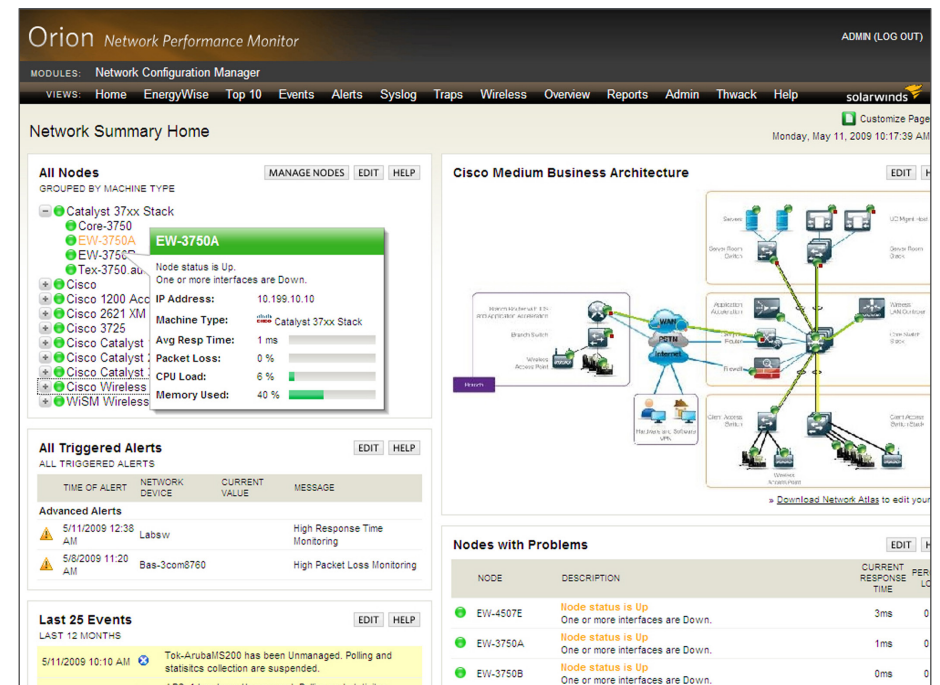
Day 1—Baseline the Network and Start Monitoring

The Day 1 section guides you through the steps necessary to baseline the network and start monitoring. Perform this section immediately following the deployment of all required Cisco SBA modules and components, so that you may back up your configurations and gain visibility into any problems affecting network performance.

Day 2+—Optimize and Maintain the Health of the Network

The Day 2+ section guides you through the steps necessary to optimize and maintain the health of your network. This section can be performed at any time, but is recommended that you perform this section immediately after the Day 1 section tasks. This allows you to determine if there are opportunities to optimize the performance of your network and resolve any capacity issues proactively.

Figure 2 - Network summary view



Prerequisites

Before you begin the deployment process, ensure that you follow the steps outlined in the universal and global settings procedures in the *Cisco SBA—Borderless Networks LAN Deployment Guide* to set up IP addresses and to configure standard management protocols for each device you want to manage.

The SolarWinds Orion network management products leverage SNMP for gathering availability and performance data, and SSH (Telnet or TFTP) for executing configuration management operations across your network devices.

Orion requires a Windows Server with the following minimum specifications:

Hardware

- Dual core processor, 3GHz
- 3 GB memory
- 20 GB available disk space

Software

- Windows 2003 Server SP2 (32-bit or 64-bit) including R2, with Microsoft Internet Information Services (IIS) installed, running in 32-bit mode
- Windows 2008 Server Enterprise or Standard (32-bit or 64-bit) including R2, with IIS installed, running in 32-bit mode
- .NET Framework Version 3.5 or later (SP1 recommended)
- Microsoft SNMP Trap Services

Database

- The Orion NPM evaluation automatically installs SQL 2005 Express by default, which can be used by Orion NCM as well
- SQL Server 2005/2008 Standard or Enterprise for production deployments



Reader Tip

Appendix A includes a table where you can record for future reference the login credentials and community string information, which you configure during the deployment process.

Process

Setting Up Network Management System (Day 0)

1. Install Orion NPM
2. Install Orion NCM

Download a fully functional 30-day trial of the Orion network management software required to complete this module from http://www.solarwinds.com/Cisco_Orion

Procedure 1

Install Orion NPM

Step 1: Log in to the Windows server using an account with Administrator privileges.

Step 2: Run the Orion NPM executable, and then select **Express installation**. This automatically installs Orion NPM and configures a SQL 2005 Express database server for monitoring data storage.

After Orion NPM Configuration Wizard has completed, the Orion Web Console automatically opens in your default browser.

Step 3: Log in by entering **admin** and a blank password (you may change this later).

The Network Sonar Wizard appears. This enables you to discover your devices.

The screenshot shows the 'SNMP Credentials' step of the Network Sonar Wizard. It includes a message about 10 new blog posts, a breadcrumb trail to 'Discovery Central', and a list of existing credentials. The list has two entries: 'public' and 'private', both using 'SNMP v1 or v2c'. Each entry has up, down, edit, and delete icons. At the bottom are 'NEXT' and 'CANCEL' buttons.

Order	Credential	Version	Actions
1	public	SNMP v1 or v2c	↑ ↓ ✎ ✕
2	private	SNMP v1 or v2c	↑ ↓ ✎ ✕

Step 4: Enter optional credentials for vCenter or ESX hosts, and then click **Next**.

Step 5: Enter optional WMI credentials for your Windows servers, and then click **Next**.

Step 6: Enter an IP address range, and then click **Next**.

The screenshot shows the 'Network Selection' step. It prompts the user to click a selection method to define the network portion for discovery. A yellow callout box suggests using the 'Specific Nodes' method for IPv6 addresses. Under 'SELECTION METHOD', 'IP Ranges' is selected. Below it are input fields for 'Start address' and 'End address', and an 'Add More' button. At the bottom are 'BACK', 'NEXT', and 'CANCEL' buttons.

Step 7: Leave the Discovery Settings unchanged, and then click **Next**.

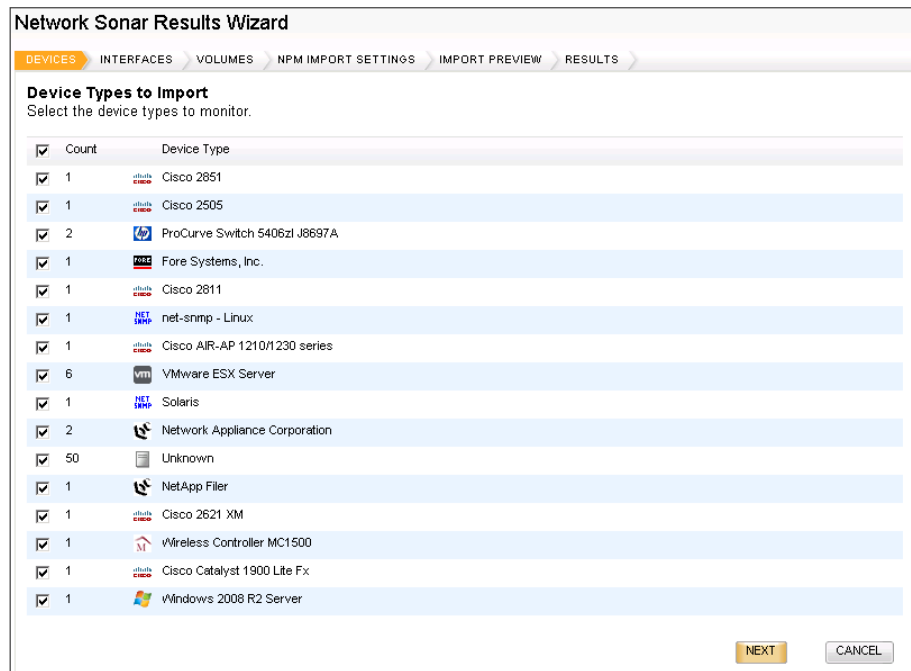
Step 8: Leave the frequency at Once, and then click **Discover**.

The screenshot shows the 'Discovery Scheduling' step. It allows configuring a schedule for discovery. The 'Frequency' is set to 'Once'. Under 'Execute immediately', the radio button for 'Yes, run this discovery now' is selected. At the bottom are 'BACK', 'DISCOVER', and 'CANCEL' buttons.

Step 9: Let the discovery run for a few minutes.

The screenshot shows the 'Discovering Network...' progress window. It displays the progress for 'Hop 0: Discovering: 10.199.4.234'. The 'Overall Progress' and 'Current Phase' are shown as progress bars. Below, it shows 'Nodes Discovered: 66' and 'Subnets Discovered: 0'. A 'CANCEL' button is at the bottom right.

Step 10: Clear the check box next to the device types that you do not want to keep and monitor, and then click **Next**.



Network Sonar Results Wizard

DEVICES INTERFACES VOLUMES NPM IMPORT SETTINGS IMPORT PREVIEW RESULTS

Device Types to Import
Select the device types to monitor.

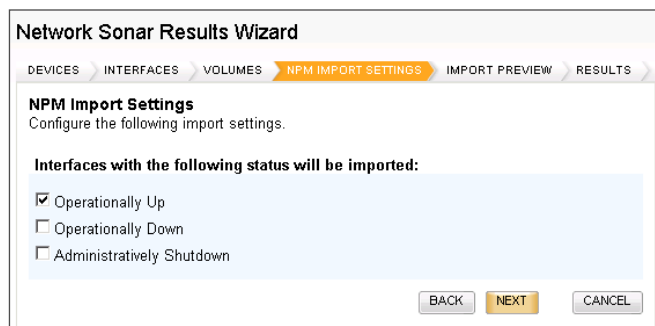
<input checked="" type="checkbox"/>	Count	Device Type
<input checked="" type="checkbox"/>	1	Cisco 2851
<input checked="" type="checkbox"/>	1	Cisco 2505
<input checked="" type="checkbox"/>	2	ProCurve Switch 5406zl J8697A
<input checked="" type="checkbox"/>	1	Fore Systems, Inc.
<input checked="" type="checkbox"/>	1	Cisco 2811
<input checked="" type="checkbox"/>	1	net-snmp - Linux
<input checked="" type="checkbox"/>	1	Cisco AIR-AP 1210/I230 series
<input checked="" type="checkbox"/>	6	VMware ESX Server
<input checked="" type="checkbox"/>	1	Solaris
<input checked="" type="checkbox"/>	2	Network Appliance Corporation
<input checked="" type="checkbox"/>	50	Unknown
<input checked="" type="checkbox"/>	1	NetApp Filer
<input checked="" type="checkbox"/>	1	Cisco 2621 XM
<input checked="" type="checkbox"/>	1	Wireless Controller MC1500
<input checked="" type="checkbox"/>	1	Cisco Catalyst 1900 Lite Fx
<input checked="" type="checkbox"/>	1	Windows 2008 R2 Server

NEXT **CANCEL**

Step 11: Clear the check box next to the interface types that you do not want to keep and monitor, and then click **Next**.

Step 12: Clear the check box next to volume types that you do not want to keep and monitor, and then click **Next**.

Step 13: Ensure the default option, **Operationally Up**, is selected, and then click **Next**.



Network Sonar Results Wizard

DEVICES INTERFACES VOLUMES NPM IMPORT SETTINGS IMPORT PREVIEW RESULTS

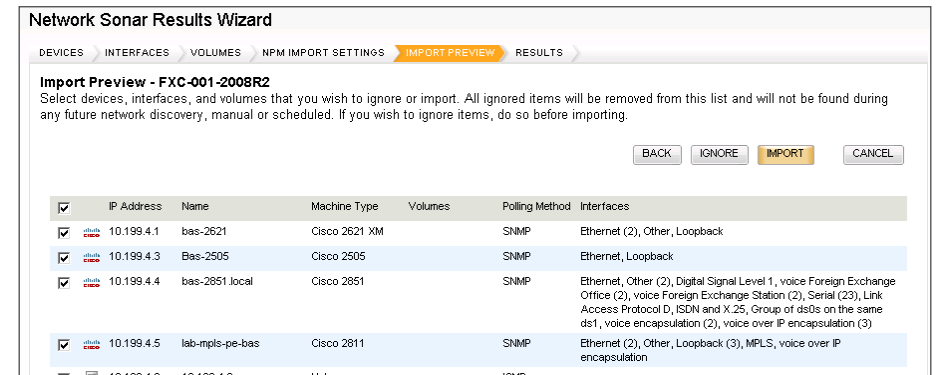
NPM Import Settings
Configure the following import settings.

Interfaces with the following status will be imported:

- ☒ Operationally Up
- ☐ Operationally Down
- ☐ Administratively Shutdown

BACK **NEXT** **CANCEL**

Step 14: Click **Import**. NPM imports all discovered objects.



Network Sonar Results Wizard

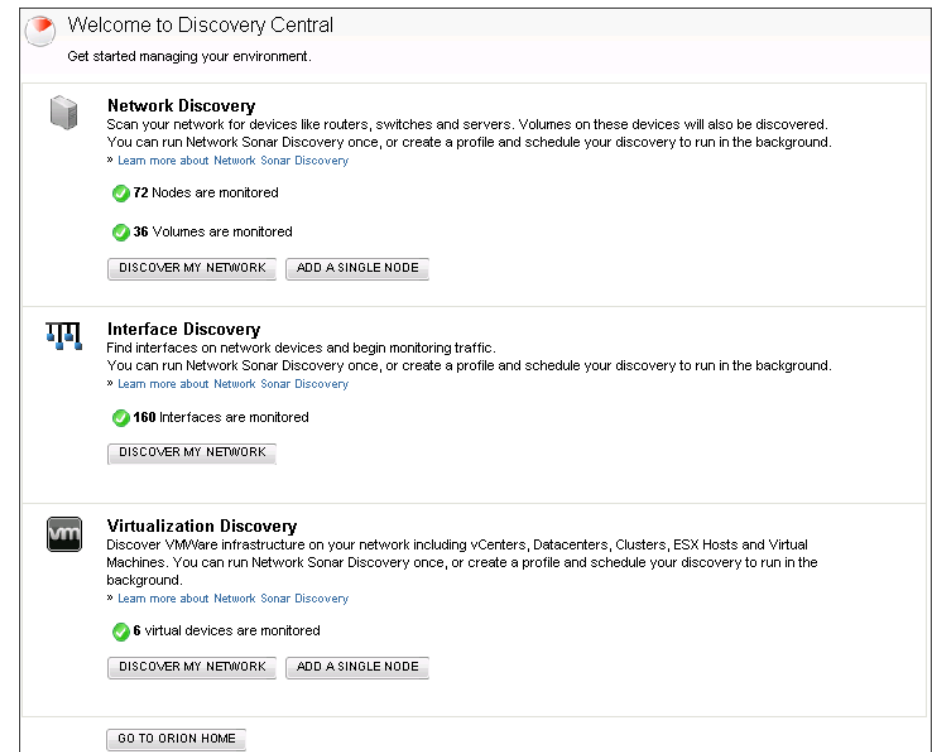
DEVICES INTERFACES VOLUMES NPM IMPORT SETTINGS IMPORT PREVIEW RESULTS

Import Preview - FXC-001-2008R2
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.

BACK **IGNORE** **IMPORT** **CANCEL**

<input checked="" type="checkbox"/>	IP Address	Name	Machine Type	Volumes	Polling Method	Interfaces
<input checked="" type="checkbox"/>	10.199.4.1	bas-2621	Cisco 2621 XM		SNMP	Ethernet (2), Other, Loopback
<input checked="" type="checkbox"/>	10.199.4.3	Bas-2505	Cisco 2505		SNMP	Ethernet, Loopback
<input checked="" type="checkbox"/>	10.199.4.4	bas-2851 local	Cisco 2851		SNMP	Ethernet, Other (2), Digital Signal Level 1, voice Foreign Exchange Office (2), voice Foreign Exchange Station (2), Serial (23), Link Access Protocol D, ISDN and X.25, Group of disks on the same ds1, voice encapsulation (2), voice over IP encapsulation (3)
<input checked="" type="checkbox"/>	10.199.4.5	lab-mlps-pe-bas	Cisco 2811		SNMP	Ethernet (2), Other, Loopback (3), MPLS, voice over IP encapsulation
<input checked="" type="checkbox"/>	10.199.4.6	10.199.4.6	Unknown		ICMP	

Step 15: Click **Finish**, and then click **Go To Orion Home**.



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](#)

72 Nodes are monitored
36 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](#)

160 Interfaces are monitored

DISCOVER MY NETWORK

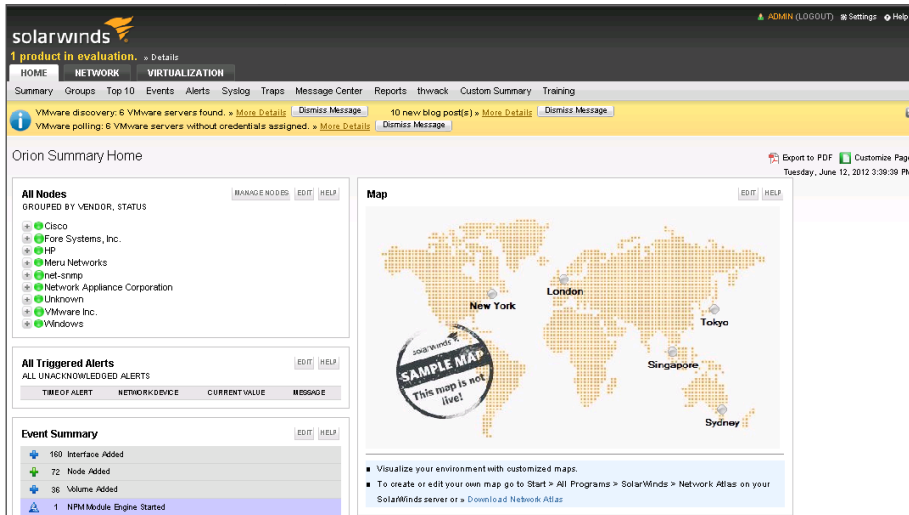
Virtualization Discovery
Discover VMWare infrastructure on your network including vCenters, Datacenters, Clusters, ESX Hosts and Virtual Machines. You can run Network Sonar Discovery once, or create a profile and schedule your discovery to run in the background.
» [Learn more about Network Sonar Discovery](#)

6 virtual devices are monitored

DISCOVER MY NETWORK **ADD A SINGLE NODE**

GO TO ORION HOME

Your discovered objects are now monitored by NPM.



Procedure 2

Install Orion NCM

Step 1: Run the Orion NCM server executable on the same server where you installed Orion NPM. The Configuration Wizard opens.

Step 2: In the Configuration Wizard, select **Advanced**, and then select the same SQL Server that you configured for Orion NPM (by doing this, you avoid installing a second SQL Server just for NCM).

Step 3: In Database Settings, ensure that the NPM SQL server is pre-defined as (local)\SOLARWINDS_ORION, and then click **Next**.

Step 4: Ensure that **Create a new database** is selected, and then keep the default NCM database name (ConfigMgmt) and website settings.

You have just created a new Orion NCM database called ConfigMgmt.

Step 5: Keep all other options at the default value.

Step 6: In System Default Settings, ensure you have entered the correct community string and default authentication settings as configured in the Global Configuration module.



Tech Tip

The default authentication settings are used by Orion NCM to connect to your devices and perform the initial device inventory and configuration backups.

Step 7: On the last page of the wizard, click **Finish**. The Discovery Central web page opens.

Step 8: In the Discovery Central window, scroll down to the Orion NCM section.



NCM Nodes

To manage your node(s), select from these options:

- **Discover Nodes.**

Use this option if you are adding more than a few nodes.

[NETWORK SONAR DISCOVERY >](#)

- **Add a New Node.**

Use this option to add one or two nodes.

[ADD A SINGLE DEVICE >](#)

- **Manage More Nodes.**

Select nodes to manage in NCM.

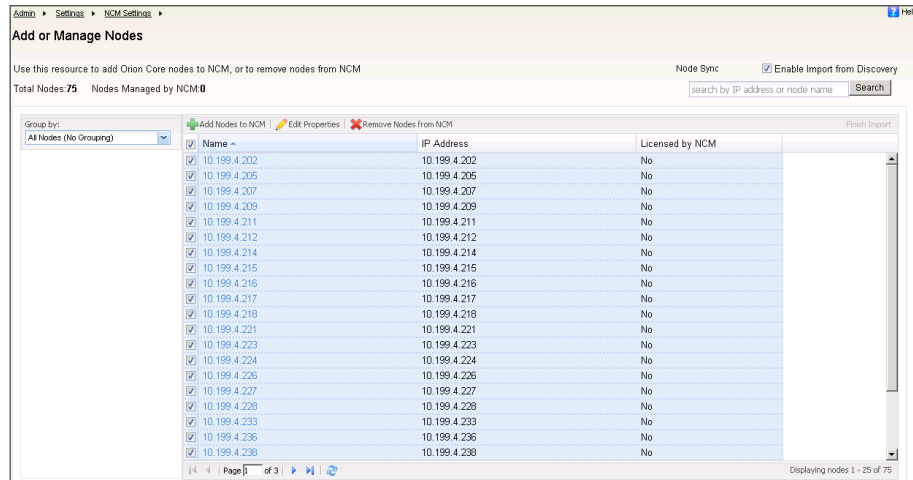
✖ 0 of 75 monitored nodes are currently managed by NCM.

With your license, you can manage an unlimited number of nodes with NCM.

[> Learn more about licensing](#)

[MANAGE MORE NODES >](#)

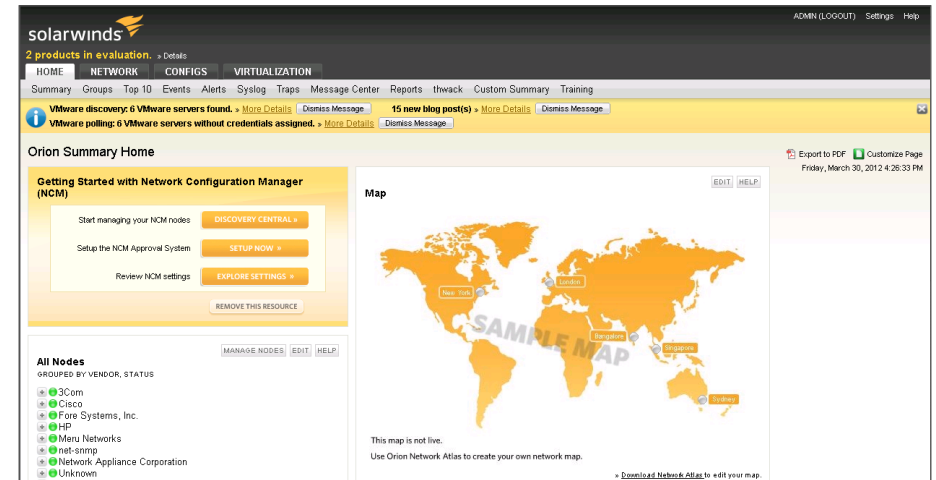
Step 9: Click **Manage More Nodes**, select all your nodes, and then click **Add Nodes to NCM**. This ensures that all the nodes previously discovered and managed by NPM are also managed by NCM.



Step 10: Edit your node properties, including both NPM (example: polling frequency) and NCM (example: device credentials) properties, and then click **Submit**.

After you have installed NPM and NCM on the same server, the Orion view should look like the following figure, with the NPM (Home and Networks and Virtualization tabs) and NCM (Configs tab) integrated in the same pane of glass.

Figure 3 - Orion home view



Process

Assessing and Configuring Network Devices (Day 0)

1. Inventory existing network infrastructure
2. Deploy configuration snippets
3. Assess your variance

Next, you complete the final network preparation activities before finishing the actual deployment.

Procedure 1

Inventory existing network infrastructure

Before you begin the actual deployment process, inventory the existing network infrastructure to determine compatibility with the Cisco SBA architecture.

Step 1: Navigate to **All Programs > SolarWinds Orion Network Configuration Manager > Orion Network Configuration Manager**, and then log in to the Orion NCM client application.

Step 2: Select **Schedule > Display/Edit Jobs**.

Step 3: Right-click the default Nightly Network Inventory job, select **Test Job**, and then click **Start**.

Step 4: If there are any devices with inventories that were unsuccessful, edit each failing device and validate your SNMP credentials.

Step 5: After you have verified that the job completes for all devices, navigate to **Reports > View Reports**, and then run the following reports to help assess hardware and firmware compatibility of the existing devices:

- **Cisco IOS Image Details**—This report displays the feature level, image, system description, and IOS version for each Cisco device.
- **Cisco Card Data**—This report displays the hardware details for each Cisco device, including card name, description, class, position, hardware revision, serial number, and model.

Procedure 2 Deploy configuration snippets

For this example, you enable Syslog and Traps on all Cisco Catalyst 3750 switches you configured in the universal and global settings procedures of the *Cisco SBA—Borderless Networks LAN Deployment Guide*, without having to manually log in to each device. Other global config snippets referenced in the guide can be deployed in a similar fashion.

Step 1: Download the Cisco Catalyst 3750 Enable Syslog-Trap script from the SolarWinds Thwack Content Exchange to your Orion server, from <http://solarwinds.hosted.jivesoftware.com/docs/DOC-75229>

Step 2: Navigate to **All Programs > SolarWinds Orion Network Configuration Manager > Orion Network Configuration Manager**, and then log in to the Orion NCM client application.

Step 3: Right-click the devices tree, and then select **Execute Command Script**.

Step 4: Click **Load Script**. This allows you to browse and select the Cisco Catalyst 3750 script that you downloaded above.

```
{EnterConfigMode}
service timestamps log datetime localtime
logging host <Orion server IP>
snmp-server enable traps
snmp-server host <Orion server IP> public
exit
write memory
```

Step 5: Select the Cisco Catalyst 3750 switches you discovered and configured, and then click **Execute Command Script**.



Tech Tip

The `{EnterConfigMode}` macro automatically enters into config t mode for each target device. For a complete list of macros and variables available for use with command line scripting, consult the Orion NCM Administrator Guide here: <http://www.solarwinds.com/support/orionNCM/docs/orionNCMAdministratorGuide.pdf>

NCM Config Change Templates provide a GUI-based method of generating and distributing configuration snippets. The change templates can be created by extracting the relevant configuration sections from the LAN Configuration Files Guide and parameterizing them as described in the NCM Administrator Guide.

Procedure 3

Assess your variance

If your organization has existing network infrastructure that is referenced in the *Cisco SBA—Borderless Networks LAN Deployment Guide*, perform the following steps to assess its variance from the Cisco baseline configurations for those device types.

Step 1: Navigate to **All Programs > SolarWinds Orion Network Configuration Manager > Orion Network Configuration Manager**, and then log in to the Orion NCM client application.

Step 2: Download the Cisco SBA—Borderless Networks LAN Configuration Files Guides from <http://www.cisco.com/go/sba>, and then import the configurations into your Orion NCM server, following the instructions in the Importing Configuration Files section of the NCM Administrator Guide here: <http://www.solarwinds.com/support/orionNCM/docs/orionNCMAdministratorGuide.pdf>

Step 3: Open the Orion Network Configuration manager application.

Step 4: Select the node in the node list to which you want to import a configuration file.

Step 5: Open the Windows Explorer file browser and browse to the folder containing your configuration file.

Step 6: Drag the file from Windows Explorer to the Orion Network Configuration Manager node list.

Step 7: Type a name for the configuration file, and then click **OK**.

Step 8: Select each imported config on the device navigation tree on the left, and then select the **Configs/Set/Clear** baseline Settings.

Step 9: Right-click and select **Download Configs**.

Step 10: Add all devices you wish to compare against baseline configs you set above, and then click **Download**. This downloads the running configuration into Orion NCM for comparison.

Step 11: Navigate to **Configs > Config Change Report**, and then run the **Config Change Report**. This compares each selected device against their imported Cisco baseline configs.

Step 12: Select your devices and **Compare most recent Download to the last Baseline Config**, and then click **Generate Report**.

BEFORE		AFTER	
service timestamps debug datetime msec		service timestamps debug uptime	
service timestamps log datetime msec		service timestamps log datetime localtime	
hostname EW-3750B		hostname EW-3750A	
		mls qos	
energywise domain Cisco secret 0 cisco_		energywise domain SolarWinds secret 0 test	
energywise importance 80		energywise importance 100	
energywise level 9		energywise name SolarWinds	
energywise name test_for_chris		energywise role Test	
energywise role WS-C3750-24P		energywise keywords test,test2,test3	
energywise keywords keyword,keyword1,ke			
Interface : FastEthernet1/0/1			
energywise level 6 recurrence importan			
energywise level 8 recurrence importan			
energywise level 1			
energywise importance 99			
energywise role tebut			
energywise keywords key,key			
Interface : FastEthernet1/0/2			
energywise level 10 recurrence importa			
energywise level 3 recurrence importan			

Step 13: If you see discrepancies that need to be resolved, you may right-click anywhere in the configuration and select **Edit Config** to see the full configuration. From there you can make any changes necessary and upload to the devices.

Process

Baselining the Network and Start Monitoring (Day 1)

1. Back up all of your network devices
2. Enable config change reporting
3. Configure fault and performance alerts
4. Configure custom monitoring
5. Create network maps
6. Customize your dashboard (optional)

After you have completed the setup steps from any of the associated modules, use Orion to quickly baseline your network configuration and start monitoring performance. Baselining the network provides you with an automated way to validate this network against recommended settings in Cisco SBA guides in the future.

Procedure 1 Back up all of your network devices

Step 1: Navigate to **All Programs > SolarWinds Orion Network Configuration Manager > Orion Network Configuration Manager**, and then log in to the Orion NCM client application.

Step 2: Select **Schedule > Display/Edit Jobs**.

Step 3: Right-click the default Nightly Config Backup job, select **Test Job**, and then click **Start**. This downloads the configurations.

Step 4: If there are any devices with backups that were unsuccessful, edit each failing device and validate your login credentials. After you have verified that the job completes for all devices, you may perform ad-hoc backups as necessary through the Orion Web Console.



Reader Tip

For additional information about the Orion product family, or to connect with the SolarWinds Thwack community of over 50,000 network professionals, visit <http://www.thwack.com>

Procedure 2

Enable config change reporting

Step 1: Log in to the Orion NCM client application.

Step 2: Navigate to **Schedule > Display/Edit Jobs**.

Step 3: On the Edit Nightly Config Backup Job page, on the Download Config tab, under the Changed Configs section, select **Last Config** and **Send config change notification details in a separate HTML email**.

The screenshot shows the 'Edit Nightly Config Backup' dialog box with the 'Download Config' tab selected. The 'Download Options' section has 'Config Types' set to 'Running'. The 'Changed Configs' section has 'Last Config' selected, and 'Send config change notification details in a separate HTML email' is checked. The 'Only save Configs that have changed' option is also checked. The 'Edit Comparison Criteria' button is visible.

Step 4: On the Notifications tab, select **E-mail results**, and then enter the appropriate information in the **Email To**, **Email From**, and **SMTP Server** sections.

The screenshot shows the 'Edit Nightly Config Backup' dialog box with the 'Notifications' tab selected. The 'E-Mail Results' checkbox is checked. The 'Email Settings' section is expanded, showing the 'Email To', 'Email From', and 'SMTP Server' fields. The 'Subject' field is filled with 'SolarWinds, Inc. Configuration Management Job Completion Notification'. The 'Attach copy of Report in PDF format' checkbox is unchecked. The 'Only E-Mail results if this Job encounters an error during execution' checkbox is also unchecked.

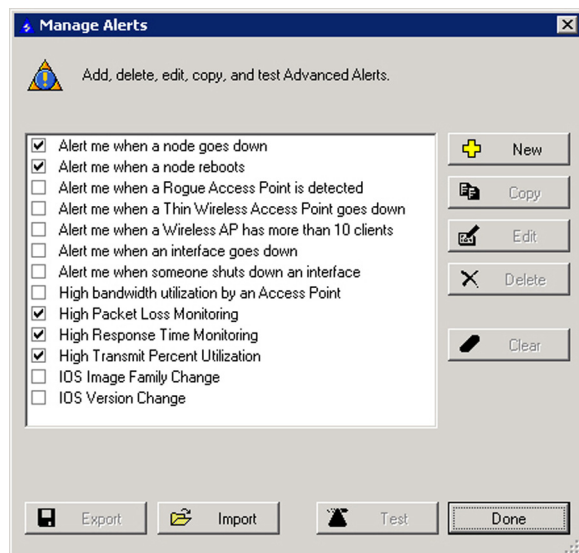
Step 5: Click OK.

Procedure 3 Configure fault and performance alerts

By default, Orion provides a number of advanced alerts that are configured at install. If, when you first log on to the Orion Web Console, there are any devices on your network that trigger any of these alerts, the Active Alerts resource on the Network Summary Home view displays the triggered alerts with a brief description.

Step 1: Navigate to **All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager**, and then click **Configure Alerts**. This allows you to view the configured alerts.

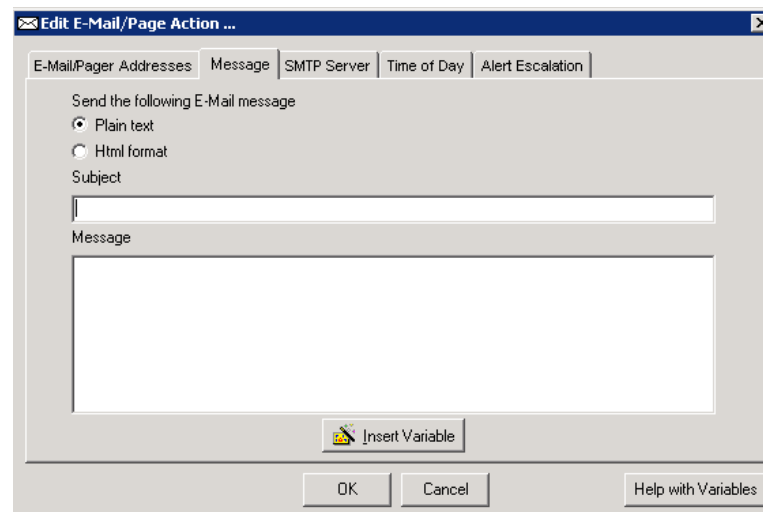
Step 2: If you are implementing Cisco SBA Wireless LAN Deployment Guide, check the boxes next to the wireless alerts as appropriate. Note, several alerts are enabled by default. Check additional alerts as necessary, or create new ones.



Step 3: Add an email notification action to the desired alerts by editing the alert and selecting the **Trigger Actions** tab.

Step 4: Click **Add New Action**, and then, in the list of alert actions, select **Send an Email/Page**.

Step 5: Click **OK**.



You may also use alert variables within the messages that are parsed dynamically when an alert is triggered or reset. For example, the variable `${AvgResponseTime}` parses to the average response time of the node that is triggering the alert.



Tech Tip

For detailed information about alert variables, configuring sustained state trigger and reset conditions, multiple condition matching, and automatic alert escalation, see the online help section here: <http://www.solarwinds.com/NetPerfMon/SolarWinds/wwhelp/wwhimpl/js/html/wwhelp.htm#href=OrionAGManagingAlertsAdvanced.htm>

Procedure 4 Configure custom monitoring

Optional

While Orion NPM comprehensively monitors a broad set of device statistics and data out-of-the-box, there may be cases where additional monitoring of certain device attributes may be desirable.

You can quickly configure a Universal Device Poller (UnDP) to support these custom situations, or a UnDP may have already been created for the information you're looking for by the extensive SolarWinds user community. UnDPs and other community shared content are available in the Content Exchange area on the SolarWinds thwack community site here: http://thwack.solarwinds.com/community/content-exchange_tht

As an example, download an UnDP to monitor licensing status on the ISR G2 here: <http://solarwinds.hosted.jivesoftware.com/docs/DOC-92118>

Procedure 5 Create network maps

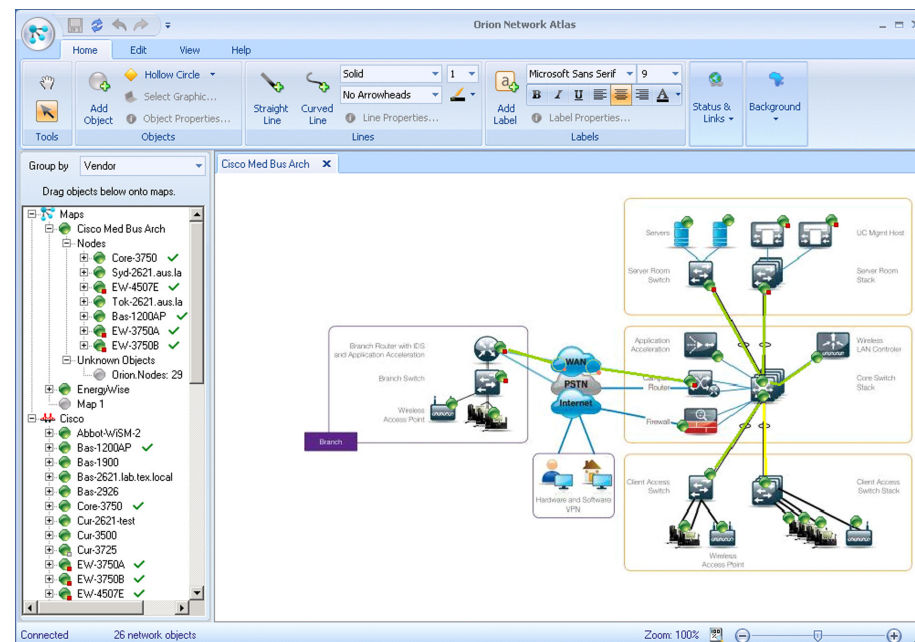
Optional

Orion Network Atlas lets you create custom maps and network diagrams, which can then be made visible in the Orion Web Console. You can use Network Atlas to document the network deployment and print and export the diagram so that you can refer to it later should you need it.

Step 1: Navigate to **All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Orion Network Atlas**.

Step 2: Create a basic map by selecting a background image, dragging nodes to the image, and connecting them with lines. You may assign a status to each line to reflect the actual status of each link.

You can also use the ConnectNow™ feature in Network Atlas to automatically draw links between directly connected nodes discovered on your network. More information on ConnectNow can be found in the Orion Network Atlas Administrator Guide here: <http://www.solarwinds.com/support/orion/docs/OrionNetworkAtlasAdminGuide.pdf>



Tech Tip

For examples of network maps with drill-down and Orion View customizations, watch the Orion online demo here: <http://oriondemo.solarwinds.com>

Procedure 6 Customize your dashboard (optional)

Views in the Orion Web Console are configurable presentations of network information. A view can include maps, charts, summary lists, reports, events, and links to other resources. Views can be assigned to menu bars and each view can be customized. You may also select the charts and device properties that are displayed on each view.

Step 1: Edit a view from within the Orion Web Console by clicking **Customize Page** in the upper right corner when viewing a page you would like to customize.

Process

Optimizing and Maintaining Network Health (Day 2+)

1. Run historical performance reports
2. Analyze future trends
3. Run policy compliance reports (optional)

Use Orion reporting to determine if there are opportunities for performance optimization and if there are any capacity or security issues that need to be resolved.

Procedure 1 Run historical performance reports

Step 1: Log in to the Orion Web Console, and then, on the menu bar, click **Reports**. This allows you to access the list of built-in reports.

Step 2: Review the following reports to determine if there are any anomalies worth exploring:

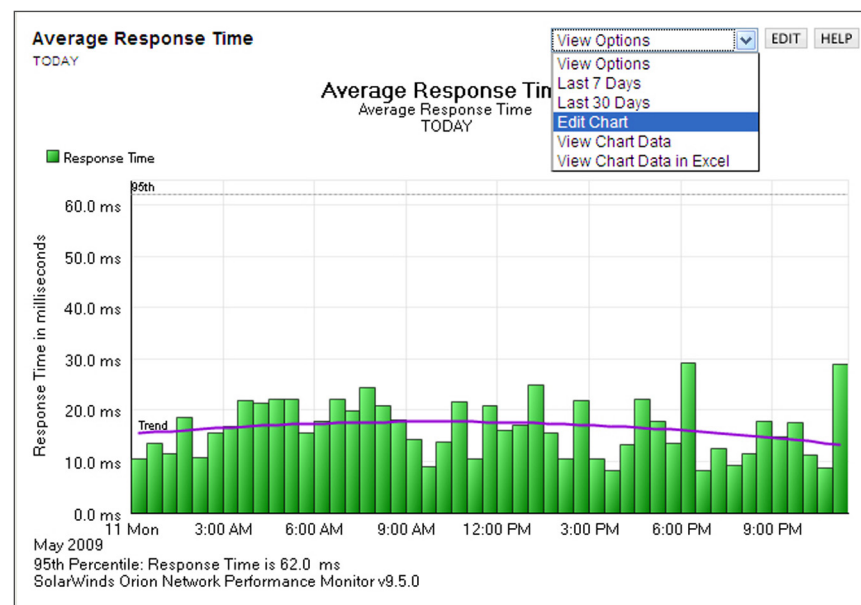
- **Node Reports > Events > Triggered Alerts—Last 30 Days**—This report displays a list of all triggered alerts over the last 30 days. For each triggered alert event, this report displays the date and time of the alert trigger, the node that triggered the alert, and a message describing the triggered alert event.

- **NPM Reports > Historical Cisco Buffer Miss Reports > Cisco Buffer Misses—Last 7 Days**—This report displays all buffer misses (small, medium, big, large, and huge) on monitored Cisco devices over the last 7 days.
- **NPM Reports > Historical Traffic Reports > Average and Peak Traffic Rates—Last 7 Days**—This report displays the average and peak response times for the top ten monitored nodes over the last 7 days.
- **NPM Reports > Historical Traffic Reports > 95th Percentile Traffic Rate—Last 7 Days**—This report displays the 95th percentile traffic rates (receive, transmit, and maximum) for all monitored interfaces over the last 7 days.

Procedure 2 Analyze future trends

Orion includes trend lines on charts to help with analyzing future requirements on network devices.

Step 1: Select **Edit** in the drop-down of any chart and customize the chart to a future timeframe. This leverages trend lines.





Tech Tip

You can modify reports to suit your specific requirements. For more information about using Orion Report Writer, see Understanding Orion Report Writer here: <http://www.solarwinds.com/support/Orion/docs/UnderstandingOrionReportWriter.pdf>

Procedure 3 Run policy compliance reports (optional)

Orion NCM includes policy reporting which allows you to scan configuration files and report any discovered rule violations. For example, a rule may dictate that configurations should not include the read-only community string, "public."

Step 1: On the Configs tab, navigate to the Compliance view, and then select, update, and view the desired report. This allows you to access the built-in policy reports from the Orion Web Console.

Step 2: You can create new policy reports, policies, and rules, by navigating to All Programs > SolarWinds Orion Network Configuration Manager > Orion NCM Policy Reporter. This opens the Orion NCM Policy Reporter application.

Edit Rule...

Orion Network Configuration Manager Rules define the search pattern used to search device configs. Patterns can be a RegEx Expression, or a simple find expression using '*' and '?'. The error level defines how the violation will be noted on the Policy Report if the search criteria is found.

Name: Disable Reverse-Telnet

Comment: Prevents anyone initiating a reverse-telnet session

Pattern: line con 0:.*\n{.*}\n.*transport input none

[More Information about RegEx Patterns...](#)

Pattern Type: ☒ RegEx Expression ☐ Find String

Rule is violated if pattern is: ☐ Found ☒ Not Found

Error Level: ☐ Informational ☐ Warning ☒ Critical

Grouping: Cisco Console Settings

A Rule may test for the line to be found, such as an access list, or to be not found, such as 'public' for a community string. If the condition is not met, the policy will be marked with the error level set for this policy, and the error message will be shown in the Policy Report.

OK Cancel



Tech Tip

If you used the 30-day trial versions of the Orion products (http://www.solarwinds.com/register/registration.aspx?program=901&c=70150000000EmKh&CMP=BIZ-CSCO-NMA-NPM_NCM-DL) for setting up your network, be sure to convert them to a full license before the end of the 30-day evaluation period. All settings are maintained in the conversion from the 30-day trial to the full license.

Appendix A: Network Details

Network Device Connectivity	
Login username =	
Login password =	
Enable password =	
Community string =	
Orion Login Credentials	
NCM Administrator password =	
NPM Administrator password =	

Appendix B: SolarWinds Contact Information

End Users

- Please contact sales@solarwinds.com with any questions.
- Submit an Inquiry about SolarWinds and the Cisco SBA initiative

Resellers

- Please contact reseller@solarwinds.com with any questions.
- For more information about how to become a SolarWinds reseller, please visit the Partner Section of our website.

For more information about the SolarWinds and Cisco Partnership, please visit the Cisco Resource Center.

Notes

Feedback

Please use the [feedback form](#) to send comments and suggestions about this guide.



SMART BUSINESS ARCHITECTURE



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2013 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)