HOW-TO GUIDE

INSTALLING AND INTEGRATING NCM

INTRODUCTION

Network Configuration Manager (NCM) delivers powerful automation to help network engineers save time and improve reliability. You can use NCM to:

- Automatically back up and easily restore network configuration files.
- Know when and how a configuration has changed, and who changed it.
- Simplify repetitive and complex configuration changes.
- Approve, schedule, and execute configuration changes.
- Continuously audit configurations to help ensure compliance.

This guide will help you install the evaluation version of NCM, and become familiar with what the tool can do.

Step 1: Install your NCM software

You can install Network Configuration Manager in about 30 minutes. Network Configuration Manager runs on a standard Windows® server (physical or virtual), uses Microsoft® SQL on the back-end, and IIS on the front-end.

Before you start, take a minute to review the most current system requirements. Don't worry if your server does not meet some of the software and version requirements. The install program will automatically detect what software packages are needed and install the necessary components for you.

Launch the install program, and follow the steps in the wizard. In most cases you can accept the default options.

Step 2: Discover your network

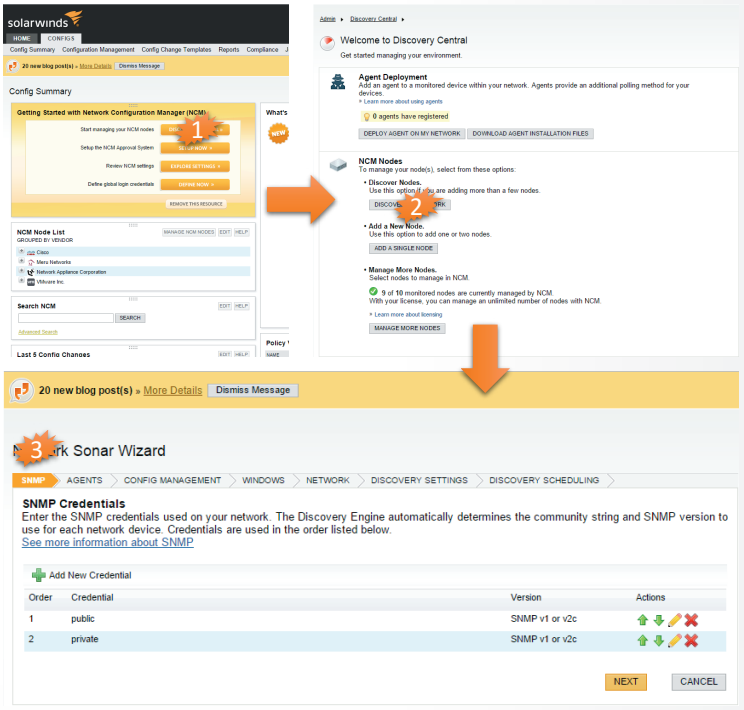
Start your evaluation by discovering the devices you want to monitor. The integrated Network Sonar wizard makes this step quick and easy.

Launch your NCM management console. Look for Getting Started with Network Configuration Manager, and click Discovery Central. Find the section labeled NCM Nodes, and click Discover My Network.

You will be asked to provide information about how to access your SNMP managed devices, what protocols and logon credentials to use to remotely access your devices, and where and how the discovery process should run on your network.

After you have gathered the required information, take a few minutes to work through this wizard.

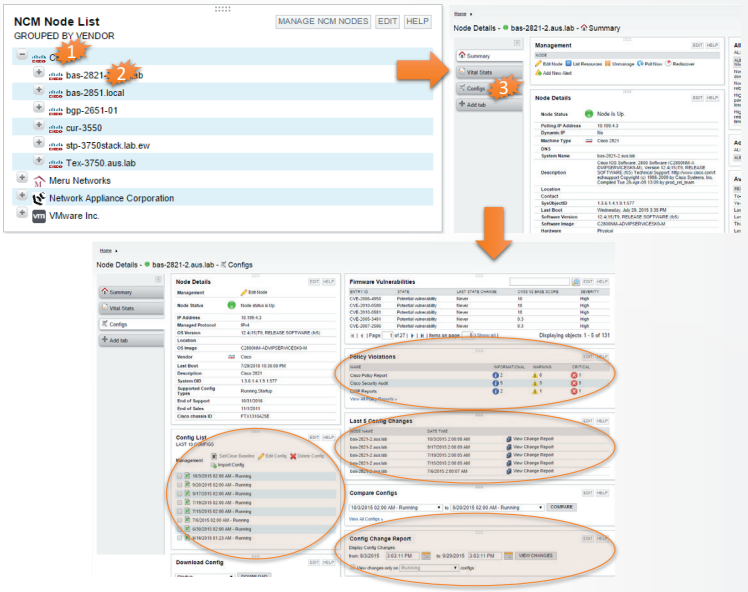
That's all there is to it! After you have completed your initial discovery, NCM automatically organizes and displays your network devices, backs up device configurations, monitors configurations for changes, and more.



Step 3: See how to back up, monitor, and audit device configurations

Configuration mistakes cause most network disruptions. NCM protects configurations using automated backups, change monitoring, and compliance auditing.

In the NCM Config Summary screen, your devices are organized by vendor. To see your devices, expand a vendor heading (click the + sign). To see device details, simply click on a device name. (TIP: Don't click the + sign next to a device name unless you want to see a history of configurations for that device). From the Node Details screen, click the Configs tab, and view the screen.



NCM is already hard at work backing up your device configurations, and will begin to display a running history in the Config List panel. Check back the following morning to see the results.

In addition, NCM is now actively monitoring your configurations for any changes, and will show you summaries in the Last 5 Config Changes panel. Check back the following morning to see the results.

Finally, NCM is also busy analyzing your environment and building audit reports based on best practice security and risk assessment policies. You can view these results in the Policy Violations panel. Check back soon to see these results.

Step 4: See how to manage device configuration changes

It used to take days to make repetitive configuration changes to hundreds of devices. NCM makes these same changes, error-free, in minutes. NCM lets you create, use, and manage configuration change templates that are designed to streamline repetitive and complex configuration changes. Let's see how.

Navigate to the Config Change Templates page using the menu option Config Change Templates. In the list on the left, locate and select the Passwords template. In the display to the right, select Execute Cisco_Password_SNMPv3_Change, and click Define Variables and Run.

NCM allows you to select the specific systems to target for this change. Once you have selected the systems to target, click Next.

NCM collects information for script variables from NCM device profiles and/or by providing a form where values can be manually entered. In this example, all passwords must be manually entered. Fill in the fields, and click Next.

You can preview the change script for any targeted system. Next, either execute the changes, or schedule a job.