



SBA
FOR
GOVT

MIDSIZE

BORDERLESS
NETWORKS

SolarWinds Network Management Guide



● ● ● SBA FOR GOVERNMENT

The Purpose of This Guide

In keeping with the blueprint theme of the Cisco Smart Business Architecture (SBA) for Government Midsize 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 *SBA for Midsize Agencies—Borderless Networks Foundation Deployment Guide*.

Related Documents

Before reading this guide

- BN** Foundation Design Overview
- BN** Foundation Deployment Guide
- BN** Foundation Configuration Guide
- DC** Data Center Deployment Guide
- DC** Data Center Configuration Guide

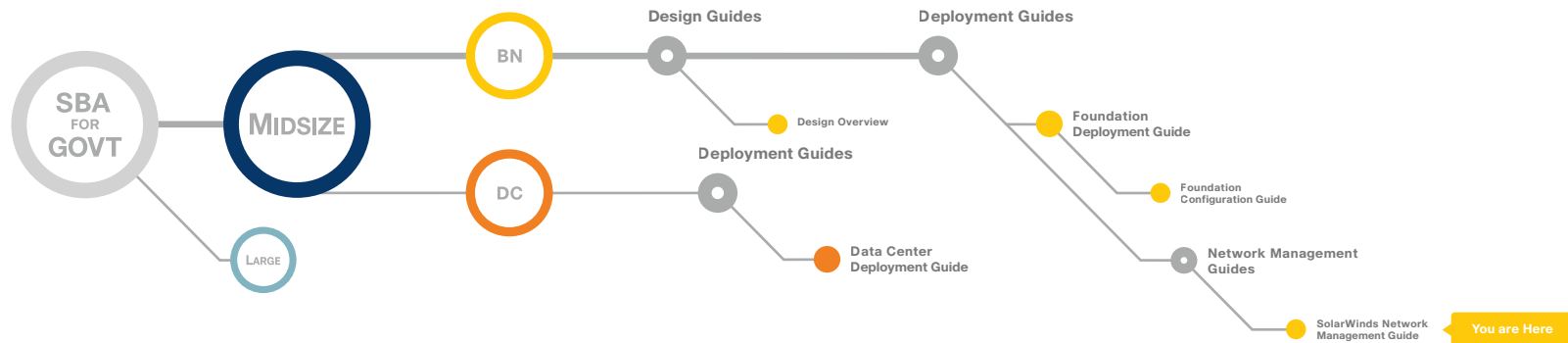


Table of Contents

SBA Overview	1
Guiding Principles	1
Introduction.....	2
Deploying SolarWinds' Orion Network Management Server	4
Day 0: Setup 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	4
Prerequisites	4
Appendix A: Network Details	14
Appendix B: SolarWinds Contact Information	15
Appendix C: SBA for Midsize Agencies Document System.....	16

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

© 2010 Cisco Systems, Inc. All rights reserved.

SBA Overview

The Cisco® SBA is a comprehensive design for networks with up to 1000 users. This out-of-the-box design is simple, fast, affordable, scalable, and flexible.

The Cisco SBA for Midsize Agencies incorporates LAN, WAN, wireless, security, WAN optimization, and unified communication technologies tested together as a solution. This solution-level approach simplifies the system integration normally associated with multiple technologies, allowing you to select the modules that solve your agency's problems rather than worrying about the technical details.

We have designed the Cisco SBA to be easy to configure, deploy, and manage. This architecture:

- Provides a solid network foundation
- Makes deployment fast and easy
- Accelerates ability to easily deploy additional services
- Avoids the need for re-engineering of the core network

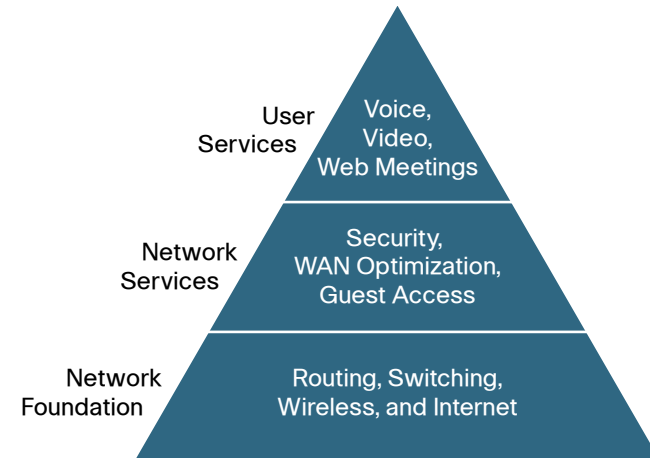
By deploying the Cisco SBA, your agency can gain:

- A standardized design, tested and supported by Cisco
- Optimized architecture for midsize agencies with up to 1000 users and up to 20 remote sites
- Flexible architecture to help ensure easy migration as the agency grows
- Seamless support for quick deployment of wired and wireless network access for data, voice, teleworker, and wireless guest
- Security and high availability for agency information resources, servers, and Internet-facing applications
- Improved WAN performance and cost reduction through the use of WAN optimization
- Simplified deployment and operation by IT workers with CCNA® certification or equivalent experience
- Cisco enterprise-class reliability in products designed for midsize agencies

Guiding Principles

We divided the deployment process into modules according to the following principles:

- **Ease of use:** A top requirement of Cisco SBA was to develop a design that could be deployed with the minimal amount of configuration and day-two management.
- **Cost-effective:** Another critical requirement as we selected products was to meet the budget guidelines for midsize agencies.
- **Flexibility and scalability:** As the agency grows, so too must its infrastructure. Products selected must have the ability to grow or be repurposed within the architecture.
- **Reuse:** We strived, when possible, to reuse the same products throughout the various modules to minimize the number of products required for spares.



The Cisco SBA can be broken down into the following three primary, modular yet interdependent components for the midsize agency.

- **Network Foundation:** A network that supports the architecture
- **Network Services:** Features that operate in the background to improve and enable the user experience without direct user awareness
- **User Services:** Applications with which a user interacts directly

Introduction

Network management systems allow you to automate configuration tasks and monitor network health, giving you the visibility you need to proactively manage your network and quickly troubleshoot issues.

Deploying the configuration modules outlined in the SBA for Midsize Agencies—Borderless Networks Foundation Deployment Guide 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.

Cisco offers a number of options to provide Network Management capabilities. This guide is focused on Cisco's partnership with SolarWinds and their products that meet Cisco's goal to deliver affordable, easy-to-use network configuration and change management.

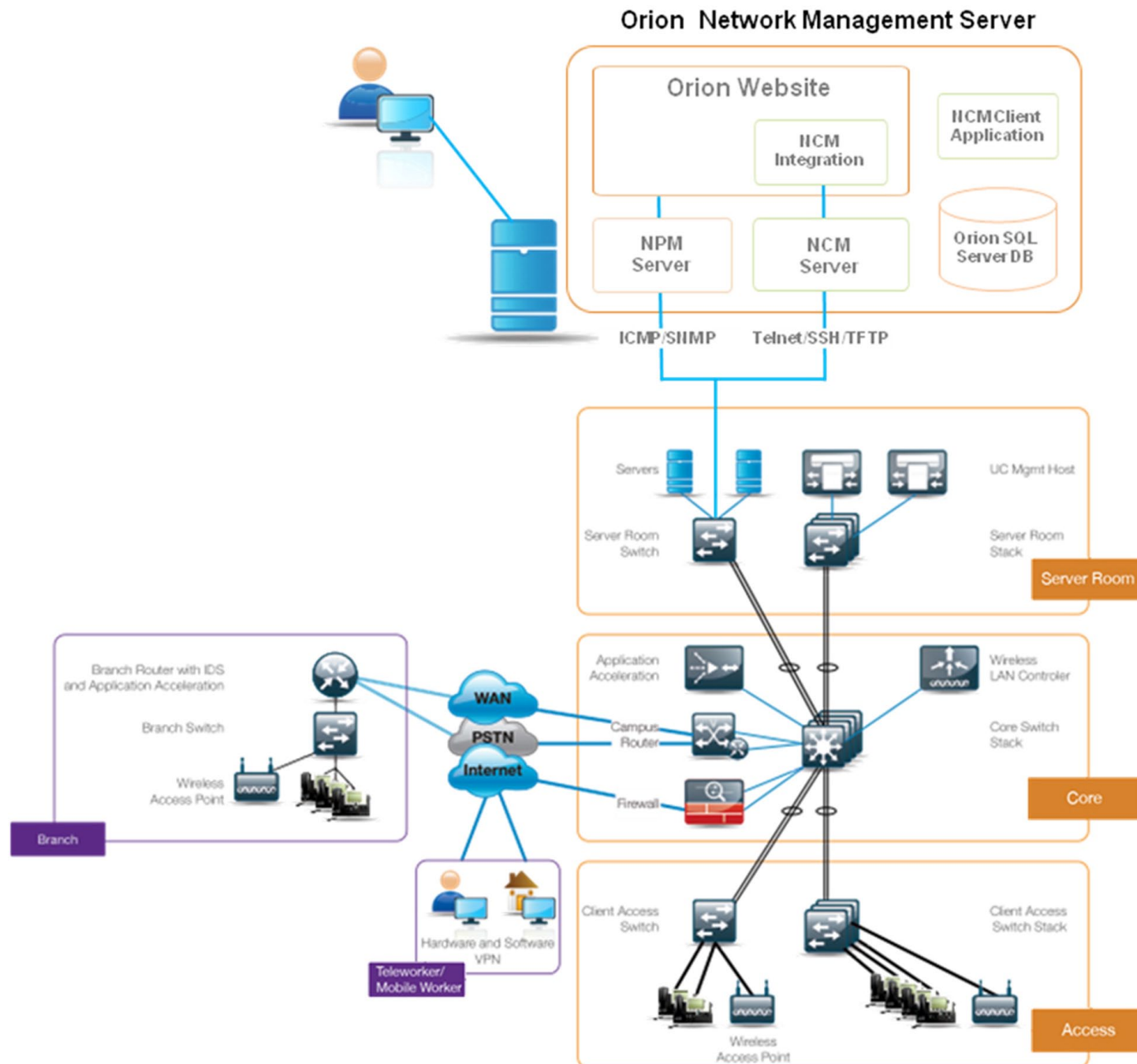
The Orion family of products has been tested and validated with the components described in the SBA for Midsize Agencies—Borderless Networks Foundation Deployment Guide.

The SolarWinds Orion network management products leverage SNMP for gathering availability and performance data and Secure Shell (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 Global Configuration module in the Cisco SBA Foundation Deployment Guide to setup IP addresses and configure these standard management protocols for each device you want to manage.

You can download a free trial of NPM and NCM from http://www.solarwinds.com/Cisco_Orion.

Notes

Figure 1. Architectural Overview



Deploying SolarWinds' Orion Network Management Server

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 SBA network deployment process. 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 for your Cisco SBA network. Perform the steps in this section immediately following the Global Configuration module in the *Cisco SBA for Midsize Agencies—Borderless Networks Foundation Deployment Guide*. This will enable 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.

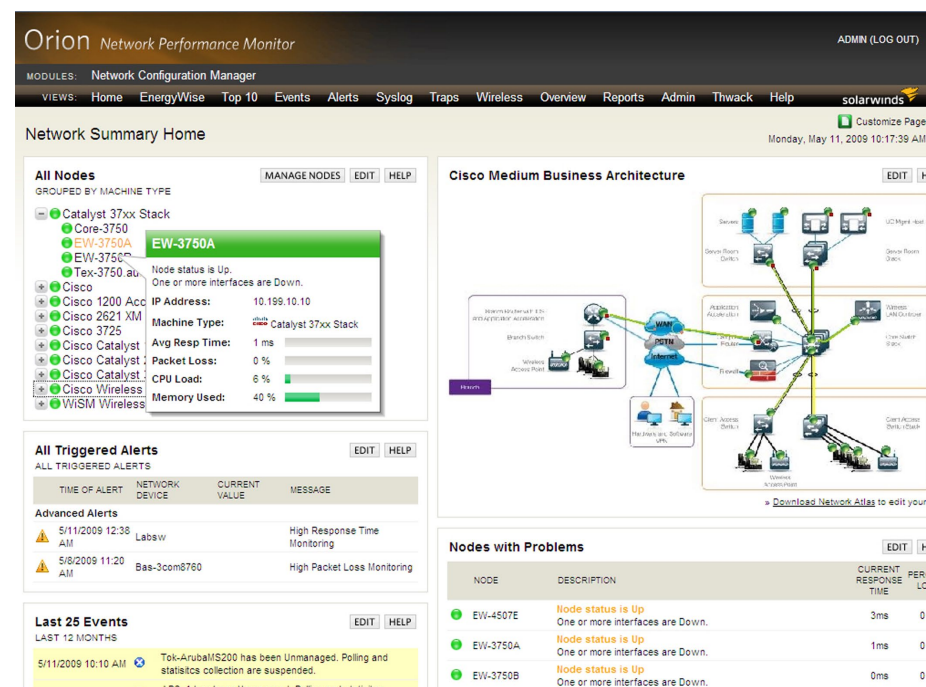
Day 1: Baseline the Network and Start Monitoring

The Day 1 section will guide you through the steps necessary to baseline the network and start monitoring. Perform this section immediately following the deployment of all required SBA modules and components so that you may backup 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 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 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, please ensure that you follow the steps outlined in the Global Configuration module in the *Cisco SBA for Midsize Agencies—BN Foundation Deployment Guide* to set up IP addresses and 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 (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.



Reader Tip

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

Process

Setting Up Network Management System (Day 0)

1. Install Orion NPM
2. Install Orion NCM
3. Install the NCM Integration Module

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 into the Windows server using an account with Administrator privileges.

Step 2: 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.

Step 3: After Orion NPM Configuration Wizard has completed, the Orion Web Console will automatically open in your default browser.

Step 4: Login using Admin and blank password (you may change this later) and follow the steps in the automated discovery wizard to import your devices.

Procedure 2

Install Orion NCM

Step 1: 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.

Step 2: 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.

Step 3: 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.

Step 4: 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.

Step 5: After the Config Wizard has completed, the NCM client application will automatically open. Change your Administrator password and write this down in your setup notes (Appendix A) as you will need this for authentication to NCM from the Orion Web Console.

Procedure 3 Install the NCM Integration Module

Step 1: Run the NCM 'NPM Integration' executable on your Orion server. After the installation and configuration wizard have completed, login to the Orion Web Console.

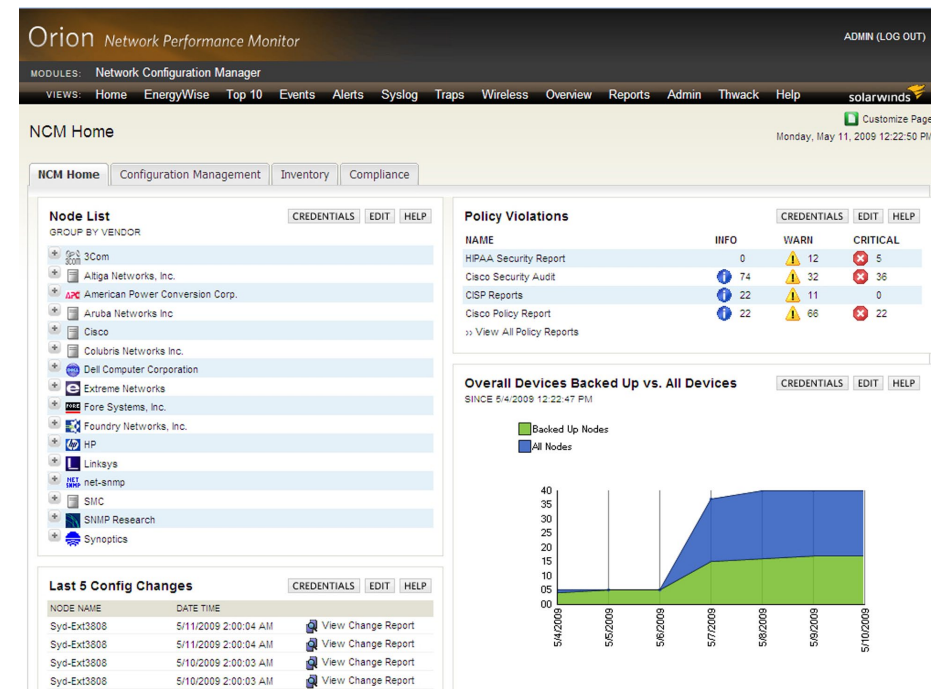
Step 2: Click **Admin** in the menu bar and navigate to **NCM Settings > Connection Settings** and enter the IP address of your NCM server and click **Submit**.

Step 3: Click **Network Configuration Manager** in the menu bar to navigate to the NCM summary view.

Step 4: 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.

Figure 3. NCM Home View



Process

Assessing and Configuring Network Devices (Day 0)

1. Inventory Existing Network Infrastructure
2. Deploy Configuration Snippets
3. Assess Your Variance

Now you'll 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 SBA architecture.

Step 1: Login to the NCM client application and select **Schedule > Display/Edit Jobs**.

Step 2: Right-click on the default Nightly Network Inventory job and select **Test Job**. Click **Start** to the start process.

Step 3: If there are any devices with inventories that were unsuccessful, edit each failing device and validate your SNMP credentials.

Step 4: After 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.

Procedure 2 Deploy Configuration Snippets

For this example, we will enable Syslog and Traps on all Cisco Catalyst 3750 switches you configured in the Campus module of the *Foundation 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.

Step 1: 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>.

Step 2: 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**).

Step 3: Right-click in the devices tree and select **Execute Script**.

Step 4: 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
```

Step 5: Select the Campus module 3750 switches you configured and click **Execute Command Script**.



Tech Tip

The `${EnterConfigMode}` macro will automatically enter into config 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, at <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 Foundation Configuration Files Guide and parameterizing them as described in the NCM Administrator Guide.

Procedure 3 Assess Your Variance

If your agency has existing network infrastructure that is referenced in the *Foundation Deployment Guide*, perform the following steps to assess its variance from the Cisco baseline configurations for those device types.

Step 1: 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**).

Step 2: Download the *Foundation Configuration Files Guides* 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>.

Step 3: Right-click and select **Set Baseline** to set each imported config as the baseline configuration within NCM.

Step 4: 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 configuration into NCM for comparison.

Step 5: Run the Config Change Report to compare each selected device against their imported Cisco baseline configs (**Configs > Config Comparison Report**).

Step 6: Select **Compare most recent Download to the last Baseline Config** and click **Generate Report**.

Figure 4. Config Comparison Report

Config Change Report		Results
Save Results		Actions
EW-3750A		
Today	5/14/2009 02:03 AM	37 adds 161 deletes 27 changes
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 keyword1,keyword1,ke		
Interface : FastEthernet1/0/1		

Step 7: 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

Baseline the Network and Start Monitoring (Day 1)

1. Back Up All Your Network Devices
2. Enable Config Change Reporting
3. Configure Fault and Performance Alerts
4. Configure Custom Monitoring (optional)
5. Create Network Maps (optional)
6. Customize Your Dashboard (optional)

After 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 SBA guides in the future.

Procedure 1 Back Up All Your Network Devices

Step 1: 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).

Step 2: Right-click the default Nightly Config Backup job and select **Test Job**. Click **Start** to start downloading the configurations.

Step 3: 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.



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>.

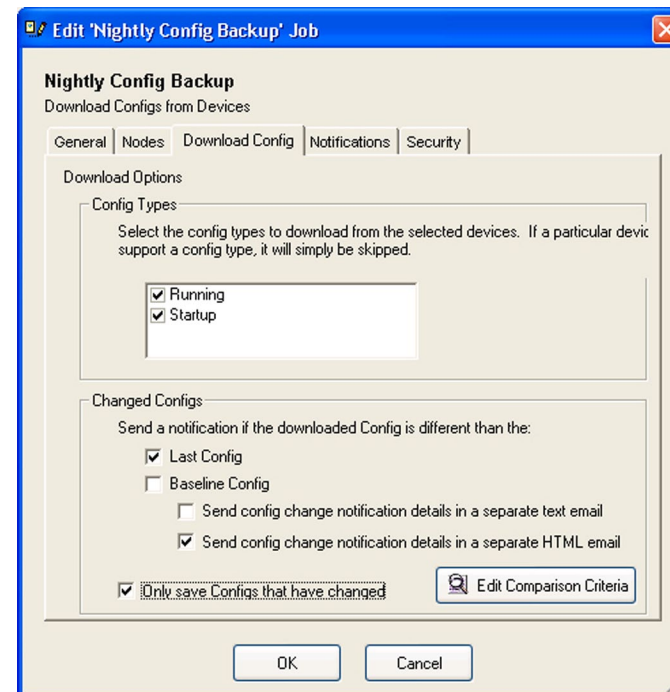
Procedure 2 Enable Config Change Reporting

Step 1: Login to the NCM client application and select **Schedule > Display/Edit Jobs**.

Step 2: Edit the default Nightly Config Backup job and navigate to the **Download Config** tab.

Step 3: Under the Changed Configs section, select checkboxes next to **Last Config** and **Send config change notifications details in a separate HTML email**.

Figure 5. Nightly Config Backup



Step 4: Select the **Notifications** tab and check box next to **E-mail results**. Enter the appropriate information in the **Email To**, **Email From**, and **SMTP Server** sections.

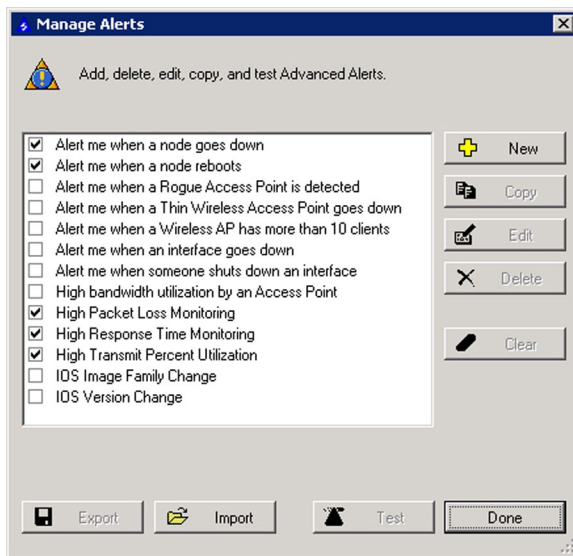
Procedure 3 Configure Fault and Performance Alerts

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: 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).

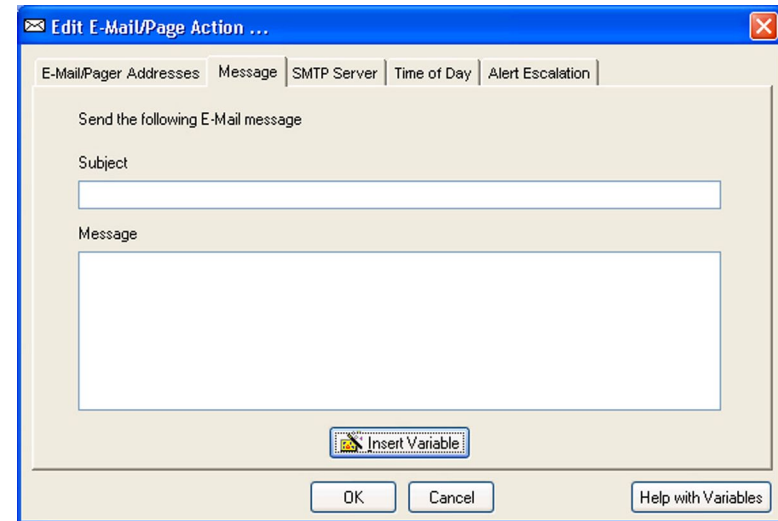
Step 2: If you are implementing the Wireless module in the SBA guide, check the boxes next to the wireless alerts as appropriate. You will notice that several alerts are already enabled by default. Check additional alerts as necessary or create new ones.

Figure 6. Manage Alerts



Step 3: 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.

Figure 7. Edit Email/Page Action



Step 4: 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 at the following location: <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 is available in the Content Exchange area on the SolarWinds thwack community site at <http://thwack.com/media/>.

As an example, download a UnDP to monitor licensing status on the ISR G2 at <http://thwack.com/media/p/82118.aspx>.

Procedure 5 Create Network Maps (optional)

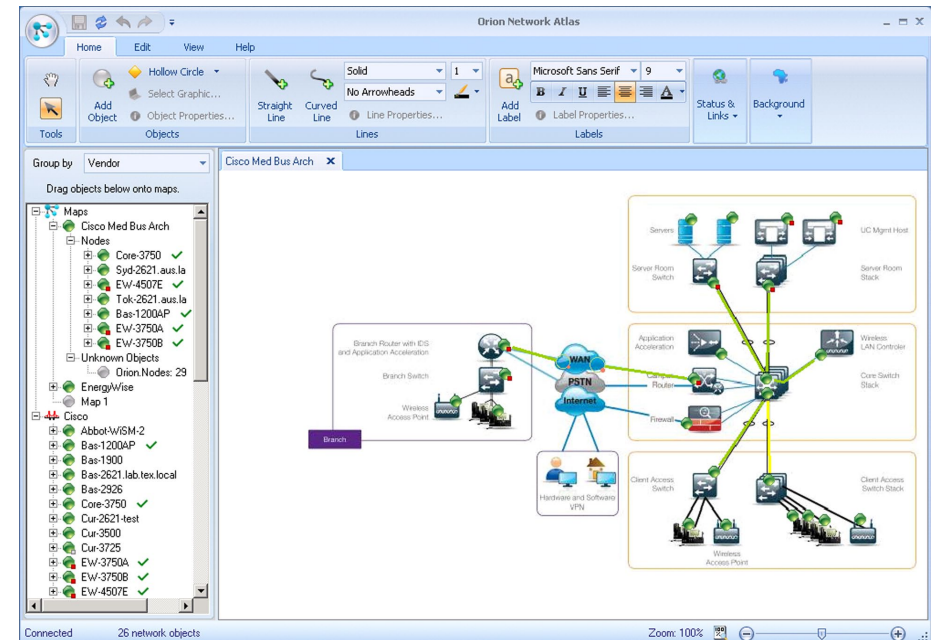
Orion Network Atlas lets you create custom maps and network diagrams, which can then be made visible in the Orion Web Console.

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**).

Step 1: To create a basic map, select 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 at <http://www.solarwinds.com/support/orion/docs/OrionNetworkAtlasAdminGuide.pdf>.

Figure 8. Network Atlas



Tech Tip

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

Procedure 6 Customize Your Dashboard (optional)

Views in the Orion Web Console are configurable pre-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: To edit a view from within the Orion Web Console, click **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 into 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 and 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.

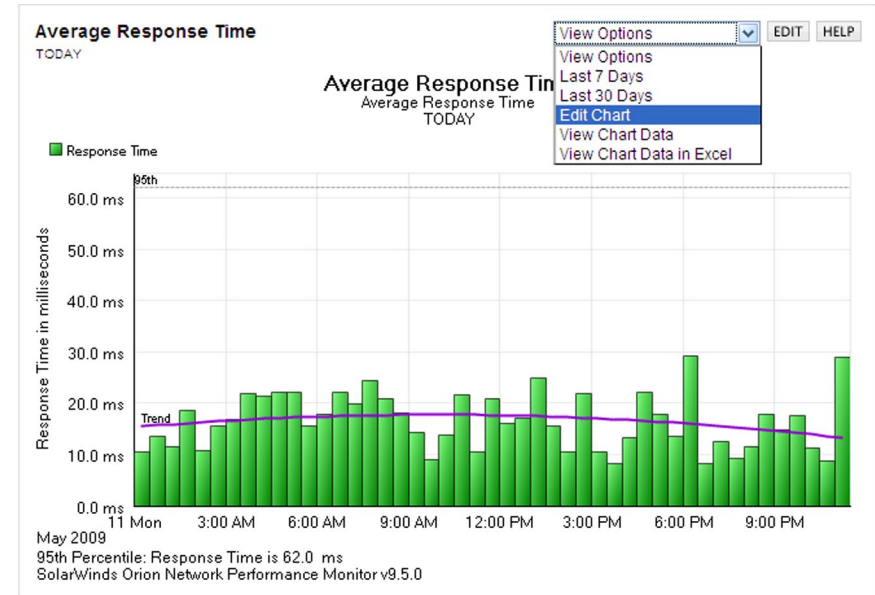
Procedure 2

Analyze Future Trends

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

Step 1: To leverage trend lines, select **Edit** in the drop-down of any chart and customize the chart to a future timeframe.

Figure 9. Average Response Time



Tech Tip

You can modify reports to suit your specific requirements. For more information about using Orion Report Writer, see “Understanding Orion Report Writer” at <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: To access the built-in policy reports from the Orion Web Console, click **Network Configuration Manager**, click **Compliance Tab**, and run the desired report.

Step 2: 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**).

Figure 10. Edit Rule

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:

Comment:

Pattern:

[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:

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.



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 full a 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.

Appendix A: Network Details



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

Notes

Appendix B: SolarWinds Contact Information

End Users

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

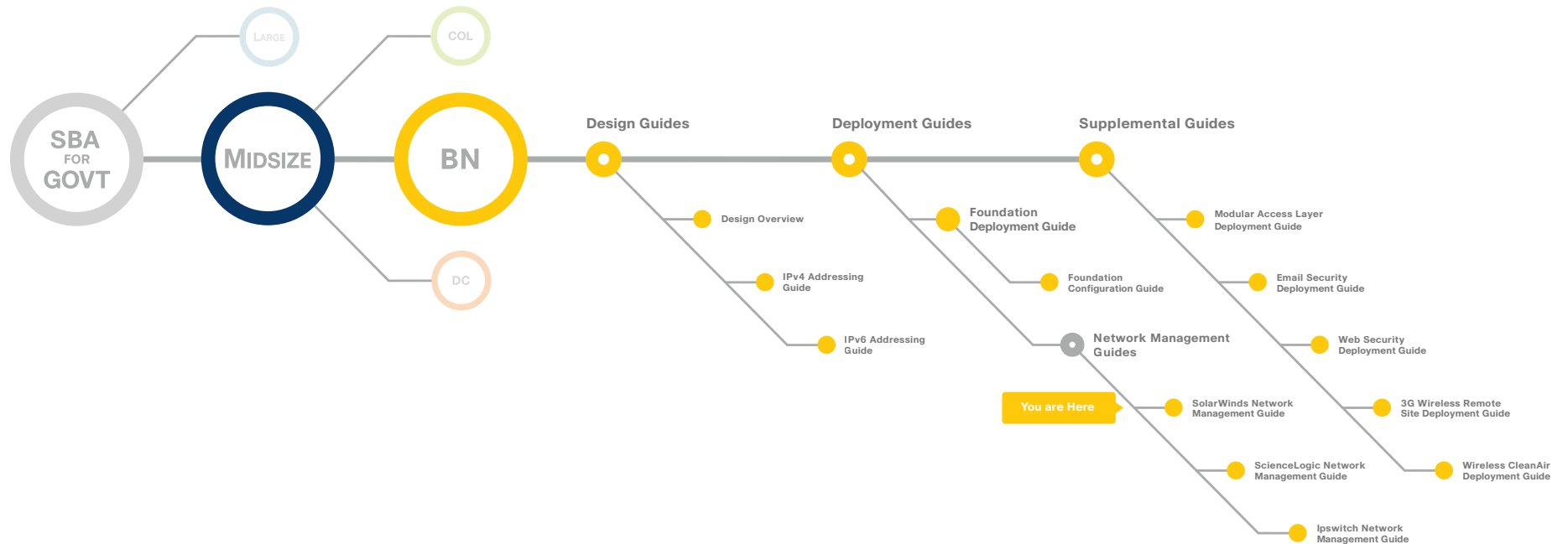
Resellers

- 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 C: SBA for Midsize 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)

C07-641132-00 12/10