



SolarWinds Network Management Guide



● ● ● SBA FOR GOVERNMENT

Revision: H2CY10

The Purpose of This Guide

In keeping with the blueprint theme of the Cisco Smart Business Architecture (SBA) for Government Large Agencies, 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.

This guide organizes the various tasks by Day 0, Day 1, and Day 2+ to help clarify the recommended timing of tasks when using the SolarWinds Orion products in conjunction with the configuration modules in the *Cisco SBA for Large Agencies—Borderless Networks LAN Deployment Guide* and *WAN Deployment Guide*.

Related Documents

Before reading this guide

- BN Design Overview
- BN LAN Deployment Guide
- BN LAN Configuration Guide
- BN WAN Deployment Guide
- BN WAN Configuration Guide

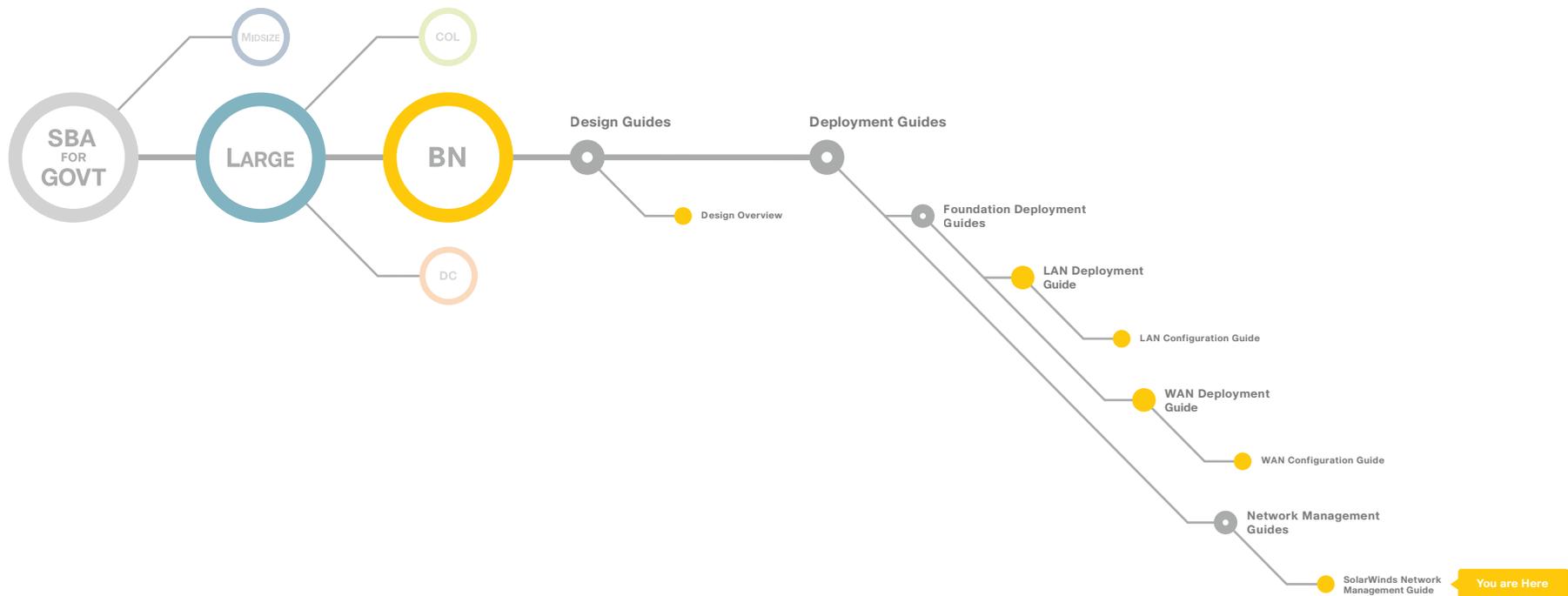


Table of Contents

Introduction	1	Day 0: Setup Network Management System	4
Technology Overview	2	Day 0: Assess and Configure Network Devices	6
Prerequisites	2	Day 1: Baseline the Network and Start Monitoring	8
Using Orion for Day 1 through Day 2+ Tasks	2	Day 2+: Optimize and Maintain Network Health	11
Day 0 Setup Network Management System/Assess and Configure Network Devices	2	How to Contact Us	13
Day 1 Baseline the Network & Start Monitoring	2	End Users	13
Day 2+ Optimize & Maintain the Health of the Network	2	Resellers	13
Architectural Overview	3	Appendix A: SBA for Large Agencies Document System	14

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 NON-INFRINGEMENT 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. Cisco Unified Communications SRND (Based on Cisco Unified Communications Manager 7.x)

© 2010 Cisco Systems, Inc. All rights reserved.

Introduction

The SBA for Large Agencies offers partners and customers valuable and easy to use network design and deployment best practices. It is designed for networks that have 2000 to 10,000 connected users and is a prescriptive, out-of-the-box deployment guide that is based on best-practice design principles and that delivers flexibility and scalability. The deployment guides are designed to make the Borderless Network for Large Agencies easy—easy to configure, easy to deploy, and easy to manage. Partners can use this architecture to grow a profitable Cisco practice and deliver a superior end-user experience that includes switching, routing, wireless, WAN optimization, and security technologies, combined with comprehensive management capabilities for the entire system. Customers can use the guidance provided in the architecture and deployment guides to maximize their Cisco network's value in a simple, fast, affordable, scalable and flexible manner.

The SBA for Large Agencies includes three primary Cisco deployment guides, one each for Local Area Network (LAN), Wide Area Network (WAN), and Internet Edge. The modular design of the architecture means that technologies can be added when the agency is ready to deploy them. It also provides Cisco-tested configurations and topologies which CCNA-level engineers can use for design and installation, and to support agency needs.

Cisco offers a number of options to provide Network Management capabilities for the SBA for Large Agencies. 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 and change management.

Notes

Technology Overview

Deploying the configuration modules outlined in the *Cisco SBA for Large Agencies* 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 the SBA for Large Agencies, 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 for Large Agencies* guides.

This Network Management Deployment Guide is comprised of two SolarWinds Orion products: Orion Network Configuration Manager (NCM) for managing and monitoring network configuration changes and Orion Network Performance Monitor (NPM) for quickly detecting, diagnosing, and resolving network performance problems and outages. You can download a free trial of NPM and NCM from http://www.solarwinds.com/Cisco_Orion.

Prerequisites

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. Prior to continuing with this module, please ensure you follow the steps outlined in the Cisco SBA guides to setup IP addresses and configure these standard management protocols for each device you want to manage.

Using Orion for Day 1 through Day 2+ Tasks

This module organizes the various tasks by Day 0, Day 1, and Day 2+ to help clarify the recommended timing of tasks when using the Orion products in conjunction with the configuration modules in this guide. The actual setup of the Orion products should take less than an hour.

Day 0 Setup Network Management System/Assess and Configure Network Devices

The Day 0 section will guide you through the initial setup of the Orion network management system and how to use the system to assess and manage the device configurations of your Cisco SBA network. It is recommended that you perform the steps in this section immediately following the Configuration Procedure Details section in the Cisco SBA guides so that you may 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 & Start Monitoring

The Day 1 section will guide you through the steps necessary to baseline the network and start monitoring. Perform this section immediately following the deployment of all required modules so that you may backup your configurations and gain visibility into any problems affecting network performance.

Day 2+ Optimize & Maintain the Health of the Network

The final Day 2+ section will guide you through the steps necessary to optimize and maintain the health of your network. The section can be performed at any time, but is recommended to be performed immediately after the Day 1 section tasks to allow you to determine if there are opportunities for performance optimization and if there are any capacity issues that need to be resolved.

Day 0: Setup Network Management System

Orion requires a Windows Server with the following specifications:

Hardware

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

Software

- Windows 2003 Server (32-bit or 64-bit) including R2, with IIS 6.0 or later installed, running in 32 bit mode
- Windows 2008 Server (32-bit or 64-bit) with IIS 6.0 or later installed, running in 32 bit mode
- .NET Framework Version 3.5 or later
- Microsoft SNMP Trap Services

Database

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

During the installation of Orion you will be asked for a several pieces of data that you may want to record here for future reference:

Network Device Connectivity

- Login username =
- Login password =
- Enable password =
- Community string =

Orion Login Credentials

- NCM Administrator password =
- NPM Administrator password =

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.

Installation and configuration of Orion NPM and NCM should take less than an hour by following the three steps outlined below.

Step 1: Install the Orion NPM Server and Website

Login onto the Windows server using an account with Administrator privileges.

Run the Orion NPM executable and select the Express installation option. This will automatically install Orion NPM and configure a SQL 2005 Express database server for monitoring data storage.

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

Login using Admin and blank password (you may change this later) and follow the steps in the automated discovery wizard to import your devices.

Step 2: Install the Orion NCM Server and Client application

Run the NCM 'server' executable on the same server where you installed Orion NPM and when the Configuration Wizard starts up, use the same SQL server as NPM: (local)\SOLARWINDS_ORION. You may leave the default NCM database name (ConfigMgmt) and website settings.

When you reach the System Default Settings portion of the wizard, 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 will be used by NCM to connect to your devices and perform the initial device inventory and configuration backups.

When you reach the Import Devices section of the wizard, uncheck Populate Node List with Devices option and click Next. The next screen will allow you to quickly import nodes you previously discovered in Orion NPM.

Check the option to enable synchronization of Orion NPM nodes into NCM and specify Windows Authentication for the SQL Server authentication method. Enter (local)\SOLARWINDS_ORION for the database server and enter NetPerfMon for the database name.

Once the Config Wizard has completed, the NCM client application will automatically open. Change your Administrator password and write this down in your setup Notes as you will need this for authentication to NCM from the Orion Web Console.

Step 3: Install the NCM integration module for your Orion Web Console.

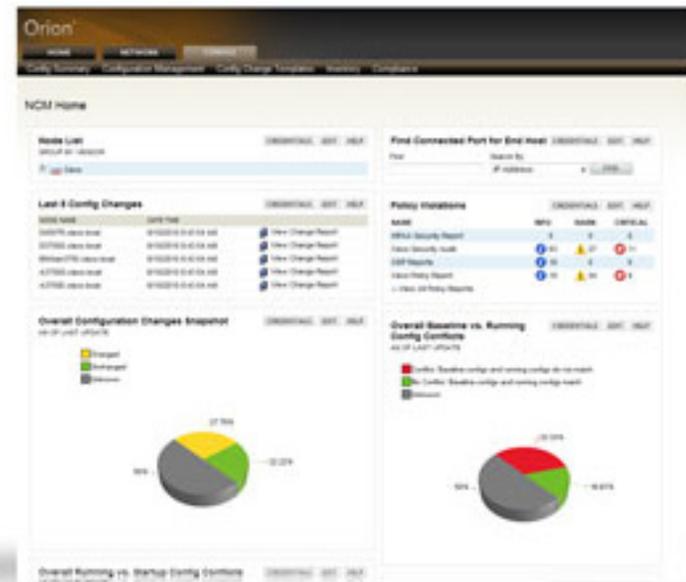
Run the NCM 'NPM Integration' executable on your Orion server. After installation and configuration wizard have completed, login to the Orion Web Console.

Click on Admin link in menu bar and navigate to NCM Settings > Connection Settings and enter the IP address of your NCM server and click Submit.

Click the Network Configuration Manager link in menu bar to navigate to the NCM summary view.

Click Credential on one of the NCM resources and enter your NCM Administrator account credentials (use the built-in Administrator account for now) and click Submit.

The NCM Home view should now be fully functional.



Day 0: Assess and Configure Network Devices

Step 1: Inventory the existing network infrastructure to determine compatibility with this architecture

Login to the NCM client application and select Schedule > Display/Edit Jobs

Right-click on the default Nightly Network Inventory job & select Test Job. Click Start to start process.

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

Once you have verified that the job completes for all devices, click Reports > View Reports and 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.

Step 2: Deploy configuration snippets referenced in the modules to devices.

For this example, we will enable Syslog and Traps on all Cisco Catalyst 3750-X switches you configured in the Access Layer module in the LAN Deployment Guide without having to manually login to each device. Other global config snippets referenced in the guide can be deployed in a similar fashion.

Download the "Cisco 3750 Enable Syslog-Trap" script from the SolarWinds Thwack Content Exchange to your Orion server from <http://thwack.com/media/p/65229.aspx>.

Login to the NCM client application. The NCM client application is available from the Start Menu (All Programs > SolarWinds Orion Network Configuration Manager > Orion Network Configuration Manager)

Right-click in the devices tree & select Execute Script.

Click Load Script to browse and select the Catalyst 3750 script 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
```

Select the Access Layer module 3750-X switches you configured and click Execute Command Script.



Tech Tip

The `${EnterConfigMode}` macro will automatically enter into config t mode for each target device. For a complete list of macros and variables available for use with command line scripting, please consult the Orion NCM Administrator Guide.

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 Cisco SBA Configuration Files Guide and parameterizing them as described in the NCM Administrator Guide.

Step 3: If the agency has existing network infrastructure referenced in this deployment guide, perform the following steps to assess its variance from the Cisco baseline configurations for those device types.

Login to the NCM client application. The NCM client application is available from the Start Menu (All Programs > SolarWinds Orion Network Configuration Manager > Orion Network Configuration Manager)

Download the Cisco SBA Configurations Files Guide from Cisco.com and import the configurations into your Orion NCM server following the instructions in the "Importing Configuration Files" section of NCM Administrator Guide, which is available at: <http://www.solarwinds.com/support/orionNCM/docs/orionNCMAdministratorGuide.pdf>

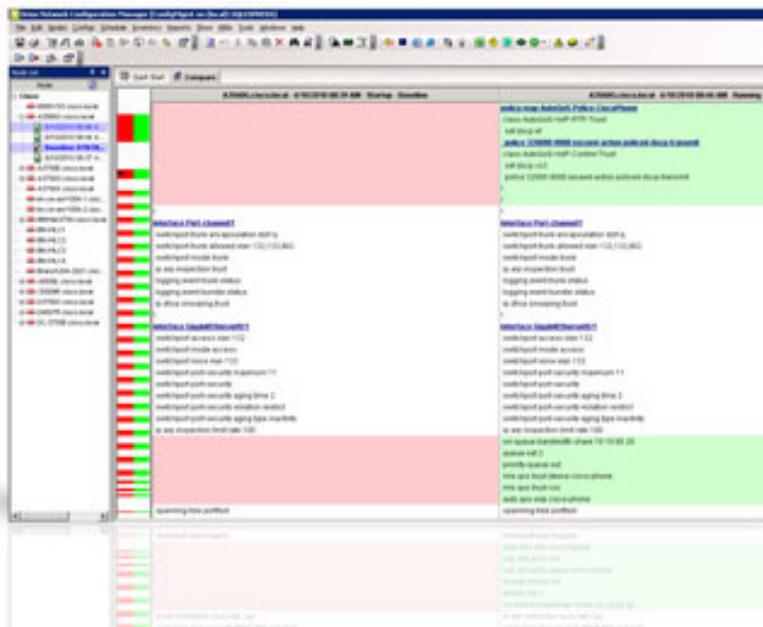
Right-click and select Set Baseline to set each imported config as the baseline configuration within NCM.

Right-click and select Download Configs. Add all devices you wish to compare against baseline configs you set above and click Download to download the running config into NCM for comparison.

Run the Config Change Report to compare each selected device against their imported Cisco baseline configs (Configs > Config Comparison Report)

Select Compare most recent Download to the last Baseline Config and click Generate Report.

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



Notes

Day 1: Baseline the Network and Start Monitoring

Once you have completed the set up steps from any of the associated modules, use Orion to quickly baseline your network configuration and start monitoring performance. Baselineing the network will provide you with an automated way to validate this network against recommended settings in this guide in the future.

Step 1: Back up all your network devices

Login to the NCM client application and select Schedule > Display/Edit Jobs. The NCM client application is available from the Start Menu (All Programs > SolarWinds Orion Network Configuration Manager > Orion Network Configuration Manager)

Right-click the default Nightly Config Backup job and select Test Job. Click Start to start downloading configurations.

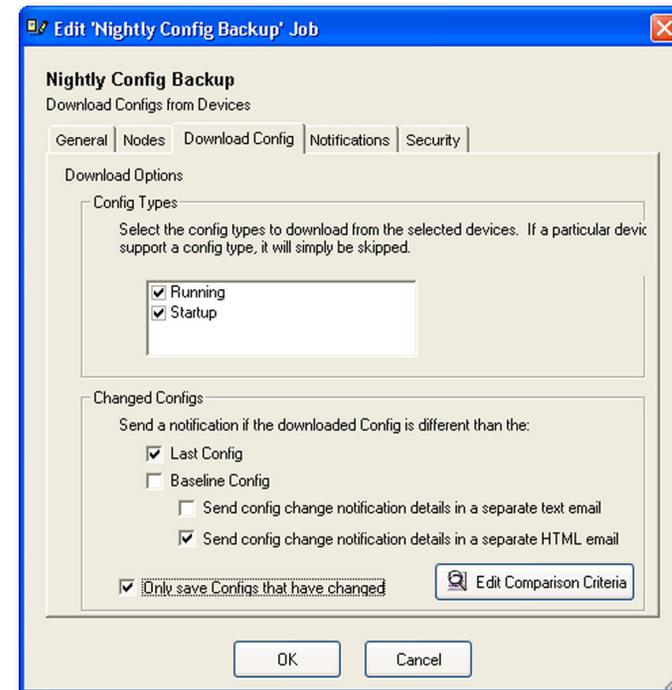
If there are any devices with backups that were unsuccessful, edit each failing device and validate your login credentials. Once you have verified that the job completes for all devices, you may perform ad hoc backups as necessary through the Orion Web Console.

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

Step 2: Enable config change reporting

Login to the NCM client application and select Schedule > Display/Edit Jobs

Edit the default Nightly Config Backup job and navigate to the Download Config tab.



Under Changed Configs section, select checkboxes next to Last Config and Send config change notifications details in a separate HTML email as shown below.

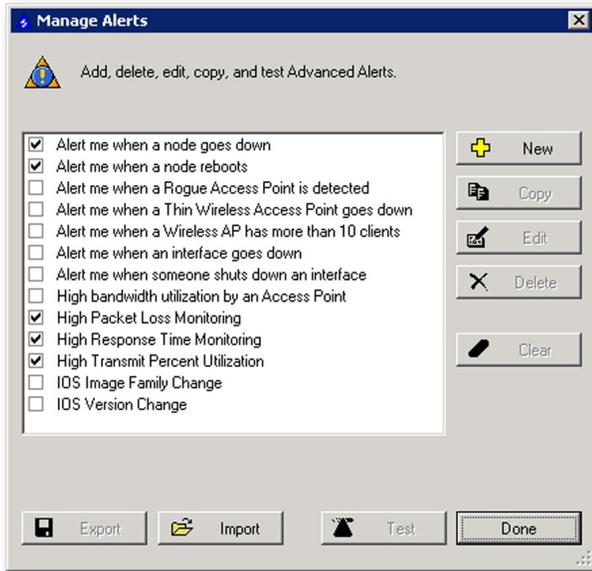
Select Notifications tab and check box next to E-mail results. Enter the appropriate information in the Email To, Email From, and SMTP Server sections.

Step 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.

To view the configured alerts, open the Advanced Alert Manager and click Configure Alerts. The Advanced Alert Manager is available from the Start Menu (All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager)

If you are implementing the Wireless LAN module in the LAN Deployment Guide, check the boxes next to the wireless alerts as appropriate. You will notice that several alerts are already enabled by default. Check additional alerts as necessary or create new ones.



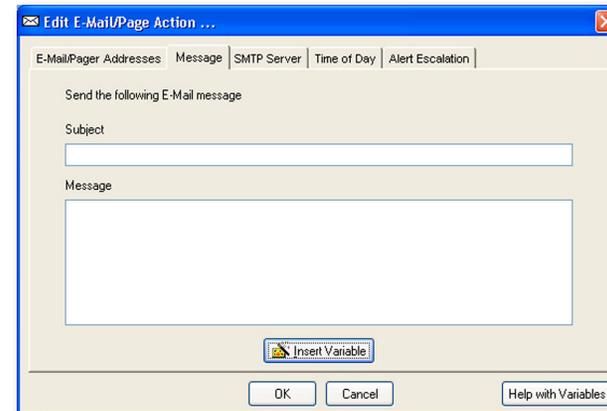
Add an email notification action to the desired alerts by editing the alert and selecting the Trigger Actions tab. Click Add New Action and select Send an Email/Page from the list of alert actions.

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}` will parse 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, please [reference the online help](#).



Step 4: (Optional) Configure custom monitoring using Orion's Universal Device Pollers (UnDPs)

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 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 is available in the Content Exchange area on the Solarwinds thwack_ community site at: <http://thwack.com/media/>

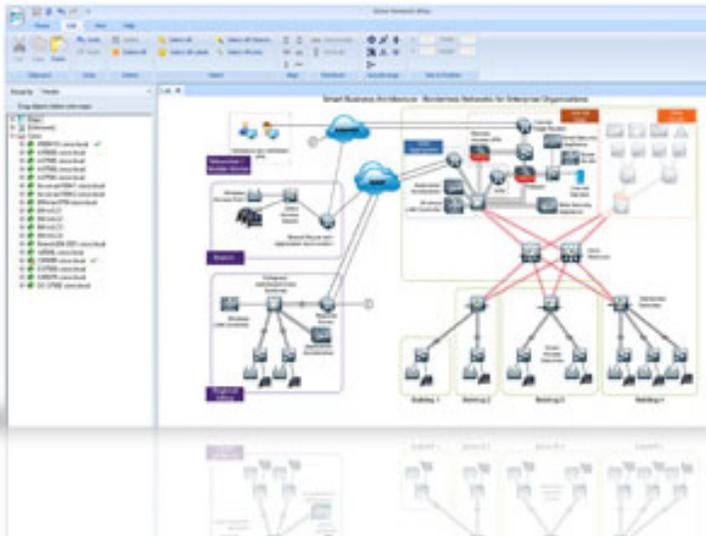
Step 5: Create network maps (optional)

Orion Network Atlas gives you the ability to create custom maps and network diagrams, which can then be made visible in the Orion Web Console.

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.

Network Atlas is available from the Start Menu (All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Network Atlas)

To create a basic map, select a background image, dragging nodes to the image, and connecting them with lines. You may assign status to each line to reflect 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.



Tech Tip

For examples of network map with drill-down and Orion View customizations, check out the Orion online demo:

<http://oriondemo.solarwinds.com>.

Step 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.

To edit a view from within the Orion Web Console, click on the Customize Page link in the upper right hand corner when viewing a page you would like to customize.

Day 2+: Optimize and Maintain Network Health

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.

Step 1: Run historical performance reports

Login to the Orion Web Console and click Reports on the menu bar to access the list of built-in reports.

Review the following reports to determine if there are any anomalies worth exploring.

Events > Triggered Alerts - Last 30 Days

This report displays a list of all triggered alerts over the past 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.

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 past 7 days.

Historical Traffic Reports > Average and Peak Traffic Rates - Last 7 Days

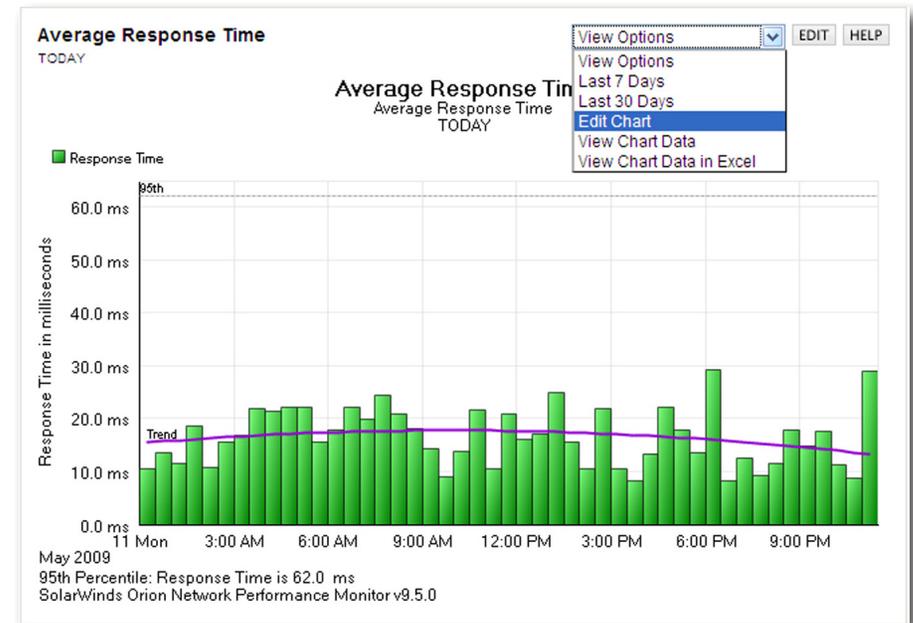
This report displays the avg & peak response times for the top ten monitored nodes over the last month.

Historical Traffic Reports > 95th Percentile Traffic Rate - Last 7 Days

This report displays the 95th percentile traffic rates (receive, transmit, maximum) for all monitored interfaces over the last 7 days.

Step 2: Analyze future trends

Orion includes trend lines on charts to help with analyzing future requirements on network devices. To leverage trend lines, select Edit in the drop-down of any chart and customize the chart to a future timeframe.



Tech Tip

You can modify reports to suit your specific requirements. For more information about using Orion Report Writer, see ["Understanding Orion Report Writer"](#)

Step 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".

To access the built-in policy reports from the Orion Web Console, navigate to the Network Configuration Manager link, click on the Compliance Tab, and run the desired report.

To create new policy reports, policies, and rules, open the Orion NCM Policy Reporter application from the Start Menu (All Programs > SolarWinds Orion Network Configuration Manager > Orion NCM Policy Reporter)

NOTE: If you used the 30-day trial versions of the Orion products for setting up your network, be sure your customer converts them to full license before the end of the 30-day evaluation period. All settings will be maintained in the conversion from the 30-day trial to the full license.

Notes

How to Contact Us

End Users

Please contact sales@solarwinds.com for any questions.

[Submit an Inquiry](#) about SolarWinds and the Cisco Small Business Architecture initiative

Resellers

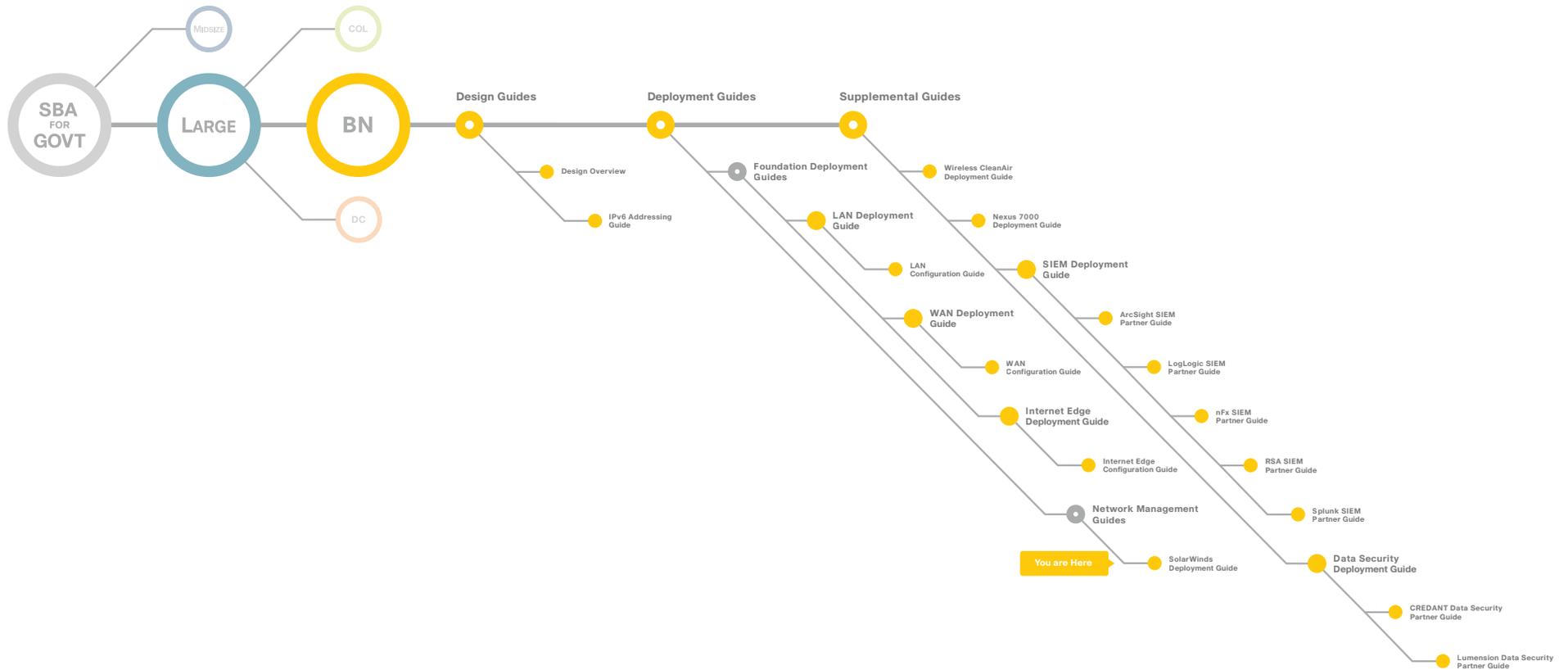
Please contact reseller@solarwinds.com for any questions.

For more information on how to become a SolarWinds reseller, please visit the [Partner Section](#) of our website.

For more information on the SolarWinds and Cisco Partnership, please visit the Cisco [Resource](#) Center.

Notes

Appendix A: SBA for Large Agencies Document System





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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

C07-641101-00 02/11