VMware Smart Assurance Network Configuration Manager Installation Guide

VMware Smart Assurance 10.1.6

You can find the most up-to-date technical documentation on the VMware by Broadcom website at:

https://docs.vmware.com/

VMware by Broadcom
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

1 Introduction to Network Configuration Manager 11

What is Network Configuration Manager? 11

Where to get help 11

About this manual 12

Product installation directory 12

Deployment architecture 12

Running a software prerequisites check 14

Product and version compatibility 15

Installation tasks 15

Product installation directory 16

Upgrade 16

Upgrade tasks 17

Upgrade tasks for Linux 17

2 Installation procedures (Linux platform) 18

Prerequisites and installation order 18

Prerequisites 18

Order of installation 19

Install Network Configuration Manager using graphical installer mode 19

Install a Database server by using graphical installer 20

Install Combination or Application server using graphical installer 21

Lockbox utility 25

Add distributed system hosts for remote servers (standard or advanced security) 25

Import Network Configuration Manager Certificates for remote servers 26

Export and import certificates for EDAA and Smarts Adapter 27

Install a Device server using graphical installer 28

Install Network Configuration Manager using console installer 30

Install Combination, Application, and Database server using console installer 31

Lockbox utility 35

Add distributed system hosts for remote servers (standard or advanced security) 35

Import Network Configuration Manager Certificates for remote servers 36

Export and import certificates for EDAA and Smarts Adapter 36

Install a Device server using console installer 37

Install Network Configuration Manager using silent installer 39

Creating the configuration file for a silent installation 39

Configuration parameters 40

Installing in silent mode 43

3 Uninstallation procedures (Linux platform) 45

Summary of uninstall tasks 45

Uninstalling the Network Configuration Manager core product 45

Uninstalling the Network Configuration Manager Device Drivers 46

4 Post-Installation procedures 47

Configuring Watch4net server 47

For Linux 48

Launching Watch4net user interface from Network Configuration Manager 48

For Linux 48

Enabling CAS configuration for EDAA URI 48

In Linux 49

Healthcheck updates 49

Database password change information 49

Error handling 50

Installer log files 50

Multi-Level cut-through mode configuration 51

Configuring Windows to accept cut-thru with default Telnet Client 51

Enable/disable auto-login features 51

Enable data on User Activity screen (Linux) 52

Client-side required configuration to disable SSLv3 52

Client-side installation 54

NCM UI Installation (Windows) 54

NCM UI Installation (Linux) 55

NCM UI Uninstallation Procedure 55

Client-side startup 56

Configuring the sysadmin user's email address 56

Setting up the profile 57

Enabling SAML authentication 57

Installing the sysadmin console (Linux) 59

Enabling Syslog messages in RHEL 8 59

Launching MSA GUI 59

5 Cluster installation 61

Overview 61

Software Requirements 61

Configuration Requirements 61

Installing the Fibre Channel Cards 62

Installing Network Configuration Manager with the Cluster installation 62

Validating the UNIX User ID and Group ID numbers 63

Operating the Network Configuration Manager Cluster 63

Restoring from a Backup 64

Uninstalling Network Configuration Manager 64

6 RSA Token service installation 66

Summary of Installation Tasks 66

Prerequisites for the RSA Token Service 67

Software Requirements 67

Installing the RSA Token Service using the graphical installer mode 68

Post-Installation Procedures 69

Importing RSA Tokens into the Network Configuration Manager RSA Token Server 70

Deleting RSA Tokens from the Network Configuration Manager RSA Token Server 71

Configuring the RSA Token ServiceNetwork Configuration Manager 72

Verifying RSA Tokens in Network Configuration Manager 72

Uninstalling the RSA Token Service 73

Network Configuration Manager RSA Token Service Instrumentation Web Page 73

Resetting the RSA Token Server Username and Password 74

7 Installation on Geo Diverse 75

Network Configuration Manager Geo Diverse 75

Features 75

Replication Requirements 76

Components 76

Installing Network Configuration Manager in a Geo Diverse Environment 77

Validating the UNIX User ID and Group ID Numbers 78

Using the vcgeoadmin.pl script 79

Logging the vcgeoadmin.pl script 80

Testing the Geo Diverse failover script without replication software 80

If you need to rollback to first Application server: 82

8 Integration Adapter for Smarts Manager 84

Introduction 84

Terminology 85

Prerequisites 85

Deployment 85

How the Integration adapter for Smarts Manager operates 86

Batch device synchronization 86

Active (device) synchronization 87

SNMP credential synchronization 87

Event notification 88

Important information about synchronization 88

Mapping between networks and IP Availability Managers 88

Installation programs 89

Installing the Integration adapters 89

For Linux 89

Installed services 90

Establish a secure connection with the server 90

Configuring the Adapter 91

Discovering Network Configuration Manager with Smarts Manager 91

Accessing the configuration GUI 91

Step 1: Network Configuration Managerpublic API connection configurations 92

Step 2: SAM connection configuration 93

Step 3: Smarts IP Availability Manager connections configuration 94

Step 4: Synchronization options 96

Mapping Configuration 98

Device Configuration Change Event 98

Credential Synchronization Configuration 98

Step 5: Mapping rules 98

Rule structure 99

Extended rule for Network Configuration Manager Device servers 100

Exclusions 102

Tips and tricks 103

Mapping NCM to Smarts 104

Mapping with topology split manager (TSM) 104

Configuring Service Assurance Manager (SAM) for contextual launch 105

Additional Required Configurations 106

Installing the contextual launch scripts for Smarts Manager 106

Setup for SAM GUI contextual launch 106

Setup for M&R GUI contextual launch 107

Client tools 108

NCM device Info client tool 108

NCM job info client tool 109

NCM Query Client Tool 109

Device communication report client tool 109

Device change report client tool 110

Device compliance report client tool 110

NCM Device query client tool 111

Configuring the Service Assurance Manager (SAM) dashboard (web client) 111

Advanced configuration 112

Customizing notifications 112

User-defined fields 113

Uninstall instructions 113

Linux 113

Uninstall instructions for client tools for Service Assurance Manager (SAM) 114

9 Integration modules configuration 116

Introducing the Integration Adapters 116

Integration adapters installation 117

Integration adapters configuration and management 117

JMiniX Console 117

Accessing the JMiniX Console 117

Updating configuration using the JMiniX Console 118

Starting or restarting integration modules 119

Integration adapters management operations 119

Managing events 120

Supported Events 121

The types of actions that can cause events to be fired 121

Transform Definition File 126

XPATH 126

CONSTANT 127

VARSTRING 127

VELOCITY 127

Flat File Integration adapters 128

Flat file Integration adapters assembly 128

Flat file integration adapters configuration 129

Tailoring the flat file integration adapters 129

Modifying the transform definition 130

Flat file integration adapters administration 130

Default file format 130

File locking considerations 132

File rolling considerations 132

Email Integration adapters 133

Email integration adapters assembly 133

Email Integration adapters configuration 134

Tailoring the email integration adapters 134

Generic SNMP Integration adapters 134

Generic SNMP integration adapters assembly 135

Generic SNMP integration adapters configuration 135

Tailoring the generic SNMP integration adapters 135

Launching the application through a URL 136

List of allowed query strings 137

10 Upgrade procedures (Linux platform) 138

Overview 138

Upgrading using the graphical installer mode 138

Upgrading an existing version using the graphical installer mode 139

Upgrading using the console installer mode 140

Upgrading an existing version using the console based installer mode 141

Updating the privLevels.xml 142

Post upgrade procedures 143

Add distributed system hosts for remote servers (standard or advanced security) 143

Reset the JMX password 143

Reapply customizations to the system-config.xml file 144

Retain RSA users after the NCM upgrade 144

11 Backup and recovery 145

Overview 145

Network Configuration Manager distributed architecture 146

Data locations 146

Backup utilities 147

Steps to backup and restore database in NCM 148

Steps to backup and restore database in NCM Combination setup 148

Steps to backup and restore database in NCM distributed setup 151

Customer responsibilities 154

Hot spare scenario 154

Backing up clustered and distributed database environments 155

12 Getting Started with Network Configuration Manager 156

Accessing additional Network Configuration Manager publications 156

After installation—getting started using Network Configuration Manager 156

Tips: 157

Lightweight Directory Access Protocol (LDAP) 157

13 Maintaining the server 161

Licensing 161

Obtaining a new license key 161

Installing a license key 162

Upgrading a license key 162

Using the runLicenseCmd script 162

The product serial number 162

Handling an expired license key 162

Command-line utilities 163

Extract config 163

Security 163

Backup and restore 163

Creating a data image 163

Restoring a data image 164

Purging device revisions and audit history 164

System services 165

Log files 165

Application server logs 165

Debug logging 166

Certificates 166

Installing Root CA certificate on the client 166

SSL Configuration—CA-signed certificates 167

Installing the private key and certificate 167

Changing the default from address 168

Changing the department and company name in the client Dashboard 169

Changing the default pull operation 169

Database vacuum 170

Searching for database tables to cleanup 170

Running a full database vacuum 171

Running a partial database vacuum 171

Disabling TCP Fusion 172

Password management 172

Changing passwords in Network Configuration Manager 172

Archiving data 173

Performance tweaks 173

Disclaimer 173

Switch between advanced and standard security modes 175

Switch from Standard Security to Advanced Security 175

Switch from Advanced Security to Standard Security 175

Location of IP addresses in Servers 176

Application server 176

Device server 176

Database server 176

14 Utilities 177

Database Archive Utility 177

Usage 178

Arguments 178

Examples 179

Lockbox utility 179

Lockbox utility features 179

Encrypting functionality 180

Decrypting functionality (for system administrators only) 180

- Unlocking functionality 180
- Unlocking the lockbox using the passphrase 180
- Changing the lockbox passphrase 180

Change NCM passwords 181

Introduction to Network Configuration Manager

1

Read the following topics next:

- What is Network Configuration Manager?
- Where to get help
- About this manual
- Product installation directory
- Deployment architecture
- Running a software prerequisites check
- Product and version compatibility
- Installation tasks
- Upgrade

What is Network Configuration Manager?

- Network Configuration Manager is a network configuration management tool that gives you the power to quickly, easily, and accurately design, modify, and maintain networks, using an intuitive graphical network view.
- Network Configuration Manager automates complex and routine engineering tasks, such as adding devices and connections, with drag-and-drop simplicity.
- Using real-time auto discovery of network devices and logical and physical topology information, Network Configuration Manager provides a proactive configuration management approach.

Where to get help

Contact your VMware technical support professional if a product does not function properly or does not function as described in this document.

Note This document was accurate at publication time. Go to VMware Online Support docs.vmware.com to ensure that you are using the latest version of this document.

VMware support and product information can be obtained as follows:

Product information

For documentation, release notes, software updates, or information about VMware products, go to VMware Online Support at:

support.vmware.com

docs.vmware.com

Technical support

Go to VMware Online Support and click Service Center. You will see several options for contacting VMware Technical Support. Note that to open a service request, you must have a valid support agreement. Contact your VMware sales representative for details about obtaining a valid support agreement or with questions about your account.

About this manual

This manual provides the following information and procedures necessary to install to Network Configuration Manager including:

- Deployment Architecture
- Installing Network Configuration Manager
- Post Installation Procedures
- Maintaining the Server
- Uninstalling Network Configuration Manager Procedures

Product installation directory

In the install and uninstall instructions, the term [Product Directory] represents your actual installation directory. You must substitute [Product Directory] with your actual installation directory path. Ensure that the name of the [Product Directory] do not have spaces.

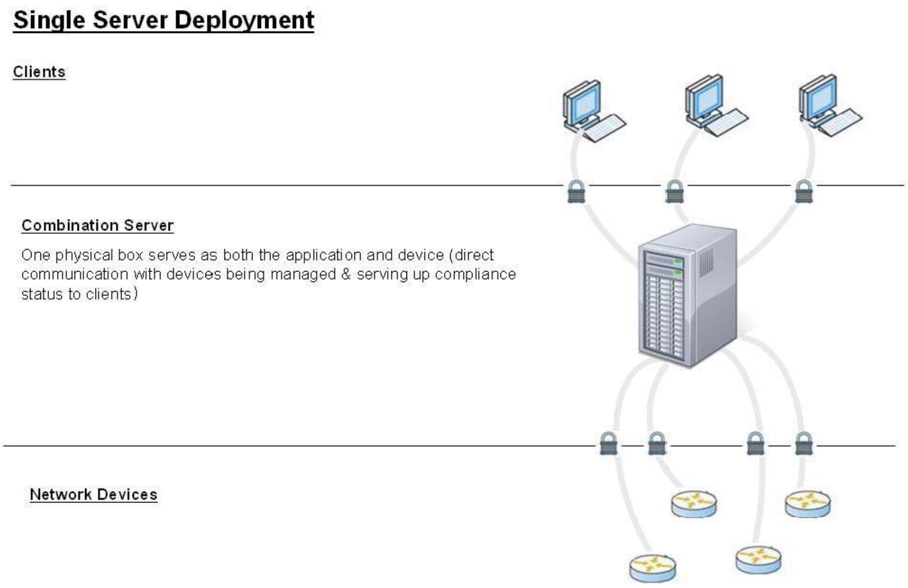
For Linux, you can determine your product installation directory by examining /etc/voyence.conf, and looking for the text VOYENCE_HOME.

Deployment architecture

The Network Configuration Manager must be installed on a dedicated server.

The Network Configuration Manager can be deployed in a single-server model or a distributed model. The distributed model is often used by multi-national corporations or managed service providers with thousands of devices to manage.

- Single server deployment
  - Combination server – One physical box serves as both the Application and Device server.

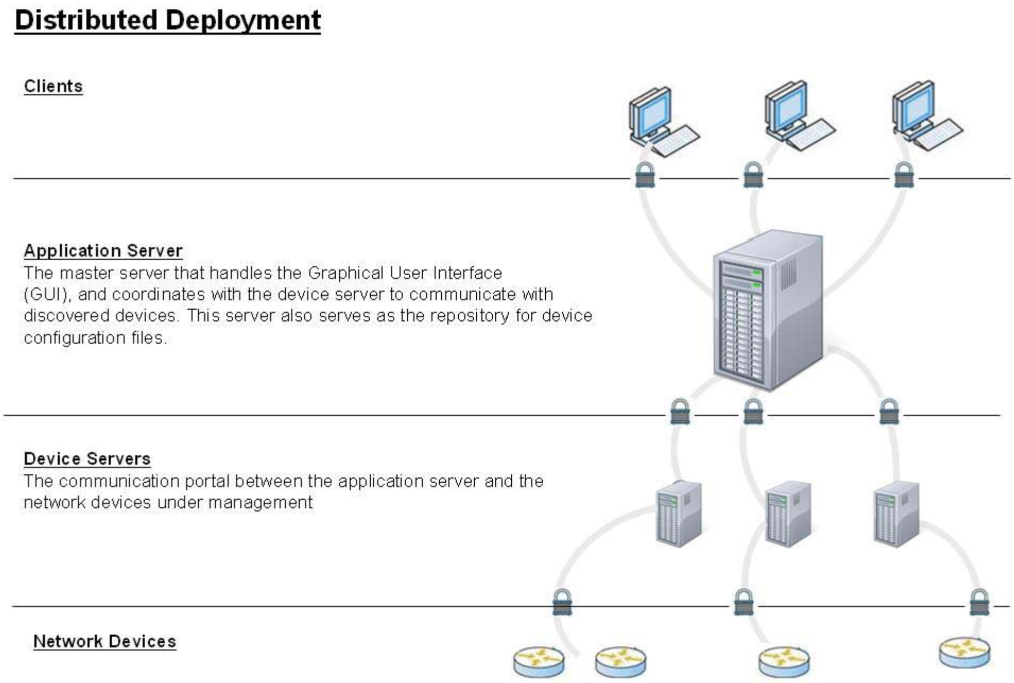


One physical box serves as both the application and device (direct communication with devices being managed & serving up compliance status to clients)

- **Distributed deployment**
  - Application server—The server that handles the Graphical User Interface (GUI), and coordinates with the Device server to communicate with discovered devices. This server also serves as the repository for device configuration files.
  - Device server—The communication portal between the Application server and the network devices under management.
  - Remote Database—A client computer monitored and professionally managed from a remote location, usually by a third-party. (For Linux only).

- Local Database—A database that is located on the Application server.

Note



Distributed Deployment

Clients

Application Server
The master server that handles the Graphical User Interface (GUI), and coordinates with the device server to communicate with discovered devices. This server also serves as the repository for device configuration files.

Device Servers
The communication portal between the application server and the network devices under management

Network Devices

The installation must be repeated for each server. If you are installing a distributed server configuration, with separate Application server and Device servers, you must first install Network Configuration Manager on the Application server, and then install it on the Device servers.

You must use the same operating system for all Network Configuration Manager servers in order for NCM features to work properly. For example, if the Application Server (AS) is on Linux and the Device Server (DS) is on other platform, the Event Manager will not show the Key Strokes for Run Cut-thru.

Running a software prerequisites check

Note These steps are optional. The software prerequisites will be verified during a normal Network Configuration Manager installation.

A software prerequisite check verifies that the Network Configuration Manager software prerequisites are installed prior to installing Network Configuration Manager. These steps are strongly recommended.

To run the software prerequisites check script, follow these steps:

Step	Action
1	On the server where you want to install Network Configuration Manager software, log in with administrator privileges.
2	In the downloaded binary for the Network Configuration Manager product, navigate to the **utils** folder.
3	Type **unzip prereq-check.zip** to unzip the software prerequisite script, and press **Enter.**
3	Type **perl prereq-check.pl <Server Type>** to run the software prerequisite script, where <Server Type> is one of the values below. ■ **CS** for Combination server ■ **AS** for Application server ■ **DS** for Device server ■ **DB** for Database server ■ **RSA** for RSA Token server If successful, the script exits displaying the results of prerequisites check. If one or more software prerequisites are missing or are the incorrect version, a message appears with instructions to fix the problems.

Product and version compatibility

Review the minimum system requirements mentioned in VMware Smart Assurance Network Configuration Manager Support Matrix document. The document provides information that helps you:

- Determine if the product is supported on your platform.
- Review the patch requirements for your operating system.
- Determine if your system meets the hardware requirements.

Installation tasks

The recommended order of installation tasks for new installations is as follows:

Step	**Task**
1	Review the minimum system requirements mentioned in VMware Smart Assurance Network Configuration Manager Support Matrix document.
2	Install the operating system including any prerequisites. **Note** Install the appropriate package groups for use with Network Configuration Manager.
3	Ensure all firewalls adhere to the Communication security settings mentioned in VMware Smart Assurance Network Configuration Manager Security Configuration Guide.
5	Install Network Configuration Manager. **Note** If errors occur during installation, refer to the VMware Smart Assurance Network Configuration Manager Troubleshooting Guide for a list of solutions.

Step	Task
6	Configure Network Configuration Manager using Chapter 4 Post-Installation procedures
7	Begin using Network Configuration Manager using the steps in Chapter 12 Getting Started with Network Configuration Manager .

Product installation directory

Note In the install and uninstall instructions, the term [Product Directory] represents your actual installation directory. You must substitute [Product Directory] with your actual installation directory path. Ensure that the name of the [Product Directory] do not have spaces.

For Linux, you can determine your product installation directory by examining /etc/voyence.conf, and looking for the text VOYENCE_HOME.

Upgrade

You can upgrade from the following versions to Network Configuration Manager 10.1.6:

- Network Configuration Manager 9.6
- Network Configuration Manager 9.6.1
- Network Configuration Manager 10.1
- Network Configuration Manager 10.1.1
- Network Configuration Manager 10.1.3
- Network Configuration Manager 10.1.4

  You cannot directly upgrade from the versions below 9.6. For these versions you must first upgrade to 9.6 versions and then upgrade to 10.1.6.

- To use Network Configuration Manager 10.1.6 on the host where you had previously installed Network Configuration Manager, you must use the upgrade procedure to upgrade to Network Configuration Manager.
- To use Network Configuration Manager 10.1.6 on a new host, use the new installation procedure to install NCM 10.1.6 on the new host.

  Then, perform an in-place upgrade from previously installed NCM to 10.1.6 on the old host and take the backup (using [Product Directory]/tools/backup.pl) of your data on the old host where Network Configuration Manager lower version was installed, and restore (using [Product Directory]/tools/restore.pl) the data on the new host where 10.1.6 is installed. Backup utilities provides more information about these utilities.

OS version support updates

The RHEL 6.x support is not supported.

For the users who are using the older NCM release on RHEL 6.x version, and want to upgrade to 10.1.6, take the backup (using [Product Directory]/tools/backup.pl) from the older NCM version, and restore (using [Product Directory]/tools/restore.pl) the same on newly installed NCM 10.1.6 server.

The NCM database backup/restore has been validated with minimum data for the following paths:

- NCM 9.6 combination server on RHEL 6.x to NCM 10.1.6 Combination server on RHEL 7.x

Upgrade tasks

If you plan to upgrade, you have to upgrade all the components to the latest Network Configuration Manager release.

Upgrade tasks for Linux

The recommended order of tasks for upgrading the Network Configuration Manager is as follows:

Step	Action
1	Review the minimum system requirements mentioned in VMware Smart Assurance Network Configuration Manager Support Matrix document. Ensure that you have met all the requirements to compete the Network Configuration Manager installation.
2	Upgrade the Database server if you are using a remote, stand-alone Database server.
3	Upgrade the current Network Configuration Manager Application server or Combination server using one of the following installation interfaces: ■ **Graphical** - The graphical installer can be used when an X Windows session is present on the server you select for installation. ■ **Console-Based Installer** - The console-based installer is appropriate for installs that take place over a command line-based connection, such as Telnet and SSH. ■ **Silent Installer** - The Network Configuration Manager installer allows you to supply a configuration file containing the variables necessary for an installation, also known as a silent installation.
4	Upgrade software on the Device server.

Installing new Device Servers in FIPS Enabled mode

Follow the procedure only when the AS or CS is upgraded 10.1.6.0 setup, and you want to add new Device Servers:

1 `source /etc/voyence.conf`.

2 Go to `cd $VOYENCE_HOME/tools`.

3 Execute the command `perl rebundlepkcs.pl <location of old bundle.p12 file> <certificate passphrase>`.

   If the `rebundlepkcs.pl` is successful, the new `bundle.p12` file replaces the `bundle.p12` file mentioned in step 3.

4 The new `bundle.p12` must be used while installing new Device Servers.

Installation procedures (Linux platform)

2

Read the following topics next:

- Prerequisites and installation order
- Install Network Configuration Manager using graphical installer mode
- Install Network Configuration Manager using console installer
- Install Network Configuration Manager using silent installer

Prerequisites and installation order

Prerequisites

The following conditions are required.

1. Install the Network Configuration Manager on a dedicated server and do not run other applications on that server.
2. Before you start the installation, ensure that you have proper FQDN set on the server where you are performing the installation.

   To verify, run the hostname command and check if it is returning the server name with DNS.
3. Before you start the installation, ensure that no instance of Tomcat exists on the target machine.

   Note If an instance of Tomcat exists on the machine, you must remove it before proceeding with installation.

   The following conditions are highly recommended.

4 Before you start the installation, run the **prereq-check.pl** script to verify that all of the Network Configuration Manager software prerequisites are met.

Note It is strongly recommended to run the **prereq-check.pl** script on a server before installing any Network Configuration Manager software on that server.

For information about obtaining and running **prereq-check.pl,** see Running a software prerequisites check.

Order of installation

Follow these sections in the order mentioned to install Network Configuration Manager:

1. Install Combination or Application server using graphical installer

   or

   Install Combination, Application, and Database server using console installer
2. Add distributed system hosts for remote servers (standard or advanced security)
3. Export and import certificates for EDAA and Smarts Adapter
4. Import Network Configuration Manager Certificates for remote servers
5. Install a Device server using graphical installer

Install Network Configuration Manager using graphical installer mode

This section describes how to use the graphical installer mode to install Network Configuration Manager. When installing Network Configuration Manager, the servers must be installed in the following order:

- Stand-alone Database server (if applicable)
- Combination server or Application server
- Device server (if applicable)

  The installation must be repeated for each server. If you are installing a distributed server configuration with separate Database server, Application server and Device servers, then:
- You must first install Network Configuration Manager on the Database server, followed by installation on the Application server, and then install on the Device server.

  Note At setup, the Device server registers itself with the Application server. Before installing the Device servers, ensure its corresponding Application server has the same date and time as the candidate Device server. If not, the Device server cannot communicate with the Application server resulting in the installation failure.

To start the installation, you have to run the script **install.sh**. When you run the script, the command prompt screen appears with four options:

- Type **1**, and press **Enter** to install NCM Core product, and Device Drivers.
- Type **2**, and press **Enter** to install NCM Smarts Adapters.
- Type **3**, and press **Enter** to install NCM Core product and NCM Smarts Adapters.
- Type **4**, and press **Enter** to exit the installation.

Install a Database server by using graphical installer

Note The graphical user interface (GUI mode) installer requires a connection to a running X server.

This section only applies to remote, stand-alone Database servers for use with Network Configuration Manager.

To install a stand-alone Database server using the graphical installer mode, follow these steps:

Step	Action
1	Log into the server as a user with administrator privileges.
2	Type **bash install.sh –i gui** to run the installer in the graphical installer mode, and press **Enter.** The command prompt screen appears: ■ Type **1**, and press **Enter** to install NCM Core product, and Device Drivers. The installer begins to load. The install.sh script checks to ensure that all the prerequisites for the Network Configuration Manager are installed. The script automatically installs any missing prerequisites if the prerequisites are located in the Utils directory. The **Core Setup Installer** begins to load.
Core Setup Installer Procedures	
3	The Introduction window opens. Click **Next** at the Introduction window. Notice that as you go through the various steps needed to install, the navigation pane on the left keeps a running list of the completed steps. For example, you can see at the License Agreement window that the Introduction has been completed. A check (√) appears by each completed phase of the installation. The right arrow (▶) indicates the current window and installation status.
4	The License Agreement window opens. Read the license agreement, select **I accept the terms of the License Agreement**, and click **Next**.
5	The Server Configuration window opens. Select **Database server** as your configuration type, and click **Next**.
6	The Choose Install Folder window opens. You are prompted to choose the Install Folder. Accept the default location, or click **Choose** and select another location. Once the install folder is selected, click **Next**. This is the location where Network Configuration Manager will be installed.
7	The Database Access List window opens. Type the **IP Address** that needs access to the Database server, and click **Next**.

Step	Action
9	The Database password window appears. Type a password for Database. The password must contain at least: ■ One letter in upper case ■ One letter in lower case ■ One special character ■ One numerical ■ Minimum fifteen characters The special characters that can be used for the database password are: ■ Tilde (~) ■ Exclamation (!) ■ At (@) ■ Number (#) ■ Percent (%) **Note** It is recommended that the password must not start or end with a special character.
10	The Summary window displays the product information, as well as the required disk space. Click **Install** to start the installation. This portion of the installation may take several minutes. When complete, the Install Complete window opens.
11	Install Combination or Application server as described in *"Install Combination or Application server using graphical installer" on page 75*.

Install Combination or Application server using graphical installer

Note The graphical user interface (GUI mode) installer requires a connection to a running X server.

To install a Combination or Application server using the graphical installer mode, follow these steps:

Step	Action
1	Log into the server as a user with administrator privileges.
2	Type **bash install.sh –i gui** to run the installer in the graphical installer mode,and press **Enter**. The command prompt screen appears: ■ Type **1**, and press **Enter** to install NCM Core product, and Device Drivers. The installer begins to load. The install.sh script checks to ensure that all the prerequisites for the Network Configuration Manager are installed. The script automatically installs any missing prerequisites if the prerequisites are located in the Utils directory. The **Core Setup Installer** begins to load.
Core Setup Installer Procedures	

Step	Action
3	The Introduction window opens. Click **Next** at the Introduction window. Notice that as you go through the various steps needed to install, the navigation pane on the left keeps a running list of the completed steps. For example, you can see at the License Agreement window that the Introduction has been completed. A check (√) appears by each completed phase of the installation. The right arrow (▶) indicates the current window and installation status.
4	The License Agreement window opens. Read the license agreement, select **I accept the terms of the License Agreement**, and click **Next**.
5	The Server Configuration window opens. Select the server you want to install, and click **Next**.
6	The Choose Install Folder window opens. You are prompted to choose the Install Folder. ■ Accept the default location, or click **Choose** and select another location. ■ Once the install folder is selected, click **Next**. This is the location where Network Configuration Manager will be installed. ■ If you are installing **Application server**, proceed to step *"11"*.
7	**Note** This step only appears if the httpd.conf directory is not in the default location. The httpd.conf Location window opens. You are now prompted to choose the httpd.conffile location. ■ Accept the default location, or click **Choose** and select another location. ■ Once the httpd.conf file location is selected, click **Next**. This is where the Apache configuration file httpd.conf is located.
8	**Note** This step only appears if the Java directory is not in the default location. The Java Location window opens. You are now prompted to choose the Java directory. ■ Accept the default location, or click **Choose** and select another location. ■ Once the Java directory is selected, click **Next**. This is the location where the Java application is installed.
9	**Note** This step only appears if the Tomcat directory is not in the default location. The Tomcat Location window opens. You are now prompted to choose the Tomcat directory. ■ Accept the default location, or click **Choose** and select another location. ■ Once the Tomcat directory is selected, click **Next**. This is the location where the Tomcat application is installed. **Note** If you are installing **Application server**, proceed to step *"11"*.
10	The Combo Server Alias window opens. Enter an **Alias** for the Combination server and click **Next**. This alias displays in the System Administration portion of Network Configuration Manager. This alias must not contain spaces or special characters.

Step	Action
11	The Database Configuration window opens. ■ The Database Configuration window lets you specify whether the database is running locally to the Application or Combination server or remotely. Select **one** of the following options: ■ Select **local** to run the database on the same server as the application. ■ Select **remote** to run the database on a separate server. If you select **remote**, the separate Database server must already be installed and available over the network, and you must type the **IP address** of the Database server. ■ Click **Next**.
12	The Watch4net configuration requirement check window appears. ■ Select **Yes** to configure the Network Configuration Manager Reporting SolutionPack and click **Next**. ■ Select **No** to continue without configuring Network Configuration Manager Reporting SolutionPack. *"Configuring EMC M&R server" on page 120* provides instructions on configuring Watch4net server post Network Configuration Manager installation.
13	The Watch4net Server IP address window appears. Type the Watch4net Server IP address and click **Next**. **Note** Do not enter the server name or FQDN.
14	The License Key window opens. You are now prompted to **Choose** the License Key File. ■ Click **Choose**, and select another location. Make the needed selection, then click **Select** when you have completed selecting another file. ■ Type the **Company Name** you want displayed on the main screen of the application. ■ Type the **Department/Division** name you want displayed on the main screen of the application. This field is optional. ■ Click **Next**. **Note** If you are installing **Application server**, proceed to step *"17"*.
15	The **Root CA Certificates** window opens. ■ To import a 3rd party root CA certificate, select **Yes**, or to accept the default certificate, select **No**. **Note** Root CA certificates should only need to be imported if a 3rd party SSL certificate is used in the Network Configuration Manager configuration.
16	The Certificate password window appears. Type a password for Certificate. The password must contain at least: ■ One letter in upper case ■ One letter in lower case ■ One special character ■ One numerical ■ Minimum fifteen characters **Note** The password must not start or end with a special character. Special characters that can be used for the certificate password are: ■ Tilde (~) ■ Exclamation (!) ■ At (@) ■ Number (#) ■ Percent (%)

Step	Action
17	If you selected **Yes** in the previous step, you are prompted to select the file containing the Root CA certificate. Click **Next** to continue. At the end of this step, you are able to import additional certificates, if needed.
18	The Email Configuration window opens. ■ Enter a **From Address** for the email notifications that come from the server. This is the email address where the job notifications are sent from. ■ Enter a **FQDN** or **IP Address** for the outbound SMTP mail server. ■ Click **Next**. **Note** Ensure that mail is accepted from the Network Configuration Manager server.
19	The Lockbox passphrase window appears. Type a passphrase for Lockbox. The passphrase must contain at least: ■ One letter in upper case ■ One letter in lower case ■ One special character ■ One numerical ■ Minimum fifteen characters The special characters that can be used for the lockbox passphrase are: ■ Tilde (~) ■ At (@) ■ Number (#) ■ Percent (%) ■ Exclamation (!) **Note** It is recommended that the passphrase must not start or end with a special character.
20	The Security Questions window appears. Type the answers for the security questions and click **Next**.
21	The Encryption Key store option window appears. Choose a location where NCM should store the encryption key that is used to encrypt and decrypt data. The options are: ■ 1 for Standard Security – Key stored encrypted in a flat file ■ 2 for Advanced Security – Key stored in RSA Lockbox **Note** If you return to this window later during the installation process, the option you selected will be displayed in encrypted format (not in clear text).

Step	Action
22	The Database password window appears. Type a password for Database. The password must contain at least: ■ One letter in upper case ■ One letter in lower case ■ One special character ■ One numerical ■ Minimum fifteen characters The special characters that can be used for the database password are: ■ Tilde (~) ■ Exclamation (!) ■ At (@) ■ Number (#) ■ Percent (%) **Note** It is recommended that the password must not start or end with a special character.
23	The Summary window displays the product information, as well as the required disk space. Click **Install** to start the installation. This portion of the installation may take several minutes. When complete, the Device Driver Installer begins to load. **Note** If there is not enough available disk space, the installer displays an error message until sufficient disk space is free. You can continue once enough disk space is available.
Device Driver Installer Procedures	
24	While the Device Driver installer is running, a progress bar displays the install status. This portion of the installation may take several minutes. **Note** During installation of the device drivers, the files in the custompackage directory that matches the files in the device drivers directory are listed. These files will override similar files in the device drivers directories. For example, if you have modified the file stdfuncs.inc for CiscoIOSRouter, it would be placed in the custom package directory and will override the same file in the /opt/voyence/package/cisco/ios directory.
After installing Combination server or Application server	
26	Add distributed system hosts to the lockbox for remote servers.

Lockbox utility

Lockbox utility provides increased security for data. The lockbox is a file that serves as a local repository for storing the passphrase which is used for encryption of sensitive data such as user credentials. The encryption algorithm is upgraded from Blowfish to AES. The lockbox file can be opened only on the machine on which it is created.

Lockbox utility provides more information for Lockbox utility functionalities.

Add distributed system hosts for remote servers (standard or advanced security)

Use the following steps to add distributed system hosts:

1 If you choose Standard Security mode during AS installation, copy **lockb.ekey** from [product directory]/data in the AS to [product directory]/data on the remote server (DS, RA, or Database).

2 If you chose Advanced Security mode during AS installation:

3 On the Application server, go to [Product directory]/bin directory.

4 Source the voyence.conf file

```
source /etc/voyence.conf
```

5 Add distributed system hosts to the lockbox using the **cstdriver** utility:

```
./cstdriver -lockbox  [Product directory]/data/lockb.clb
-passphrase <passphrase> -addHost <FQDN of Database server>
./cstdriver -lockbox [Product directory]/data/lockb.clb
-passphrase <passphrase> -addHost <FQDN>
./cstdriver -lockbox [Product directory]/data/lockb.clb
-passphrase <passphrase> -addHost <FQDN of Device server>
```

6 Go to [Product directory]/data directory.

7 Copy the lockbox file to any directory on each of the distributed system hosts.

8 For example:

```
scp lockb.clb Host2_DB_Server:/root/
scp lockb.clb Host3_Device_Server:/root/
```

Next step, go to Export and import certificates for EDAA and Smarts Adapter.

Import Network Configuration Manager Certificates for remote servers

For establishing a secure connection from Application server to remote Device server, you have to get the certificates from the Application server.

Follow these steps to get the certificates from Application server:

1 On a Linux server, run the command

```
# source /etc/voyence.conf
```

2 Go to **[Product directory]/conf** directory.

3 Copy the bundle.p12 certificate file to remote Device server. For example:

```
scp bundle.p12 Host3_Device_Server:/root/
```

Note If new Device Server is being installed in FIPs enabled mode and is being added to the upgraded 10.1.6 CS or AS setup. Then re-generate the bundle.p12 in AS or CS by following steps mentioned under *Installing new Device Servers in FIPS Enabled mode* in Upgrade tasks for Linux section.

Next step, go to Export and import certificates for EDAA and Smarts Adapter.

Export and import certificates for EDAA and Smarts Adapter

For establishing a secure connection to the Network Configuration Manager server:

1 From the Network Configuration Manager Application or Combination server, export the self signed certificate from `[Product Directory]/conf/voyence-ssl.keystore` to a file using the steps:

   a `source /etc/voyence.conf`

   b `$JAVA_HOME/bin/keytool -export -keystore [Product directory]/conf/voyence-ssl.keystore -alias selfsigned -file <CERTIFICATE>`

   To find the location of `JAVA_HOME`, type the command echo `$JAVA_HOME`. Ensure that `JAVA_HOME` is pointing to the right version of Java. For example, `<<VOYENCE_HOME>>/java`.

   Note <CERTIFICATE> can be any name and it is the file that is created from the export.

   c Press **Enter** without entering a password.

2 Import the self signed certificate from the file <*CERTIFICATE*>.

```
$JAVA_HOME/bin/keytool -keystore $JAVA_HOME/jre/lib/security/cacerts -import -file
<CERTIFICATE> -alias selfsigned
```

3 Type the password **changeit** during the prompt.

4 This is the default password, unless otherwise modified.

5 Type **Yes** and click **Enter** when the **Trust the certificate** prompt appears.

   To view the imported certificate, type:

```
$JAVA_HOME/bin/keytool -keystore $JAVA_HOME/jre/lib/security/cacerts -list -alias
selfsigned
```

Install a Device server using graphical installer

Note The graphical user interface (GUI mode) installer requires a connection to a running X server.

If you are installing a distributed server configuration, with separate Application server and Device servers, you must first install Network Configuration Manager on the Application server, and then install it on the Device servers.

Note Before installing Device servers, ensure the Application or Combination servers have the same date and time as the candidate Device server. If not, the Device server will not be able to register with the Application or Combination servers, and the installation will fail.

If the Device server cannot communicate with the Application server, this step fails, and you must reinstall the Device server.

To install a Device server using the graphical installer mode, follow these steps:

Step	Action
1	Log into the server as a user with administrator privileges.
2	Type **bash install.sh –i gui** to run the installer in the graphical installer mode, and press **Enter**. The command prompt screen appears: ■ Type **1**, and press **Enter** to install NCM Core product, and Device Drivers. The installer begins to load. The install.sh script checks to ensure that all the prerequisites for the Network Configuration Manager are installed. The script automatically installs any missing prerequisites if the prerequisites are located in the Utils directory. The **Core Setup Installer** begins to load.
Core Setup Installer Procedures	
3	The Introduction window opens. Click **Next** at the Introduction window. Notice that as you go through the various steps needed to install, the navigation pane on the left keeps a running list of the completed steps. For example, you can see at the License Agreement window that the Introduction has been completed. A check (√) appears by each completed phase of the installation. The right arrow (▶) indicates the current window and installation status.
4	The License Agreement window appears. Read the license agreement, select **I accept the terms of the License Agreement**, and click **Next**.
5	The Server Configuration window opens. Select **Device server** as your configuration type, and click **Next**. **Note** When installing a Device server, you must install the Application server first, and have it running and available to the Device server over the network.
6	The Choose Install Folder window opens. You are prompted to choose the Install Folder. ■ Accept the default location, or click **Choose** and select another location. ■ Once the install folder is selected, click **Next**. This is the location where Network Configuration Manager will be installed.

Step	Action
7	**Note** This step only appears if the httpd.conf directory is not in the default location. The httpd.conf Location window opens. You are now prompted to choose the directory where httpd.conf is located. - Accept the default location, or click **Choose** and select another location. - Once the httpd.conf file location is selected, click **Next**. This is where the Apache configuration file httpd.conf is located.
8	**Note** This step only appears if the Java directory is not in the default location. The Java Location window opens. You are now prompted to choose the Java directory. - Accept the default location, or click **Choose** and select another location. - Once the Java directory is selected, click **Next**. This is the location where the Java application is installed.
9	**Note** This step only appears if the Tomcat directory is not in the default location. The Tomcat Location window opens. You are now prompted to choose the Tomcat directory. - Accept the default location, or click **Choose** and select another location. - Once the Tomcat directory is selected, click **Next**. This is the location where the Tomcat application is installed.
10	The Application server IP window opens. - Enter an **IP Address** for the Application server, and click **Next**.
11	The Device server Alias window opens. - Enter an **Alias** for the Device server and click **Next**. This alias appears in the System Administration portion of Network Configuration Manager. This alias must not contain spaces or special characters.
12	The **Root CA Certificates** window opens. To import a 3rd party root CA certificate, select **Yes**, or to accept the default certificate, select **No**. **Note** Root CA certificates should only need to be imported if a 3rd party SSL certificate is used in the Network Configuration Manager configuration.
13	If you selected **Yes** in the previous step, you are prompted to select the file containing the Root CA certificate. Click **Next** to continue. At the end of this step, you are able to import additional certificates, if needed. **Note** If there is not enough available disk space, the installer displays an error message until sufficient disk space is free. You can continue once enough disk space is available.
14	The Certificate file location window appears. Provide the path for the certificate file **bundle.p12** that was copied earlier and click **Next**.
15	The Password for certificate window appears. Type the same password that you entered while installing Application server and click **Next**.
16	**Note** You must perform this step irrespective of the mode of security you selected during the installation. The lockbox file location window appears. Provide the path to the lockbox file **lockb.clb** that was copied earlier and click **Next**.
17	The database password window appears. Type the same password that you entered while installing Application or Database server and click **Next**.

Step	Action
18	The Summary window displays the product information, as well as the required disk space. Click **Install** to start the installation. This portion of the installation may take several minutes. When complete, the Device Driver Installer begins to load.
Device Driver Installer Procedures	
19	While the Device Driver installer is running, a progress bar displays the install status. This portion of the installation may take several minutes. The installer displays the installation complete message. **Note** During installation of the device drivers, the files in the custompackage directory that matches the files in the device drivers directory are listed. These files will override similar files in the device drivers directories. For example, if you have modified the file stdfuncs.inc for CiscoIOSRouter, it would be placed in the custom package directory and will override the same file in the /opt/smarts-ncm/package/cisco/ios directory.

Next step, go to Chapter 4 Post-Installation procedures.

Install Network Configuration Manager using console installer

This section describes how to use the console-based installer to install Network Configuration Manager. When installing Network Configuration Manager, the servers must be installed in the following order.

- Stand-alone Database server (if applicable)
- Combination server or Application server
- Device server (if applicable)

  The installation must berepeated for each server. If you are installing a distributed server configuration, with separate Application server and Device servers, you must *first* install Network Configuration Manager on the Application server, and then install Network Configuration Manager on the Device servers.

  Note At setup, the Device server registers itself with the Application server. Before installing the Device servers, ensure the Application or Combination servers have the same date and time as the candidate Device server. If not, the Device server cannot communicate with the Application server, this step fails, and you must reinstall the Device server.

  To start the installation, you have to run the script **install.sh**. When you run the script, the command prompt screen appears with four options:

- Type **1**, and press **Enter** to install NCM Core product, and Device Drivers.
- Type **2**, and press **Enter** to install NCM Smarts Adapters.
- Type **3**, and press **Enter** to install NCM Core product and NCM Smarts Adapters.

- Type **4**, and press **Enter** to exit the installation.

Install Combination, Application, and Database server using console installer

To install a Combination, Application, and Database server using the console installer mode, follow these steps:

Step	Action
1	Log into the server as the root user.
2	Type **bash install.sh –i console** to run the installer in the console-based installer mode, and press **Enter**. The command prompt screen appears: ■ Type **1**, and press **Enter** to install NCM Core product, and Device Drivers. The installer begins to load. The install.sh script checks to ensure that all the prerequisites for the Network Configuration Manager are installed. The script automatically installs any missing prerequisites if the prerequisites are located in the Utils directory. The **Core Setup Installer** begins to load.
Core Setup Installer Procedures	
3	The introduction to the installer appears. Press **Enter** to continue.
4	The License Agreement appears. Read the license agreement. Press **Enter**, and continue to press **Enter** to move through each page of the license agreement until you reach the final page.
5	On the final page of the license agreement, type Y, and press **Enter** to accept the terms of the license agreement.
6	The installer prompts you to select a server configuration. Type **1**, and press **Enter** to select **Combination server**. Type **2**, and press **Enter** to select **Application server**. Type **4**, and press **Enter** to select **Database server**.
7	The installer prompts you to choose an install folder. Press **Enter** to accept the default, or enter a **location** for the install folder. This is the location where Network Configuration Manager will be installed. If you are installing **Combination server**, proceed to step *“9”* If you are installing **Application server**, proceed to step *“13”*.
8	**For Database server installation only:** The installer prompts you for the Database Access List IP Address. Type the IP Address that needs access to the Database server and Press Enter. Proceed to step *“14”*.
9	**Note** This step only appears if the httpd.conf directory is not in the default location. The installer prompts you for the directory where httpd.conf is located. Press **Enter** to accept the default, or type the **location** of the httpd.conf file. This is where the Apache configuration file httpd.conf is located.

Step	Action
10	**Note** This step only appears if the Java directory is not in the default location. The installer prompts you for the directory where Java is located. Press **Enter** to accept the default, or type the **location** of the Java directory. This is the location where the Java application is installed.
11	**Note** This step only appears if the Tomcat directory is not in the default location. The installer prompts you for the directory where Tomcat is located. Press **Enter** to accept the default, or type the **location** of the Tomcat directory. This is the location where the Tomcat application is installed. **Note** If you are installing Application server, proceed to step *"13"*.
12	**For Combination server installation only:** The installer prompts you for the combination server alias. Press **Enter** to accept the default, or enter an **Alias** for the Combination server. This alias displays in the System Administration portion of Network Configuration Manager. This alias must not contain spaces or special characters.
13	The installer prompts you for the database configuration type. - The Database Configuration screen lets you specify whether the database is running *locally* to the Application or Combination server or *remotely*. Select **one** of the following options: - Press **Enter** to select **local** (the default) to run the database on the same server as the application. - Type **2** to select **remote** to run the database on a separate server. If you select **remote**, the separate Database server must already be installed and available over the network. The default option is local. If you select remote, you will be prompted for the **IP address** of the Database server. - Press **Enter**.
14	The installer prompts you for the Reports server configuration type. Select **one** of the following options: - Press **Enter** to select **local** to run the reporting server on the same server as the application. - Type 2 to select **remote** to run the reporting server on a separate server and press **Enter**. For **Database server installation**, proceed to step *"27"*.
15	The installer prompts you for Watch4net configuration requirement check. - Select **Yes** to configure the Network Configuration Manager Reporting SolutionPack and press **Enter**. - Select **No** to continue without configuring Network Configuration Manager Reporting SolutionPack. *"Configuring EMC M&R server" on page 120* provides instructions on configuring Watch4net server post Network Configuration Manager installation.
16	The installer prompts you for the Watch4net server IP address. Type the Watch4net server IP address and press **Enter**.
17	The installer prompts you for the License Key. Type the **path** and **file name** for the text file that contains the license key, and then press **Enter**.
18	The installer prompts you to enter a company name. Press **Enter** to accept the default, or type the **company name** you want displayed on the main screen of the application.

Step	Action
19	The installer prompts you to enter a department or division name. Type the **department or division name** you want displayed on the main screen of the application, and press **Enter**. This field is optional. **Note** If you are installing **Application server**, proceed to step *“21”*.
20	**For Combination server installation only:** The installer prompts you to import root CA certificates. If you have any root CA certificates to import, type the **appropriate number**, and then press **Enter**.
21	The installer prompts for a password for Certificate. Type a password for Certificate. The password must contain atleast: ■ One letter in upper case ■ One letter in lower case ■ One special character ■ One numerical ■ Minimum fifteen characters **Note** The password must not start or end with a special character. Special characters that can be used for the certificate password are: ■ Tilde (~) ■ Exclamation (!) ■ At (@) ■ Number (#) ■ Percent (%)
22	The installer prompts you to enter an **Email From address**. Press **Enter** to accept the default, or enter a **From Address** for the email notifications that come from the server. This is the email address where the job notifications are sent from.
23	Enter a **FQDN** or **IP Address** for the outbound SMTP mail server, and press **Enter**.

Step	Action

24	The installer prompts for a lockbox passphrase. Type a passphrase for Lockbox.
	The passphrase must contain at least:
	■ One letter in upper case
	■ One letter in lower case
	■ One special character
	■ One numerical
	■ Minimum fifteen characters
	Note It is recommended that the passphrase must not start or end with a special character.
	The special characters that can be used for the lockbox passphrase are:
	■ Tilde (~)
	■ At (@)
	■ Number (#)
	■ Percent (%)
	■ Exclamation (!)
	If you use an Exclamation (!) in the lockbox passphrase, enclose the passphrase within single quotes, for example, **'Test!1234567890'**. This is applicable only if the passphrase needs to be typed in the command line.
	Example:
	`./cstdriver -lockbox /opt/smarts-ncm/data/lockb.clb -passphrase 'Test!1234567890'`
	`-addHost linbgh130.lss.vmware.com`
	If you have not used an Exclamation (!) in the lockbox passphrase, then the lockbox passphrase need not be enclosed within single quotes, for example, **Test@1234567890** does not need to be enclosed within single quotes.
	Note Use single quotes to unlock the lockbox from the command line. Do not use single quotes during installation.

25	The installer prompts for answers to the security questions. Type the answers for the security questions and press **Enter**.
26	The installer prompts you to select an Encryption Key store option. Type a location where NCM should store the encryption key that is used to encrypt and decrypt data. The options are: ■ 1 for Standard Security – Key stored encrypted in a flat file ■ 2 for Advanced Security – Key stored in RSA Lockbox **Note** If you return to this window later during the installation process, the option you selected will be displayed in encrypted format (not in clear text).
27	The installer prompts for a database password. Type a password for Database. The password must contain minimum fifteen characters. The special characters that can be used for the database password are: ■ Tilde (~) ■ Exclamation (!) ■ At (@) ■ Number (#) ■ Percent (%) **Note** It is recommended that the password must not start or end with a special character.

Step	Action
28	The Summary window displays the product information (before installing), as well as the required disk space. Press **Enter** to start the installation. This portion of the installation may take several minutes. **Note** If there is not enough available disk space, the installer displays an error message until sufficient disk space is free. You can continue once enough disk space is available.
Device Driver Installer Procedures	
29	While the Device Driver installer is running, a progress bar displays the install status. This portion of the installation may take several minutes. **Note** During installation of the device drivers, the files in the custompackage directory that matches the files in the device drivers directory are listed. These files will override similar files in the device drivers directories. For example, if you have modified the file stdfuncs.inc for CiscoIOSRouter, it would be placed in the custom package directory and will override the same file in the /opt/voyence/package/cisco/ios directory.
After installing Combination server or Application server	
31	Add distributed system hosts to the lockbox for remote servers.

Lockbox utility

Lockbox utility provides increased security for data. The lockbox is a file that serves as a local repository for storing the passphrase which is used for encryption of sensitive data such as user credentials. The encryption algorithm is upgraded from Blowfish to AES. The lockbox file can be opened only on the machine on which it is created.

Lockbox utility provides more information for Lockbox utility functionalities.

Add distributed system hosts for remote servers (standard or advanced security)

Use the following steps to add distributed system hosts.

1 If you chose Standard Security mode during AS installation, copy **lockb.ekey** from [product directory]/data in the AS to [product directory]/data on the remote server (DS or Database).

2 If you chose Advanced Security mode during AS installation:

3 On the Application server, go to [Product directory]/bin directory.

4 Source the voyence.conf file

```
 source /etc/voyence.conf
```

5 Add distributed system hosts to the lockbox using the **cstdriver** utility:

```
./cstdriver -lockbox  [Product directory]/data/lockb.clb
-passphrase <passphrase> -addHost <FQDN of Database server>
```

```
./cstdriver -lockbox [Product directory]/data/lockb.clb
-passphrase <passphrase> -addHost <FQDN>
./cstdriver -lockbox [Product directory]/data/lockb.clb
-passphrase <passphrase> -addHost <FQDN of Device server>
```

6 Go to [Product directory]/data directory.

7 Copy the lockbox file to any directory on each of the distributed system hosts.

8 For example:

```
 scp lockb.clb Host2_DB_Server:/root/
 scp lockb.clb Host3_Device_Server:/root/
```

Import Network Configuration Manager Certificates for remote servers

For establishing a secure connection from Application server to remote Device server, you have to get the certificates from the Application server.

Follow these steps to get the certificates from Application server:

1 On a Linux server, run the command

```
# source /etc/voyence.conf
```

2 Go to **[Product directory]/conf** directory.

3 Copy the **bundle.p12** certificate file to remote Device server. For example:

```
scp bundle.p12 Host3_Device_Server:/root/
```

Next step, go to Export and import certificates for EDAA and Smarts Adapter.

Export and import certificates for EDAA and Smarts Adapter

For establishing a secure connection to the Network Configuration Manager server:

1 From the Network Configuration Manager Application or Combination server, export the self signed certificate from [Product Directory]/conf/voyence-ssl.keystore to a file using the steps:

2 source /etc/voyence.conf

3 $JAVA_HOME/bin/keytool -export -keystore [Product directory]/conf/voyence-ssl.keystore -alias selfsigned -file <CERTIFICATE>

To find the location of JAVA_HOME, type the command echo $JAVA_HOME. Ensure that JAVA_HOME is pointing to the right version of Java. For example, <<VOYENCE_HOME>>/java.

Note <CERTIFICATE> can be any name and it is the file that is created from the export.

Press **Enter** without entering a password.

4 Import the self signed certificate from the file <*CERTIFICATE*>.

```
$JAVA_HOME/bin/keytool -keystore $JAVA_HOME/jre/lib/security/cacerts -import -file
<CERTIFICATE> -alias selfsigned
```

5 Type the password **changeit** during the prompt.

6 This is the default password, unless otherwise modified.

7 Type **Yes** and click **Enter** when the **Trust the certificate** prompt appears.

To view the imported certificate, type:

```
$JAVA_HOME/bin/keytool -keystore $JAVA_HOME/jre/lib/security/cacerts -list -alias
selfsigned
```

Next step, install the Device server as described in *"Install a Device server using console installer" on page 95*.

Install a Device server using console installer

If you are installing a distributed server configuration, with separate Application server and Device servers, you must first install Network Configuration Manager on the Application server, and then install it on the Device servers.

Note Before installing Device servers, ensure the Application or Combination servers have the same date and time as the candidate Device server. If not, the Device server will not be able to register with the Application or Combination servers, and the installation will fail.

To install a Device server using the console-based installer, follow these steps:

Step	Action
1	Log into the server as the root user.
2	Type **bash install.sh –i console** to run the installer in the console-based installer mode, and press **Enter**. The command prompt screen appears: ■ Type **1**, and press **Enter** to install NCM Core product, and Device Drivers. The installer begins to load. The install.sh script checks to ensure that all the prerequisites for the Network Configuration Manager are installed. The script automatically installs any missing prerequisites if the prerequisites are located in the Utils directory. The **Core Setup Installer** begins to load.
Core Setup Installer Procedures	

Step	Action
3	The introduction to the installer appears. Press **Enter** to continue.
4	The License Agreement appears. Read the license agreement. Press **Enter**, and continue to press **Enter** to move through each page of the license agreement until you reach the final page.
5	On the final page of the license agreement, type Y, and press **Enter** to accept the terms of the license agreement.
6	The installer prompts you to select a server configuration. Enter **3**, and press **Enter** to select **Device server** as your configuration type.
7	The installer prompts you to choose an install folder. Press **Enter** to accept the default, or enter a location for the install folder. This is the location where Network Configuration Manager will be installed.
8	**Note** This step only appears if the httpd.conf directory is not in the default location. The installer prompts you for the directory where httpd.conf is located. Press **Enter** to accept the default, or type the **location** of the httpd.conf file. This is where the Apache configuration file httpd.conf is located.
9	**Note** This step only appears if the Java directory is not in the default location. The installer prompts you for the directory where Java is located. Press **Enter** to accept the default, or type the **location** of the Java directory. This is the location where the Java application is installed.
10	**Note** This step only appears if the Tomcat directory is not in the default location. The installer prompts you for the directory where Tomcat is located. Press **Enter** to accept the default, or type the **location** of the Tomcat directory. This is the location where the Tomcat application is installed.
11	The installer prompts you for the Application server IP. Enter an **IP Address** for the Application server, and press **Enter**. If you are installing Device server with a Cluster installation, then enter an **IP Address** for the active Network Configuration Manager Application server cluster, and press **Enter**. The Device servers will be set to the appropriate node when the clustered Application server becomes active. Do not type the virtual IP address of the cluster.
12	The installer prompts you for the Device server alias. Press **Enter** to accept the default, or enter an **Alias** for the Combination server. This alias appears in the System Administration portion of Network Configuration Manager. This alias must not contain spaces or special characters.
13	The installer prompts you to import root CA certificates. If you have any root CA certificates to import, provide the path for certificate root CA certificate file and then press **Enter**.
14	The installer prompts for Certificate file location. Provide the path for the certificate file **bundle.p12** and press **Enter**.

Step	Action
15	The installer prompts for a password for Certificate. Type the same password that you entered while installing Application server and press **Enter**.
16	**Note** You must perform this step irrespective of the mode of security you selected during the installation. The installer prompts for lockbox file location. Provide the path to the lockbox file **lockb.clb** that was copied earlier and press **Enter**.
17	The installer prompts for a database password. Type the same password that you entered while installing Application or Database server and press **Enter**.
18	The Summary window displays the product information (before installing), as well as the required disk space. Press **Enter** to start the installation. This portion of the installation may take several minutes. When complete, the Device Driver Installer begins to load.
Device Driver Installer Procedures	
19	While the Device Driver installer is running, a progress bar displays the install status. This portion of the installation may take several minutes. The installer displays the installation complete message. **Note** During installation of the device drivers, the files in the custompackage directory that matches the files in the device drivers directory are listed. These files will override similar files in the device drivers directories. For example, if you have modified the file stdfuncs.inc for CiscoIOSRouter, it would be placed in the custom package directory and will override the same file in the /opt/smarts-ncm/package/cisco/ios directory.
20	If you had chosen Standard Security mode during AS installation, copy **lockb.ekey** from [product directory]\data in the AS to [product directory]\data in DS. Change ownership of the file to ncm:voyence.

Note NCM stops *firewalld/iptables* during installation to avoid interruption of the ports used by NCM. You will observe communication issues, if ports are interrupted. If required the *firewalld/iptables* needs to be manually started post installation.

Next step, go to Chapter 4 Post-Installation procedures.

Install Network Configuration Manager using silent installer

The Network Configuration Manager installer allows you to supply a configuration file containing the variables necessary for an installation, also known as a silent installation.

A sample configuration file is supplied in the following directory of the Network Configuration Manager distribution: **silent-install.properties** available in the Utils directory.

Creating the configuration file for a silent installation

Note Before you can run a silent installation, you must create a configuration file that the installer uses to complete your installation.

To create a configuration file, follow these steps:

Step	Action
1	Copy the **sample configuration file** from the distribution (silent-install.properties) to a **directory** on the server where you are installing Network Configuration Manager.
2	Use the **vi** command to modify this file.
3	Define each of the properties in this file for your server type, according to the table below. **Note** Errors occur during installation if all required properties do not contain a value.
4	**Save** your changes to the file. You are now ready to install Network Configuration Manager in silent mode.

Configuration parameters

Property	Description	Applicable server configurations
API_VERSION	Defines the versions of the API to install. **Note** For maximum compatibility, it is highly recommended that 9.1 be selected. (space delimited if entering more than one version)	AS, CS
APPLICATION_SERVER_IP	If you are installing a Device server, this property defines the IP address of the associated Application server. The Application server must be installed, running, and available over the network before installing the Device server. If you are not installing a Device server, any value entered for this property is ignored.	DS
CERT_FILE	Defines the location of the Certificate file. CERT_FILE=<FilePathFull>	DS
COMPANY_NAME	Defines the company name that displays on the main screen of the application.	AS, CS
CRED_MODE	Defines the Privilege Password Mode for Network Configuration Manager. Valid values are the following: **Single-Level**—Network Configuration Manager users accustomed to the previous credentials system should select this option. **Multi-Level**—This mode allows multiple leveled privileged passwords to be created and associated within the Network Configuration Manager application. Note that this setting is permanent.	AS, CS

Property	Description	Applicable server configurations
DATABASE_PASSWORD	Database password. Type a password for the database. The password must contain at least: ■ One letter in upper case ■ One letter in lower case ■ One special character ■ One numerical ■ Minimum fifteen characters The special characters that can be used for the database password are: ■ Tilde (~) ■ Exclamation (!) ■ At (@) ■ Number (#) ■ Percent (%) A special character must be preceded by a backlash (\ ) in the password. **Note** It is recommended that the password must not start or end with a special character.	AS, CS, DB
DIVISION	Defines the division name that displays on the main screen of the application. This is optional, and *none* is a valid value.	AS, CS
FROM_ADDRESS	Network Configuration Manager has the ability to send email notifications to users. This property defines the From address for Network Configuration Manager notification emails.	AS, CS
HTTPD_CONF_DIR	Defines the directory in which the httpd.conf Apache configuration file resides on the server.	AS, DS, CS
JAVA_INSTALL_DIR	Defines the directory in which Java is installed.	AS, DS, CS
KEY_STORE	Value:Standard Security/Advanced Security Encryption Key store option to specify where NCM should store the encryption key that is used to encrypt or decrypt data.	AS, CS
LICENSE_FILE	Defines the location of the license file used for new installations. If you are upgrading, this property is ignored.	AS, CS
LOCKBOX_FILE	Defines the location of the lockbox flle or eKey file. LOCKBOX_FILE=<FilePathFull>	DS

Property	Description	Applicable server configurations
PKCS_PASSWORD	Certificate Password The password must contain at least: - One letter in upper case - One letter in lower case - One special character - One numerical - Minimum fifteen characters **Note** The password must not start or end with a special character. Special characters that can be used for the certificate password are: - Tilde (~) - Exclamation (!) - At (@) - Number (#) - Percent (%) A special character must be preceded by a backlash (\ ) in the password.	AS, CS, DS
ROOT_CERT_LIST	List the files that contain the root CA certificates. This is only necessary for DS and CS configurations that use either a third-party certificate or Cisco RME integration. Use comma as delimiter if you entering more than one file.	AS, DS, CS
SECURITY_ANSWER_ONE	Defines the answer for the question “What is your Customer Site ID Number?”	AS, CS
SECURITY_ANSWER_THREE	Defines the answer for the question “What is the Software Licensing Contract Number?”	AS, CS
SECURITY_ANSWER_TWO	Defines the answer for the question “What is the Customer Service Support Phone Number?”	AS, CS
SERVER_ALIAS	Defines a symbolic name for a device or Combination server. This server name displays in the System Administration portion of Network Configuration Manager. This name cannot contain spaces or special characters. If you are not installing a combination or Device server, any value entered for this property is ignored.	DS, CS
SERVER_CONFIG	Defines the type of server being installed. Valid values include the following: **AS –** Application server **DB–** Database server **DS –** Device server **CS –** Combination server	AS, DB, DS, CS
SMTP_SERVER	Defines the outbound SMTP mail server FQDN or IP address, used for sending email notifications.	AS, CS
TOMCAT_INSTALL_DIR	Defines the directory in which Tomcat is installed.	AS, DS, CS

Property	Description	Applicable server configurations
USER_INSTALL_DIR	Installation directory for Network Configuration Manager.	AS, DS, CS
USER_SUPPLIED_PASSWORD	Lockbox passphrase The passphrase must contain at least: - One letter in upper case - One letter in lower case - One special character - One numerical - Minimum fifteen characters **Note** It is recommended that the passphrase must not start or end with a special character. The special characters that can be used for the lockbox passphrase are: - Tilde (~) - At (@) - Number (#) - Percent (%) - Exclamation (!) A special character must be preceded by a backlash (\ ) in the password.	AS, CS
W4N_IP	Defines the IP address for the Watch4net server.	AS, CS, DB
W4N_SKIP	Value: Yes/No Set this parameter to **Yes** to configure the Network Configuration Manager Reporting SolutionPack. If you set **Yes**, you must provide the Watch4net server IP address for the property W4N_IP.	AS, CS, DB

Installing in silent mode

To install in silent mode, follow these steps:

Step	Action
1	Log into the server as the root user.
2	Type **bash install.sh –i silent -f <configuration file> -m <NCM_COMPONENT>** to run the installer in the silent installer mode, and press **Enter**. where NCM_COMPONENT refers to: ■ NCM_CORE - Installs the NCM Core product, and Device Drivers ■ ADAPTERS - Installs the NCM Smarts Adapters ■ NCM_COMPLETE - Installs the NCM Core product, and Adapters **Note** The path to the silent configuration file must not contain any spaces. The file should be referenced with a full path that does not contain spaces (for example, -f /opt/voyence/silent-install.properties). The installer begins to load. The install.sh script checks to ensure that all the prerequisites for the Network Configuration Manager are installed. The script automatically installs any missing prerequisites if the prerequisites are located in the Utils directory. The installer does not require any user interaction. Once it completes, a message displays indicating the installation is complete, and you are returned to the shell prompt. If the installer is unable to complete the installation, an error message is saved in the *[Product directory]/logs/* directory.

Uninstallation procedures (Linux platform)

3

Read the following topics next:

- Summary of uninstall tasks
- Uninstalling the Network Configuration Manager core product
- Uninstalling the Network Configuration Manager Device Drivers

Summary of uninstall tasks

The recommended order of uninstall tasks is as follows:

Step	Task
1	To uninstall the entire Network Configuration Manager product: 1 Run the Core Product uninstaller using the steps in Uninstalling the Network Configuration Manager core product . This uninstalls Network Configuration Manager, Device Drivers, Integration modules, and the RSA Token Service. Skip this step if you do not want to uninstall the main Network Configuration Manager product.
2	To uninstall the Network Configuration Manager Device Drivers: Run the Device Driver uninstaller using the steps in *“Uninstalling the Network Configuration Manager Device Drivers” on page 115*. Skip this step if you do not want to uninstall the Network Configuration Manager Device Drivers. **Note** You do not need to complete this step if you completed step 1.

Uninstalling the Network Configuration Manager core product

Note Running the core product uninstaller will uninstall Network Configuration Manager, as well as the Network Configuration Manager Device Drivers, and Integration modules.

The Network Configuration Manager uninstaller is named Uninstall_Network Configuration Manager, and is located in **[Product Directory]/software/Uninstall_Core/**.

To uninstall the Network Configuration Manager core product, follow these steps:

Step	Action
1	Log into the server as the root user.
2	Type **cd [Product Directory]/software/Uninstall_Core/** to navigate to the uninstall directory.
3	Type **bash Uninstall_ VMware_Smart_Network_Configuration_Manager** to run the uninstaller in the console mode, and press **Enter**.
4	The introduction to the uninstaller appears. Press **Enter** to start the uninstall process. This portion of the uninstaller may take several minutes. When the uninstaller completes, the program exits.

Uninstalling the Network Configuration Manager Device Drivers

The Network Configuration Manager uninstaller is named Uninstall_Network Configuration Manager_Device_Drivers, and is located in **[Product Directory]/software/Uninstall_Device_Drivers/**.

To uninstall the Network Configuration Manager Device Drivers, follow these steps:

Step	Action
1	Log into the server as the root user.
2	Type **cd [Product Directory]/software/Uninstall_Device_Drivers/** to navigate to the uninstall directory.
3	Type **bash Uninstall_ VMware_Smart_Network_Configuration_Manager _Device_Drivers** to run the uninstaller in the console mode, and press **Enter**.
4	The introduction to the uninstaller appears. Press **Enter** to start the uninstall process. This portion of the uninstaller may take several minutes. When the uninstaller completes, the program exits.

Post-Installation procedures

4

Read the following topics next:

- Configuring Watch4net server
- Launching Watch4net user interface from Network Configuration Manager
- Enabling CAS configuration for EDAA URI
- Healthcheck updates
- Database password change information
- Error handling
- Multi-Level cut-through mode configuration
- Configuring Windows to accept cut-thru with default Telnet Client
- Enable/disable auto-login features
- Enable data on User Activity screen (Linux)
- Client-side required configuration to disable SSLv3
- Client-side installation
- Client-side startup
- Configuring the sysadmin user’s email address
- Setting up the profile
- Enabling SAML authentication
- Installing the sysadmin console (Linux)
- Enabling Syslog messages in RHEL 8
- Launching MSA GUI

Configuring Watch4net server

Perform these steps to configure Watch4net server post Network Configuration Manager installation:

For Linux

1 Open the [Product directory]/db/controldb/data/pg_hba.conf file for editing.

2 Add the following line at the end of the file:

```
host     all     all     <Watch4net IP address>/32    md5
```

3 Save, and exit the pg_hba.conf file.

4 Restart **controldb** service using the command:

```
service controldb restart
```

Launching Watch4net user interface from Network Configuration Manager

If you had not specified the Watch4net host information during NCM installation and would like to specify it as a post-installation procedure, perform the steps below. If you need to update the Watch4net host information, modify the same file, but search for the current IP address of Watch4net host and update it with the new value.

To launch the Watch4net user interface from Network Configuration Manager welcome screen or dashboard, you have to manually update the Watch4net IP address in the powerup.jnlp file.

Perform these steps to update the Watch4net IP address in the powerup.jnlp file:

For Linux

1 Open the $VOYENCE_HOME/ncmcore/webapps/voyence/powerup.jnlp file for editing.

2 Replace the text $W4N_IP$ with Watch4net IP address.

3 Type the port number of the Watch4net installation.

Default port is 58080.

4 Save, and exit the powerup.jnlp file.

5 Open the [Product directory]/ui/html/index.html file for editing.

6 Replace the text $W4N_IP$ with Watch4net IP address.

7 Type the port number of the Watch4net installation.

8 Restart the **ncm-as** service using the command:

```
service ncm-as restart
```

Enabling CAS configuration for EDAA URI

The EMC Data Access API (EDAA) provides an MSA URI and interface that is used by Watch4net reporting. By default NCM installs a CAS server and the EDAA URI is authenticated using the CAS server. The EDAA server certificate is available in the [product directory]\conf directory and is required to be imported to the keystore,

To establish a secure connection between Network Configuration Manager EDAA and the CAS server, do the following:

In Linux

1. Import the MSA certificate:
2. source /etc/voyence.conf
3. $JAVA_HOME/bin/keytool -keystore $JAVA_HOME/jre/lib/security/cacerts -import -file <PRODUCT_HOME>/conf/server.crt -alias trustmsa
4. Type the password **changeit** during the prompt.
5. This is the default password, unless otherwise modified.
6. Type Yes and click Enter when the prompt **Trust the certificate** appears.

   To view the imported certificate, type:

   ```
   $JAVA_HOME/bin/keytool -keystore $JAVA_HOME/jre/lib/security/cacerts -list -alias trustmsa
   ```
7. Restart ncm-msa service:

   ```
   service ncm-msa restart
   ```

Healthcheck updates

The location for the health check status html has changed. When the health check is started, the status file is located at https://<server ip>/HealthCheckStatus.html.

Database password change information

To change the password for the database, run the following command from the [Product directory]/tools directory:

```
./password-change.pl -c database <Current password> <New password>
```

The New password must contain at least:

- One letter in upper case
- One letter in lower case
- One special character

- One numerical
- Minimum fifteen characters

The special characters that can be used for the database password are:

- Tilde (~)
- Exclamation (!)
- At (@)
- Number (#)
- Percent (%)

This command should be run on each server on distributed installs to maintain connectivity to the database for each server. The **vcmaster** services should be restarted (service *vcmaster* restart) after the database password has been changed.

Error handling

The Network Configuration Manager installers have improved internal error handling over previous releases. If an error is encountered, the following events occur:

Note For a list of error messages and their solutions, see the VMware Smart Assurance Network Configuration Manager Troubleshooting Guide.

Step	Action
1	The installation complete screen states that serious errors have occurred, and no longer displays a success message.
2	The error is captured in the install log file.
3	The install.sh script exits, without continuing to the next installer.

Installer log files

Each installer will generate two log files regardless if there were errors during the install. The log files are created in the [Product Directory]/logs directory or, if no [Product Directory] was specified, the /logs directory.

- component_install.log (also referred to as the "install" log)

  For example, the Core installer generates a *NCM-10.1.6.0-install.log* file.
- component_debug.log (also referred to as the "debug" log)

  For example, the Core installer generates a *NCM-10.1.6.0-debug.log* file.

The **install log file** contains a high level overview of the installation. If an error message is displayed at the end of an installer, open the install log file and search for **ERROR**. This will give a high level description of the error.

The **debug log file** contains the *stdout*, *stderr*, and e*xit code* from every operation in the installer. The debug log file contains a large amount of information and is often overwhelming. It is advisable to start with the install log file to find any installation errors.

Note If you are installing using Silent Mode and the install fails, only the *core_debug.log* file will be generated.

Multi-Level cut-through mode configuration

To configure Network Configuration Manager for Multi-Level Cut-Through Mode, follow these steps:

Step	Action
1	Create an empty file named **cutthruonlylevelmode** in the [Product Directory]/data/devserver/cm/cache directory on each Device Sever.
2	Type **touch cutthruonlylevelmode**.
3	Restart the *voyence* process using the **/etc/init.d/voyence restart** command.

Configuring Windows to accept cut-thru with default Telnet Client

To allow Windows to use the default Telnet Client to accept cut-thrus, the Telnet Client feature must be enabled on the Network Configuration Manager client computer.

Step	Action
1	Log onto the Network Configuration Manager client.
2	Navigate to **Start > Control Panel > Programs and Features >Turn Windows Features On or Off**.
3	Check **Telnet Client.**

Enable/disable auto-login features

If enabled, you can have Network Configuration Manager remember your User ID and Password to automatically log you into the system.

Step	Action
1	Login to the Network Configuration Manager Server.

2	Navigate to this location: C:\smarts-ncm\ncmcore\webapps\voyence.
3	Open the file **powerup.jnlp**. Go to the end of the file, and change the value under <property name=feature.autoLogin.enabled value="**false**"/>" to "**true**".
4	**Save** the file.
5	In a web browser, launch the Network Configuration Manager UI.
6	Login using approved credentials and select the check box to **save credentials**.
7	Exit the Network Configuration Manager UI.
8	Re-launch the Network Configuration Manager UI. It automatically logs you in with the saved credentials.

Enable data on User Activity screen (Linux)

On a Linux server, the Network Configuration Manager User Activity tab does not get populated with data unless the permissions and ownership of the voyence-audit.log are changed.

Step	Action
1	Go to the following directory: **$VOYENCE_HOME/ncmcore/logs**
2	Use the following command to change the permissions: **chmod 644 voyence-audit.log**
3	Use the following command to change the ownership: **chown ncm:voyence voyence-audit.log**

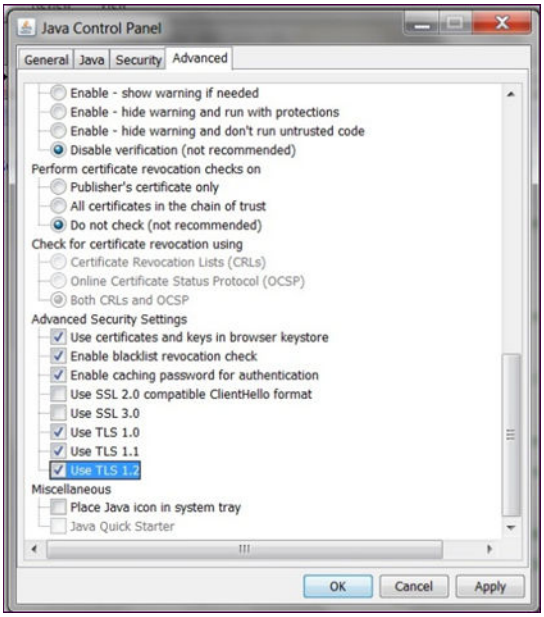
Client-side required configuration to disable SSLv3

On a client machine that will access the Network Configuration Manager, SSLv3 must be disabled. On each client machine, disable SSLv3 in the Java Console and in the browser using the following steps.

Step	Action
1	Log on to the client machine.
2	Open **control panel >java**.
3	Click the Advancedtab.

4 Under **Advanced security settings**:

- Uncheck the SSLV3 box.
- Check the TLSv1, TLSv1.1 and TLSv1.2 boxes.



Java Control Panel

○ Enable - show warning if needed
○ Enable - hide warning and run with protections
○ Enable - hide warning and don't run untrusted code
● Disable verification (not recommended)

Perform certificate revocation checks on
○ Publisher's certificate only
○ All certificates in the chain of trust
● Do not check (not recommended)

Check for certificate revocation using
○ Certificate Revocation Lists (CRLs)
○ Online Certificate Status Protocol (OCSP)
● Both CRLs and OCSP

Advanced Security Settings
☑ Use certificates and keys in browser keystore
☑ Enable blacklist revocation check
☑ Enable caching password for authentication
□ Use SSL 2.0 compatible ClientHello format
□ Use SSL 3.0
☑ Use TLS 1.0
☑ Use TLS 1.1
☑ Use TLS 1.2

Miscellaneous
□ Place Java icon in system tray
□ Java Quick Starter

5 Open the browser and perform the following steps.

On Internet Explorer:

From the Startmenu, open Internet Options.

Click the Advancedtab.

Uncheck Use SSL 3.0.

Click OK.

On Mozilla Firefox version 34

SSLV3 is disabled by default.

On Mozilla Firefox versions other than 34

Type about:configin the address bar and press Enter.

Set the value of security.tls.version.min to 1.

Note Alternatively, install the SSLVersion Control extension available from Mozilla here:`https://addons.mozilla.org/en-US/firefox/addon/ssl-version-control/`

On Safari

Apple released Security Update 2014-005, which disables CBC-mode ciphers in coordination with SSLv3. The patch is available for Mac OS Mavericks, Mountain Lion, and Yosemite here: `https://support.apple.com/en-us/HT203107`.

After you apply the update, no action is needed on your part.

Client-side installation

Once the server installations are completed, you need to install Network Configuration Manager UI Client to launch the Network Configuration Manager UI.

Note

- If you want to continue with Java 8, then following instructions are not required and you can still launch NCM UI using older way of JNLP method, for more information refer, Client-side startup section.
- Upgrade of NCM UI Installer is not supported, you need to uninstall the older version of NCM UI and install the new version.

NCM UI Installation (Windows)

This section describes how to install and launch Network Configuration Manager UI Client on Windows machine. If you want to use Java 11, for NCM UI, then follow the below instructions.

To install NCM UI Client:

Prerequisites

NCM UI Client executable (.exe for Windows) file is present in NCM_UI folder.

Procedure

1. Double-click the NCM UI Client executable file or binary file, present in the NCM_UI folder.

   The introduction application window appears.

2. Click **Next**.

   The **Choose Install Folder** application window appears. You are prompted to choose the Install Folder. Accept the default location, or click **Choose** and select another location. This is the location where NCM UI will be installed.

3. Click **Next**.

   Pre-Installation Summary application window appears. Review information about the install. The Summary window displays the product information, and the required disk space.

4. Click **Install**.
5. Click **Done**, to complete the installation.

What to do next

Double click on **NCM_Launcher.bat** present under <ncm-ui Installed Location> to launch the NCM UI.

NCM UI Installation (Linux)

This section describes how to install and launch Network Configuration Manager UI Client on Linux machine. If you want to use Java 11, for NCM UI, then follow the below instructions.

To install NCM UI Client on Linux machine:

Prerequisites

NCM UI Client binary (.bin for Linux) file is present in NCM_UI folder.

Procedure

- Invoke `.bin` file (`./<binary filename>`) and follow the prompts.

What to do next

Goto Installed directory (for example: `/opt/ncm-ui`) and invoke `./NCM_Launcher.sh`, to launch the NCM UI

Note In Linux, to launch UI client and also to install in GUI mode, the VNC server or any equivalent server has to be configured. Post which user needs to launch with VNC client.

NCM UI Uninstallation Procedure

This section illustrates, how to uninstall NCM UI (Windows and Linux).

NCM UI Linux Uninstallation

1. Goto `<Installed Directory>/Uninstall_VMWare_Smart_Assurance_Network_Configuration_Manager_10.1.6.0_UI`.
2. Invoke `./Uninstall_VMWare_Smart_Assurance_Network_Configuration_Manager_10.1.6.0_UI` to uninstall NCM UI.

NCM UI Windows Uninstallation

1. Goto installed folder (for example: `C:\Program Files\ncm-ui\Uninstall_VMWare_Smart_Assurance_Network_Configuration_Manager_10.1.6.0_UI`)
2. Double-click on `Uninstall_VMWare_Smart_Assurance_Network_Configuration_Manager_10.1.6.0_UI.exe`, to uninstall NCM UI.

Note

- In login window, user must give correct IP/host name of NCM while launching. UI Client must be relaunched in case user provides invalid IP/host of NCM.
- After login to the NCM UI, in help window, NCM build number and OS version are not available.

Client-side startup

Once the server installations are completed, you are ready to open Network Configuration Manager.

Step	Action
1	Type the **URL** that has been provided for your company. If you need assistance, contact your System Administrator for the server where the application was setup. At the login screen, enter your username and password, then click **Ok**. The default username/password is sysadmin/sysadmin.
2	Ensure that Java Runtime is installed on your local machine. Click the **click here** link to download and install the correct version. When the installation of Java Runtime is finished, **refresh** your browser window. On the first execution of Network Configuration Manager, a security warning window appears.
3	Click **Start**. The Login window opens.
4	Continue to login by entering a **User ID** and **Password** (as described in the Network Configuration Manager Online User's Guide). To access the procedures in the Online User's Guide: ■ From the Network Configuration Manager launch window, click **Help** on the tool bar, and select **Help Contents** from the drop-down menu. The Online User's Guide displays. ■ From the Table of Contents, select Getting Started - Accessing Network Configuration Manager. Click Logging in to Network Configuration Manager.

Note Client-side startup is applicable only for older way of client launch, i.e. using powerup.jnlp.

Configuring the sysadmin user's email address

When installing Network Configuration Manager, mail must be allowed to relay through the internal mail servers from the sysadmin user's account.

To configure the sysadmin user's email address for Network Configuration Manager, follow these steps:

Step	Action
1	Open a browser and type the **URL** used to access Network Configuration Manager. (for example **https://<IP address>**)
2	Select **System Administration** from the Tools menu. The System Administration window opens.
3	Select **System Administration -> Global -> User Management -> System Users** from the navigation pane.
4	Select the **sysadmin** user, and click the **Edit** button. The Edit User window opens.

5	Enter a valid email address in the *Email* field, and click **Ok**. The email address must be valid for your domain, for example sysadmin@mycompany.com.
6	Click the **Close** button to exit the System Administration window.

Setting up the profile

When completing System Administrative tasks at the command line interface, you must first source the profile to set up your environment. The command to source the profile is:

. /etc/voyence.conf

This command is used to expand the required environmental variable.

Enabling SAML authentication

If enabled, you can login to Network Configuration Manager using Security Assertion Markup Language (SAML) authentication.

To enable SAML authentication in Network Configuration Manager, follow these steps:

Step	Action
1	Log into the server as the root user.
2	Navigate to the **[Product Directory]/tools/saml-util** directory. **Note** Replace [Product Directory] with the path to the directory where Network Configuration Manager is installed. For example, **VOYENCE_HOME/tools/saml-util** directory.
3	Type **perl enableSaml.pl** to run the enable SAML utility, and press Enter.
4	After successful execution of the preceding script, the **samlsysadmin** user is created in NCM under **System Administration > User management > System Users**. For reference, the content of the sample **SamlAssertion.xml** file has been provided with this section.
5	Modify the sample **SamlAssertion.xml** file as follows to add the user name that exists in NCM: <saml:NameID SPNameQualifier="http://sp.example.com/demo1/metadata.php" Format="urn:oasis:names:tc:SAML:2.0:nameid- format:transient">samlsysadmin</saml:NameID>
6	Modify the sample **SamlAssertion.xml** file as follows to add NotBefore, NotOnOrAfter dates, so that NCM allows the user to log in if the date is between a valid range: <saml:Conditions NotBefore="2016-12-22T15:41:54.000Z" NotOnOrAfter= "2019-02-04T15:41:54.000Z">
7	Encode to base64 format, and then perform urlencode the **SamlAssertion.xml** content. For reference, the content of the sample **SamlAssertion.xml** file has been provided with this section.

8	Modify the IP address to point to the NCM AS and generate the **powerup.jnlp** file using the encoded string. Execute the following command from any Linux server or from command prompt if you have curl:
	`curl -k -X POST https://<NCM AS IP address>:8880/voyence/launchClient?`
	`samlAssertion=encoded-string > powerup.jnlp`

9	Copy the **powerup.jnlp** file to your client machine from where you want to launch NCM, and then launch NCM UI.
10	NCM is launched successfully without asking the user to enter credentials.

Following is the content of the sample SamlAssertion.xml file:

```
<?xml version="1.0"?>
-<samlp:Response InResponseTo="ONELOGIN_4fee3b046395c4e751011e97f8900b5273d56685"
Destination="http://sp.example.com/demo1/index.php?acs" IssueInstant="2016-12-20T01:01:48Z"
Version="2.0" ID="_8e8dc5f69a98cc4c1ff3427e5ce34606fd672f91e6"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
<saml:Issuer>http://idp.example.com/metadata.php</saml:Issuer>
-<samlp:Status>
<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
</samlp:Status>
-<saml:Assertion IssueInstant="2016-12-19T01:01:48Z" Version="2.0"
ID="_d71a3a8e9fcc45c9e9d248ef7049393fc8f04e5f75" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<saml:Issuer>http://idp.example.com/metadata.php</saml:Issuer>
-<saml:Subject>
<saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
SPNameQualifier="http://sp.example.com/demo1/metadata.php">samlsysadmin</saml:NameID>
-<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData
InResponseTo="ONELOGIN_4fee3b046395c4e751011e97f8900b5273d56685" Recipient="http://
sp.example.com/demo1/index.php?acs" NotOnOrAfter="2024-01-18T06:21:48Z"/>
</saml:SubjectConfirmation>
</saml:Subject>
-<saml:Conditions NotOnOrAfter="2019-02-04T15:41:54.000Z"
NotBefore="2016-12-22T15:41:54.000Z">
-<saml:AudienceRestriction>
<saml:Audience>http://sp.example.com/demo1/metadata.php</saml:Audience>
</saml:AudienceRestriction>
</saml:Conditions>
-<saml:AuthnStatement SessionIndex="_be9967abd904ddcae3c0eb4189adbe3f71e327cf93"
SessionNotOnOrAfter="2024-07-17T09:01:48Z" AuthnInstant="2016-12-19T01:01:48Z">
-<saml:AuthnContext>
<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</
saml:AuthnContextClassRef>
</saml:AuthnContext>
</saml:AuthnStatement>
-<saml:AttributeStatement>
-<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="uid">
<saml:AttributeValue xsi:type="xs:string">samlsysadmin</saml:AttributeValue>
</saml:Attribute>
-<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="mail">
<saml:AttributeValue xsi:type="xs:string">test@example.com</saml:AttributeValue>
</saml:Attribute>
-<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="eduPersonAffiliation">
<saml:AttributeValue xsi:type="xs:string">users</saml:AttributeValue>
<saml:AttributeValue xsi:type="xs:string">examplerole1</saml:AttributeValue>
```

```
</saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>
```

Installing the sysadmin console (Linux)

On Linux, you can install the sysadmin console tool.

To install the sysadmin console, follow these steps:

Step	Action
1	Log into the Linux server.
2	Navigate to the **[Product Directory]/tools** directory. **Note** Replace [Product Directory] with the path to the directory where Network Configuration Manager is installed.
3	Type **perl install_sysadmin.pl** and press Enter.

Enabling Syslog messages in RHEL 8

Follow below steps to enable Syslog messages in RHEL 8 Server.

Procedure

1 Open */etc/rsyslog.conf* file.

2 Uncomment below lines for UDP:

```
#module(load="imudp") # needs to be done just once
#input(type="imudp" port="514")
```

3 Uncomment below lines for TCP:

```
#module(load="imtcp") # needs to be done just once
#input(type="imtcp" port="514")
```

4 Restart *rsyslog* service using following command:

`systemctl restart rsyslog`.

Launching MSA GUI

MSA will be installed, once application server installation is completed.

Procedure

1 To access MSA GUI, go to the URL:

```
https://[SERVER-IP]:9443/ncm-msa/msa/ncm
```

Where, [SERVER-IP] is usually the Network Configuration Manager server IP.

2 Provide the following default credentials:

- Login ID: `msa-user`
- Password: `sysadmin`

Note Ensure that, you launch the MSA in Internet explorer browser only. Supported Internet Explorer versions are 10 and 11.

Cluster installation

5

Read the following topics next:

- Overview
- Software Requirements
- Configuration Requirements
- Installing Network Configuration Manager with the Cluster installation
- Operating the Network Configuration Manager Cluster
- Restoring from a Backup
- Uninstalling Network Configuration Manager

Overview

This chapter is intended as a general guide for configuring a Network Configuration Manager Cluster Server. Additional hardware configurations are possible. The instructions may differ slightly between hardware vendors.

Also covered within this chapter are the specific procedures in terms of interaction with Network Configuration Manager. However, it is advisable that you familiarize yourself with the official Red Hat Cluster Suite documentation.

The Red Hat Cluster Suite documentation is available for Red Hat Enterprise Linux, in its entirety, at **http://www.redhat.com/docs/manuals/csgfs/browse/rh-cs-en/**.

Software Requirements

The following software must be installed on the server prior to installing Network Configuration Manager.

- Red Hat Cluster Suite (RHEL 6 x86_64) or higher is required to properly run Network Configuration Manager in a clustered environment.

Configuration Requirements

Installing the Fibre Channel Cards

Follow these steps to install the Fibre Channel Cards prior to installing Red Hat Enterprise Linux.

Step	Task
1	Install the **Fibre Channel card** (following the manufacturer's instructions).
2	Attach the **Fibre Channel Shortwave cable** to the HBA card in the server, and the disk array (or Fibre switch).
3	Disable the **ports** on the Fibre switch.
4	Repeat these steps for **each cluster** member.

Installing Network Configuration Manager with the Cluster installation

Follow these steps to install Network Configuration Manager with the Cluster module.

Step	Task
1	Obtain both the Network Configuration Manager Installer and the Network Configuration Manager Cluster Module installer.
2	Place these files onto the **server**.
3	Create the [Product directory] directory using: **mkdir [Product directory]**
4	Mount the shared disk array device to [Product directory] using: **mount <device> [Product directory]** **For example:** mount /dev/sdb1 [Product directory] **Note** Ensure you have access to Installing Network Configuration Manager on Linux to complete the next step.
5	Ensure that SELinux is **disabled**.
6	Install Tomcat on the shared partition. If you are using the install.sh script to install the product, use the **-b <shared mount point>** argument to automatically install Tomcat under the shared partition. For example: ./install.sh -b /opt/smarts-ncm
7	Run the **Network Configuration Manager installer** as described in Chapter 2 Installation procedures (Linux platform).
8	When the installation is complete, run the **Network Configuration Manager Cluster Module** installer using one of the following commands: For the Console Interface mode use: ./**NCM_x_x_x_xxx_Cluster_linux-x64.bin** –i console For the GUI Interface mode use: ./**NCM_x_x_x_xxx_Cluster_linux-x64.bin** –i gui

9	If you are not installing the first server in the cluster, skip this step, and proceed to **step 10**. If you are installing the first server in the cluster, run the following command to **delete the files** from the shared storage, so the second server can successfully install on that same storage device. rm –rf [Product directory]/* **Note** Only remove the contents of the [Product directory]. Do not delete the directory itself, as it will be the mount point.
10	For Application server installations, modify the $VOYENCE_HOME/ncmcore/webapps/voyence/powerup.jnlp file, and change the **IP address** (that appears several times in that file) to the virtual IP address of the cluster. You can accomplish this with a global search and replace.
11	Unmount [Product directory] using: **umount [Product Directory]** **Note** If the error message “device is busy” displays when attempting to unmount [Product directory], first find and stop the processes that are running in the directory using the lsof [Mount Point] command, and then run the umount [Product Directory] command.
12	Repeat **steps 1 through 9** for each server in the cluster.

Validating the UNIX User ID and Group ID numbers

When installing Network Configuration Manager on a cluster environment, the UNIX User ID numbers and the UNIX Group ID numbers must be **identical** on each Application servers.

Follow these steps to validate the UNIX User ID and Group ID numbers.

Step	Task
1	Open the **/etc/passwd** file on all the Application servers.
2	Verify the **UNIX User ID** numbers for **pgdba** and **tomcat** match for all Application servers.
3	Close the **/etc/passwd** files.
4	Open the **/etc/group** file on all the Application servers.
5	Verify the **UNIX Group ID** numbers for **pgdba**, **tomcat**, and Network Configuration Manager match for all Application servers.
6	Close the **/etc/group** files.

Operating the Network Configuration Manager Cluster

The **vc_cluster service script** controls the mounting, httpd, controldb, controldaemon, and Network Configuration Manager processes. This service is managed through the Red Hat Cluster Suite.

Note Do not manually manage (start/stop) services from Linux. Allow Red Hat Cluster Suite to start/stop the services.

Follow these steps to operate the Network Configuration Manager Cluster.

Step	Task
1	Start the Cluster Services on Red Hat Enterprise Linux by running the following commands in the order shown: ■ service cman start ■ service rgmanager start
2	Check the cluster status with the following command: `clustat`
3	If you need to *manually start* the cluster service, use the following command: clusvcadm –e <Cluster Service Name>
4	If you need to *manually stop* the vc_cluster / controldb_cluster service, use the following command: clusvcadm –d <Cluster Service Name>
5	On the Device server, unlock the lockbox using the command:./cstdriver -lockbox [Product directory]/data/lockb.clb -passphrase <passphrase>.Restart vcmaster.

Restoring from a Backup

To restore from a backup, follow these steps

Step	Task
1	Stop the Cluster Service. clusvcadm –d <Cluster Service Name>
2	Mount the shared partition. mount <device> [Product Directory] For example, mount /dev/sdc1 /opt/voyence.
3	Navigate to the **[Product Directory]/tools** directory. Type **./restore.pl <database backup image file>** to restore the backup, and press **Enter.**
2	Stop the Network Configuration Manager services using the following command: service vcmaster stop
6	Navigate to the **/** directory. Unmount the [Product Directory] shared partition using the following command: umount [Product Directory] **Note** If the error message "device is busy" appears when attempting to unmount, first find and stop the processes that are running in the directory using the lsof [Mount Point] command, and then run the umount [Product Directory] command.
7	Start the Network Configuration Manager cluster service using the following command: clussvcadm -e <Cluster Service Name>

Uninstalling Network Configuration Manager

Step	Task
	Important: You must complete steps 1 thorough 4 on the first cluster member.
1	Stop the Cluster Service. Use: clusvcadm -d <Cluster Service Name>
2	Mount the **[Product Directory]** shared partition as defined in the /home/cluster/cluster.conf file, using: **mount <device> [Product directory]**
3	Run the **uninstaller** using: [Product directory]/software/Uninstall_Core/**Uninstall_VMware_Smart_Network_Configuration_Manager**
4	Unmount the [Product Directory] shared partition using: umount [Product Directory] **Note** If the error message "device is busy" appears when attempting to unmount [Product directory], first find and stop the processes that are running in the directory using the lsof [Mount Point] command, and then run the umount [Product Directory] command.

RSA Token service installation

6

Read the following topics next:

- Summary of Installation Tasks
- Prerequisites for the RSA Token Service
- Software Requirements
- Installing the RSA Token Service using the graphical installer mode
- Post-Installation Procedures
- Importing RSA Tokens into the Network Configuration Manager RSA Token Server
- Deleting RSA Tokens from the Network Configuration Manager RSA Token Server
- Configuring the RSA Token ServiceNetwork Configuration Manager
- Verifying RSA Tokens in Network Configuration Manager
- Uninstalling the RSA Token Service
- Network Configuration Manager RSA Token Service Instrumentation Web Page
- Resetting the RSA Token Server Username and Password

Summary of Installation Tasks

The recommended order of installation tasks for new installations is as follows:

Step	Task
1	Review the prerequisites section below and ensure you have all the items needed to complete the RSA Token Service installation.
2	Review the minimum system requirements.
3	Install the operating system including any prerequisites.
4	Ensure all firewalls adhere to the Communication security settings mentioned in VMware Smart Assurance Network Configuration Manager Security Configuration Guide.
5	Enable Network Time Protocol (NTP).

6 Install the RSA Token Service using the steps in Installing the RSA Token Service using the graphical installer mode.

If errors occur during installation, refer to the VMware Smart Assurance Network Configuration Manager Troubleshooting Guide for a list of solutions.

7 Import RSA Tokens into the Network Configuration Manager RSA Token Server using the steps in *"Importing RSA Tokens into the Network Configuration Manager RSA Token Server" on page 148*.

8 Setup the Network Configuration Manager RSA Token Server in Network Configuration Manager using the steps in Configuring the RSA Token ServiceNetwork Configuration Manager .

9 Manually download the server certificate from the RSA token server and add it as a trusted certificate in the keystore in AS.

Create the RSA.cer by downloading the certificate from

https:\\<RSA token server>:<port>

Refer to RSA documentation for details about accessing the token server.

Run the following commands in the Application server:

```
$VOYENCE_HOME/java/bin/keytool -keystore       $VOYENCE_HOME/java/jre/lib/security/
cacerts -import -file /RSA.cer -alias       VCRSA
```

Prerequisites for the RSA Token Service

The following items are needed during the installation of the RSA Token Service:

- The username and password for the RSA Token Service Administrator Account.
- The port number that will be used to access the Network Configuration Manager RSA Token Service.
- The files included with the RSA Token Service distribution, including:
- RSA_install.pl

Software Requirements

The following must be installed on the RSA Token Server prior to installing the RSA Token Service.

- Windows Server 2016
- RSA SecurID Desktop Token 4.0.0 Build 246 for Windows. This is required only if RSA server is used for authentication.
  - Visit **http://www.rsa.com** to download a copy of RSA SecurID Desktop Token 4.1 for Windows.
- Strawberry Perl

Note After installing Strawberry Perl for the first time, you must logout, and then re-login so the system PATH variable modification can take effect.

- Java
- Visual C++ Runtime Libraries
- OpenSSL for Windows:
  - It is advisable to accept the default directory (C:\OpenSSL) when installing OpenSSL on Windows. If a directory whose path contains spaces is used, the creation of the certificates will fail.

    Note Refer the the prerequisite section of *RSA Install Guide* for the required versions of the softwares.

Installing the RSA Token Service using the graphical installer mode

The RSA Token Service can be installed on Windows Server 2016 using the graphical installer mode.

Note Before installing the RSA Token Service, ensure the RSA Token Server is time-synchronized with the RSA Authentication Manager. Time-synchronization between the RSA Authentication Manager and the RSA Token Server must always be maintained; otherwise invalid token codes are created causing the RSA Authentication Manager user accounts to become locked.

To install the RSA Token Service using the graphical installer mode, follow these steps:

Step	Action
1	Log into the server as a user with administrator privileges.
2	**Note** Strawberry Perl must be installed prior to installing the RSA Token Service. Double-click on the **RSA_install.pl** file to run the installer in the graphical installer mode. The installer begins to load. The RSA_install.pl script checks for the prerequisites, and automatically installs any missing prerequisites, if the prerequisites are located in the same directory as the install.pl script. The installer begins to load.
3	The Introduction window opens. Click **Next** at the Introduction window. Notice that as you go through the various steps needed to install, the navigation pane on the left keeps a running list of the completed steps. For example, you can see at the License Agreement window that the Introduction has been completed. A check (√) appears by each completed phase of the installation. The right arrow (▶) indicates the current window and installation status.

4	**Note** This step only appears if you are not installing the RSA Token Service on the same server as Network Configuration Manager. The Choose Install Folder window opens. You are now prompted to select the Install Folder. ■ Accept the default location, or click **Choose** to select another location. ■ Once the install folder is selected, click **Next**. This is the location where the RSA Token Service is to be installed.
5	The Enter User ID window opens. You are prompted to type the RSA Token Service Administrator Account username. Enter a **username**, and then click **Next**. This is the username used by remote clients to authenticate with the RSA Token Service.
6	The Enter Password window opens. You are now prompted to type the RSA Token Service Administrator Account password. Enter a **password**, and then click **Next**. This is the password used by remote clients to authenticate with the RSA Token Service.
7	The Windows User Account window opens. You are prompted to type the Windows Account username. Enter a **username**, and then click **Next**. **Note** This is the username used for running the RSA Token Service. This username must have “administrative” and “log on as a service” privileges.
8	The Enter Password for the Windows Account window opens. You are now prompted to type the Windows Account password. Enter a **password**, and then click **Next**. This is the password used for running the RSA Token Service.
9	The RSA Port Number window opens. You are now prompted to enter a port number. Enter a **port number**, and then click **Next**. This is the port number used to access the Network Configuration Manager RSA Token Service.
10	The Pre-Installation Summary window opens and displays the product information (before installing), as well as the required disk space. Click **Install** to start the installation. This portion of the installation may take several minutes. **Note** If there is not enough available disk space, the installer displays an error message until sufficient disk space is free. You can continue once enough disk space is available.
11	The Post Install Steps window opens. A list of post-installation tasks is displayed. Post-Installation Procedures provides more information. Click **Next**. **Note** The post-installation tasks do not need to be completed until after the RSA Token Service Installer is complete.
12	When complete, the Install Complete window opens. Click **Done**. The installer displays the installation complete message.

Post-Installation Procedures

The Post-Installation procedures include the following tasks.

- Importing RSA Tokens into the Network Configuration Manager RSA Token Server
- Deleting RSA Tokens from the Network Configuration Manager RSA Token Server
- Configuring the RSA Token Service in Network Configuration Manager
- Verifying RSA Tokens in Network Configuration Manager

> **Note** Do not launch or use the RSA SecurID Token GUI on the server running the RSA Token Service. This causes the local RSA Token Database and the Network Configuration Manager RSA functionality to become corrupted.

Importing RSA Tokens into the Network Configuration Manager RSA Token Server

To import RSA Tokens using the Network Configuration Manager RSA Token Service Tool, follow these steps:

The windows service NCM_RSATokenService is stopped and restarted when running the Network Configuration Manager RSA Token Service Tool.

Step	Action
1	Log into the server as a user with administrator privileges using the Windows Account username and password created in steps 7 and 8 of the section Installing the RSA Token Service using the graphical installer mode.
3	Open a command prompt and navigate to the **[Product Directory]\tokenservice\bin** directory.
4	**Note** Running the Network Configuration Manager RSA Token Service Tool will delete the .sdtid file. It is advisable to backup the .sdtid file before running the Network Configuration Manager RSA Token Service Tool. To run the Network Configuration Manager RSA Token Service Tool: ■ Type **NCMRSATokenService -importTokens <Directory Path>**, where <Directory Path> is the location of the RSA software token files (in .sdtid format) exported from the RSA Authentication Manager and must be copied manually on to the Token Server. ■ Press **Enter**. **Note** More than one .sdtid file can be placed in the **<Directory Path>** directory.
5	Authenticate with the Network Configuration Manager RSA Token Service utility. ■ Type the **username** for the RSA Token Service Administrator Account. ■ Enter **password** for the RSA Token Service Administrator Account **Note** This is the username and password created in steps 5 and 6 of the Installing the RSA Token Service using the graphical installer mode.

6	Verify the .sdtid files are password protected. - Enter **yes** or **no** at the prompt. - If you entered **yes**, type the **password** for the .sdtid files. The Network Configuration Manager RSA Token Service Tool may take several hours to complete if you are importing a large number of RSA tokens into the Network Configuration Manager RSA Token Server.

7	1 Manually download the server certificate, using the Browser, from the RSA token server and add it as a trusted certificate in the keystore.
	2 Create the RSA.cer by downloading the certificate
	3 In the NCM AS, run the following commands:
	`$VOYENCE_HOME/java/bin/keytool -keystore`
	`$VOYENCE_HOME/java/jre/lib/security/cacerts -import -file /RSA.cer -alias VCRSA`

Deleting RSA Tokens from the Network Configuration Manager RSA Token Server

To delete RSA Tokens one at a time, using the Network Configuration Manager RSA Token Service Tool, follow these steps:

The windows service NCM_RSATokenService is stopped and restarted when running the Network Configuration Manager RSA Token Service Tool.

Step	Action
1	Log into the server as a user with administrator privileges using the Windows Account username and password created in steps 7 and 8 of the Installing the RSA Token Service using the graphical installer mode.
2	Open a command prompt.
3	Navigate to the [Product Directory]\tokenservice\bin directory.
4	**Note** Deleting an RSA token assigned to a Network Configuration Manager credential will result in the token becoming invalid in Network Configuration Manager. To delete a single tokens from the Network Configuration Manager RSA Token Server: - Type NCMRSATokenService -deleteToken <Token Serial Number> - Press **Enter**. The Network Configuration Manager RSA Token Service Tool may take several hours to complete if you are deleting a large number of RSA tokens from the Network Configuration Manager RSA Token Server.
5	Authenticate with the Network Configuration Manager RSA Token Service utility. - Type the **username** for the RSA Token Service Administrator Account. - Enter **password** for the RSA Token Service Administrator Account **Note** This is the username and password created in steps 5 and 6 of the Installing the RSA Token Service using the graphical installer mode.

Configuring the RSA Token ServiceNetwork Configuration Manager

To configure the RSA Token Service in Network Configuration Manager, follow these steps:

Step	Action
1	Open a browser, and type the **URL** used to access Network Configuration Manager. (for example **https://<IP address>**)
2	Log into Network Configuration Manager as a user with administrator privileges.
3	Select **System Administration** from the Tools menu. The System Administration window opens.
4	Select **System Administration -> Global -> Access -> NCM RSA Token Service** from the navigation pane.
5	Enter a **Server Name**. This is the IP or hostname used to access the Network Configuration Manager RSA Token Server.
6	Enter a **Port**. This is the port used to access the Network Configuration Manager RSA Token Server. **Note** This is the port number setup in step 9 of the Installing the RSA Token Service using the graphical installer mode.
7	Enter a **User ID**. This is the RSA Token Service Administrator Account username. **Note** This is the username created in step 5 of Installing the RSA Token Service using the graphical installer mode.
8	Enter a password in the **New Password** box. This is the RSA Token Service Administrator Account password. **Note** This is the password created in step 6 of Installing the RSA Token Service using the graphical installer mode.
9	Type the same password in the **Confirm Password** box.
10	Click **Create**.
11	Click the **Close** button to exit the System Administration window.

Verifying RSA Tokens in Network Configuration Manager

To verify RSA tokens in Network Configuration Manager, follow these steps:

Step	Action
1	Open a browser, and type the **URL** used to access Network Configuration Manager. (for example **https://<IP address>**)
2	Select **System Administration** from the Tools menu. The System Administration window opens.

3	Select **System Administration -> Global -> Global RSA Tokens Viewer** from the navigation pane. The Global RSA Tokens Manager screen can be used to view tokens that have been imported into Network Configuration Manager using the Network Configuration Manager RSA Token Service Tool. *Network Configuration Manager Online User's Guide* provides more information for Global RSA Token Manager.
4	Click the **Close** button to exit the System Administration window.

Uninstalling the RSA Token Service

Note If the RSA Token Service is installed on the same server as Network Configuration Manager, running the Network Configuration Manager Core Product Uninstaller uninstalls both Network Configuration Manager, as well as the RSA Token Service.

To uninstall the RSA Token Service:

Step	Action
1	Log into the server as a user with administrator privileges.
2	Open **Add or Remove Programs** located under the Control Panel in Windows.
3	Select **Network Configuration Manager RSA Token Service** from the Add or Remove Programs list.
4	Click the **Change/Remove** button.
5	The introduction to the uninstaller displays. Click **Uninstall** to start the uninstall process. This portion of the uninstaller may take several minutes.
6	When complete, the Uninstall Complete window opens. Click **Done**. The uninstall steps of the RSA Token Service are now complete.

Network Configuration Manager RSA Token Service Instrumentation Web Page

The VMware Smart Assurance Network Configuration Manager RSA Token Service Instrumentation web page provides information for current usage and available statistics for soft tokens on the Network Configuration Manager RSA Token Server.

To access the VMware Smart Assurance Network Configuration Manager RSA Token Service Instrumentation web page, follow these steps:

Step	Action
1	Open a web browser.

2	Navigate to the following address: ■ **https://<VCTokenServerIPAddress>:<PortNumber>** where <VCTokenServerIPAddress> is the IP Address of your Network Configuration Manager RSA Token Server and where <PortNumber> is the port number created during installation. ■ See the Installing the RSA Token Service using the graphical installer mode for more information.
3	The first time you access the VMware Smart Assurance Network Configuration Manager RSA Token Service Instrumentation web page, you must add an exception to your browser to allow and install the security certificates. To add an exception for the certificate: ■ Click **Ok** at the Alert Window. ■ Click the Or you can add an exception link. ■ Click the **Add Exception** button. ■ Click the **Get Certificate** button. ■ Click the Confirm Security Exception button.
4	Type the **username** and **password** for the RSA Token Service Administrator Account. **Note** This is the username and password created in steps 5 and 6 in Installing the RSA Token Service using the graphical installer mode.

Resetting the RSA Token Server Username and Password

To reset the Network Configuration Manager RSA Token Server Username and Password used for client authentication, follow these steps:

The windows service NCM_RSATokenService is stopped and restarted when running the Network Configuration Manager RSA Token Service Tool.

Step	Action
1	Log into the server as a user with administrator privileges.
2	Open a command prompt.
3	Navigate to the [Product Directory]\tokenservice\bin directory.
4	Type **NCMRSATokenService -resetUserPwd** to run the Network Configuration Manager RSA Token Service Tool, and press **Enter**.
5	Authenticate with the Network Configuration Manager RSA Token Service utility. ■ Type the **username** for the RSA Token Service Administrator Account. ■ Enter **password** for the RSA Token Service Administrator Account **Note** This is the username and password created in steps 5 and 6 of the Installing the RSA Token Service using the graphical installer mode.
6	Follow the prompts to reset the username and password.
7	Configure the RSA Token Service in Network Configuration Manager using the steps in Installing the RSA Token Service using the graphical installer mode.

Installation on Geo Diverse

7

Read the following topics next:

- Network Configuration Manager Geo Diverse
- Features
- Replication Requirements
- Components
- Installing Network Configuration Manager in a Geo Diverse Environment
- Validating the UNIX User ID and Group ID Numbers
- Using the vcgeoadmin.pl script
- Logging the vcgeoadmin.pl script
- Testing the Geo Diverse failover script without replication software

Network Configuration Manager Geo Diverse

The Network Configuration Manager Geo Diverse solution provides a simple method for integrating Network Configuration Manager service management into a data replication system. Distributed as a Perl script, the solution automates the process of starting and stopping services, and re-homing Device servers, so they point to the active Application server.

The script, which is compatible with Red Hat Enterprise Linux 6.x and 7.x, can easily be wrapped up into a larger Geo Diverse solution.

Note The Network Configuration Manager Geo Diverse solution does not provide the data replication software, and only the replication of Application servers is supported.

As offered, the Network Configuration Manager Geo Diverse script is not a hands-off solution, but may be integrated with a larger framework to provide automated fail-over.

Features

The following features are delivered with the Network Configuration Manager Geo Diverse solution:

- The Server status (with respect to the Network Configuration Manager services), is maintained in the vcgeo.group file.
- The Start command validates that another server is not already Active.
- Geo Diverse automatically re-homes Device servers so they only communicate with the Active server.
- The Client access to the Standby servers is disabled. A message is displayed when clients attempt to access a Standby server.
- The Network Configuration Manager services are disabled from starting at boot on a Standby server.

Replication Requirements

The chosen data replication software must meet the following requirements:

- Asynchronous byte-level replication
- Write ordering preservation
- File system and database replication support

  The following two Network Configuration Manager directories must be replicated between the Network Configuration Manager Application servers:

- [Product directory]/data
- [Product directory]/db

  For example, a typical Linux environment requires replication of the following directories:

- [Product directory]/data
- [Product directory]/db

Components

The Network Configuration Manager Geo Diverse solution is comprised of the following components:

- [Product directory]/vcgeo/vcgeoadmin.pl – Administrative script, which controls service management, validation, and group management
- [Product directory]/logs/vcgeo.log – Log file for all start and stop operations
- [Product directory]/data/vcgeo.group – File containing group membership and status information. This file is created and managed by the vcgeoadmin.pl script.

Installing Network Configuration Manager in a Geo Diverse Environment

The following steps assume that you are installing the Network Configuration Manager for the first time on a replicated environment. Review the hardware, software, and replication requirements before proceeding.

Step	Task
1	**Note** Steps 1 and 2 must be completed on both the primary and secondary replication servers. Create and configure the following directories for replication, per the instructions for your selected replication technology. ■ [Product directory]/data ■ [Product directory]/db
2	Set one server as the primary replication, so that it is replicating the data, and db volumes to the secondary servers. Enable data replication.
3	**Note** Steps 3 through 7 must be completed on the primary replication server. Mount the data and db replicated volumes on the primary server as read-write.
4	Proceed to install the Network Configuration Manager as per the instructions in Chapter 2 Installation procedures (Linux platform).
5	Install any available Network Configuration Manager hot fixes.
6	Populate the **vcgeo** group by completing these steps: 1 Open a terminal on the server 2 Change directories to [Product directory]/vcgeo 3 Run the **vcgeoadmin.pl** script and pass in “add” as the argument. For example: ./vcgeoadmin.pl add 4 The script prompts for an IP address. Type the **IP address** of the replication group member you want to add. Ensure the address is accurate and unique. 5 The script prompts for a label for the entry. Enter a **label name** that will help you distinguish this server from other servers. 6 Repeat steps a through e for each server you want to add to the replication group. You only have to do this once for the entire group, as the group file is replicated to the secondary servers.
7	Stop the vcgeo service. Using the vcgeoadmin.pl script provides more information for stopping the vcgeo service.
8	**Note** Steps 8 through 14 must be completed on the secondary replication server. Unmount the data and db replicated volumes (if mounted).
9	Proceed with installing Network Configuration Manager using the instructions mentioned in the appropriate Network Configuration Manager Installation guide.
10	Install any available Network Configuration Manager hot fixes.
11	Stop the **vcgeo service**. Using the vcgeoadmin.pl script provides more information for stopping the vcgeo service.

Step	Task
12	Remove the **[Product directory]/db** and **[Product directory]/data** directories and their contents (this data already exists in the replicated volumes on the primary server).
13	Mount the data and db replicated volumes as read-only (if the replication software permits you to do so).
14	Repeat steps 8 through 13 for each secondary replication server (if you have more than one).
15	This step must be completed on the primary replication server. Start the **vcgeo service** using **vcgeoadmin.pl** (if not already running). Using the vcgeoadmin.pl script provides more information for starting the vcgeo service. **Note** If the cluster services do not get started, you have to unlock the lockbox using the command: ./cstdriver -lockbox [Product directory]/data/lockb.clb -passphrase <passphrase>.Restart vcmaster.
16	**Note** Steps 16 through 18 apply when installing Remote Device servers. Open a terminal on the server which will become the Device server.
17	Install Network Configuration Manager as a Device server using the steps in the appropriate Network Configuration Manager installation guide.
18	When prompted to type the IP address of the Application server, type the **IP address** of the Active Replication server.
19	Repeat steps 16 through 18 for each Remote Device server.

Validating the UNIX User ID and Group ID Numbers

When installing the Network Configuration Manager on a Geo Diverse environment, the *UNIX User ID* numbers and the *UNIX Group ID* numbers must be **identical** on each Application servers.

Follow these steps to validate the UNIX User ID and Group ID numbers.

Step	Task
1	Open the **/etc/passwd** file on all of the Application servers.
2	Compare the *UNIX User ID* numbers for the **pgdba** and **tomcat** users between the servers, and verify that they are identical for all Application servers where you are installing Network Configuration Manager. The format of the /etc/passwd file is: USER_NAME:x:USER_ID:GROUP_ID:DESCRIPTION:HOME_DIR:SHELL If the User ID numbers are not identical on all Application servers, use the usermod program to change the User ID numbers of the offending users. The command to change a User ID is: usermod –u <USER_ID> <USER_NAME>
3	Close the **/etc/passwd** files on all of the Application servers.
4	Open the **/etc/group** file on all of the Application servers.

Step	Task
5	Compare the *UNIX Group ID* numbers for the **pgdba**, **tomcat**, and Network Configuration Manager groups between the servers, and verify that they are identical for all Application servers where you are installing Network Configuration Manager. The format of the /etc/group file is: GROUP_NAME:x:GROUP_ID: If the UNIX Group ID numbers are not identical on all Application servers, use the groupmod program to change the Group ID numbers of the offending groups. The command to change a Group ID is: groupmod –g <GROUP_ID> <GROUP_NAME>
6	Close the **/etc/group** files on all of the Application servers.

Using the vcgeoadmin.pl script

To start the vcgeo service:

Step	Task
1	Change directories to **[Product directory]/vcgeo**.
2	Run the **vcgeoadmin.pl** script, and pass in **start** as the argument. For example: ./vcgeoadmin.pl start
3	The active status validation may be bypassed by passing in **-f** as an additional argument. This causes the script to start, even if another server is currently marked as Active in the vcgeo.group file. Example: ./vcgeoadmin.pl start -f

To stop the vcgeo service:

Step	Task
1	Change directories to **[Product directory]/vcgeo**.
2	Run the **vcgeoadmin.pl** script, and pass in **stop** as the argument. For example: ./vcgeoadmin.pl stop
3	The server in group validation may be bypassed by passing in **-f** as an additional argument. This causes the script to stop, even if the server exists in the vcgeo.group file or if the vcgeo.group file does not exist. For example: ./vcgeoadmin.pl stop -f

To get the status of the vcgeo service:

Step	Task
1	Change directories to **[Product directory]/vcgeo**.
2	Run the **vcgeoadmin.pl** script, and pass in **status** as the argument. For example: ./vcgeoadmin.pl status This displays a list of the servers in the vcgeo group along with each status. This information is pulled from the vcgeo.group file on the server from which the status command is run; therefore, this information may be stale if replication is either lagging or turned off.

To add a server to the vcgeo group:

Step	Task
1	Change directories to **[Product directory]/vcgeo**.
2	Run the **vcgeoadmin.pl** script, and pass in **add** as the argument. For example: ./vcgeoadmin.pl add
3	The script prompts you for the IP address of the server you want to add, and a label for that server.
4	Alternatively, you can pass in the IP address and label by appending the following arguments: –ip=IP ADDRESS –label=LABEL

To remove a server from the vcgeo group:

Step	Task
1	Change directories to **[Product directory]/vcgeo**.
2	Run the **vcgeoadmin.pl** script, and pass in **remove** as the argument. For example: ./vcgeoadmin.pl remove
3	The script prompts you for the IP address of the server you want to remove.
4	Alternatively, you can pass in the IP address by appending the following argument: –ip=IP ADDRESS

Logging the vcgeoadmin.pl script

The vcgeoadmin.pl script logs all start and stop activity in the following log file:

[Product directory]/logs/vcgeo.log

Testing the Geo Diverse failover script without replication software

Perform these steps to test the geo-diverse failover script without installing any replication software.

1 Configure two separate Application servers.

   Use the same passwords and passphrase while installing the second Application server.

2 Configure one Device server to the first Application server.

3 Add the second Application server using the vcgeoadmin.pl script on the first Application server.

4 Stop the services on the first Application server.

5 Create a tar file containing the data and database directories:

```
tar cf first_app_server.tar db data.
```

6 Copy the tar file to the [Product directory] on the second Application server.

7 Stop the services on the second Application server.

8 Rename the original data and database directories on the second Application server:

```
mv db db_save;
mv data data_save
```

9 Extract the files from the tar file on the second Application server:

```
tar xvf first_app_server.tar
```

10 Unlock the lockbox on the second Application server using the commands:

a

```
source /etc/voyence.conf
```

b

```
[Product directory]/bin/cstdriver -lockbox [Product directory]/data/lockb.clb
-passphrase <passphrase entered during the installation>
```

11 Update the second Application server IP address in the postgres.conf file in the first Application server at [Product directory]/db/controldb/data/postgresql.conf.

Search for listen_address and update the IP address.

12 Go to the vcgeo directory on the second Application server and run the command:

```
./vcgeoadmin.pl start -f
```

13 Copy the bundle.p12 file at [Product directory]/conf/bundle.p12 from second Application server to the Device server.

14 Login to the Device server and perform the following tasks:

a

```
source /etc/voyence.conf
```

b

```
Backup the files [Product directory]/bin/demoCA/cacert.pem, [Product directory]/bin/
demoCA/index.txt, and
[Product directory]/conf/CA/voyenceca.crt.
```

c

```
perl [Product directory]/bin/importcertsintods.pl <certificate password during the
installation> <location of the copied bundle.p12 in step 14]
```

Do not keep the backup in the same location.

d Remove all the data in the [Product directory]/bin/demoCA/index.txt file.

Note Be sure to remove blank lines, if any, from index.txt. The file must be completely empty.

e Delete all the files with .0 extension from [Product directory]/conf/CA/ directory.

f bash makekeys.sh

15 Change the IP address and FQDN in the following files and point to the second Application server.

a
```
source /etc/voyence.conf
```

b
```
[Product
             directory]/data/.rhttps
```

c
```
[Product directory]/data/devserver/master.addr
```

d
```
[Product directory]/bin/cstdriver -lockbox [Product directory]/data/lockb.clb
-passphrase <passphrase entered during the installation>
```

e Restart the services on the Device server.

16 Change the IP address and FQDN in the following files and point to the second Application server.

a
```
source /etc/voyence.conf
```

b
```
[Product directory]/web/conf/web.properties /etc/voyence.conf
```

c
```
[Product directory]/cstbin/cstdriver -lockbox [Product directory]/data/lockb.clb
-passphrase <passphrase entered during the installation>
```

17 Restart vcmaster service on the second Application server.

Verify if the services have started on the second Application server and login to the Network Configuration Manager application on the second Application server.

18 Start an auto-discovery job.

If you need to rollback to first Application server:

1 Perform the steps from step 3 through step 16 on the second application server and

2 Change the tar filename to second_app_server.tar.

3 Change the database directory permission after step 9 using the command:

```
chown -R pgdba:voyence [Product directory]/db
```

Integration Adapter for Smarts Manager

8

Read the following topics next:

- Introduction
- Prerequisites
- Deployment
- How the Integration adapter for Smarts Manager operates
- Installation programs
- Configuring the Adapter
- Installing the contextual launch scripts for Smarts Manager
- Client tools
- Configuring the Service Assurance Manager (SAM) dashboard (web client)
- Advanced configuration
- Uninstall instructions
- Uninstall instructions for client tools for Service Assurance Manager (SAM)

Introduction

Network Configuration Manager provides automation and standardization of the network configuration and change management processes.

Network Configuration Manager automates configuration management at various levels, covering devices such as routers, switches, firewalls, and business policies, such as access and security configuration.

The adapter provides the following functionality:

- **Device Synchronization** – The adapter ensures that devices found in Network Configuration Manager are also found in the Smarts Manager, those found in Smarts Manager are also found in Network Configuration Manager. In addition, the adapter will reconcile devices between Smarts Manager and Network Configuration Manager internally. This provides a mapping used for notifications and contextual launches.

- **Event Notification** – Network Configuration Manager events are sent to the notification console in Smarts Manager. Device events are linked to the corresponding Smarts Manager device, while non-device events, such as Network Create events, are linked with the Network Configuration Manager server.
- **SNMP Credential Synchronization** – Network Configuration Manager has strong capabilities for managing device credentials, including credential rolling. The adapter detects when device passwords (SNMP community strings) have been changed in Network Configuration Manager, and propagates those changes into Smarts Manager.

  Note SNMPv3 and CLI credentials synchronization is not supported.
- **Contextual Launch** – The events and device reconciliation (previously mentioned in Device Synchronization), provide a number of launch points from Smarts Manager into the Network Configuration Manager application.

Terminology

The following terminology is used within this document.

Term	Refers to:
SAM	VMware Smart Assurance Service Assurance Manager
IP Availability Manager	VMware Smart Assurance IP Availability Manager, includes all Domain Managers that can act as IP Availability Managers, including IP Performance Manager, and Topology Split Manager
Smarts Manager	Refers to the system with a minimum configuration of one SAM, the Broker, and any associated IP Availability Manager
adapter	Network Configuration Manager Integration Adapter for IT Ops Manager.

Prerequisites

Review the minimum system requirements mentioned in VMware Smart Assurance Network Configuration Manager Support Matrix document. The document provides information that helps you:

- Determine if the product is supported on your platform.
- Review the patch requirements for your operating system.
- Determine if your system meets the hardware requirements.

Deployment

The adapter is middleware that connects to both Smarts Manager and Network Configuration Manager.

The basic Smarts Manager configuration assumed by the adapter is:

- Service Assurance Manager (SAM)
- IP Availability Manager

  The basic Network Configuration Manager configuration assumed by the adapter is:

- Network Configuration Manager Server is configured (any configuration)
- Before starting any operations or functions using the adapter, a network must be added in the Network Configuration Manager Server.

  Configuring the adapter requires the installer to understand the following connection points:

- Network Configuration Manager Public API
- SAM Connection
- IP Availability Manager Connections

How the Integration adapter for Smarts Manager operates

After configuring the adapter, it runs through a series of self-tests to test the connections and options. When the tests pass, the adapter becomes functional. If this is the first time the adapter has been run, it is required that batch synchronization completes before either credential synchronization or active (event-based) device synchronization is functional.

Batch device synchronization

Batch device synchronization first pulls all devices from Smarts Manager and Network Configuration Manager, and attempts to match the devices based upon an algorithm that balances performance with accurate results in a wide variety of environments. Due to the potentially long-running and processor intensive nature of full synchronization, it is a manual step to begin the initial synchronization.

The batch device synchronization algorithm attempts to match devices first by name matching, then through management IP (SNMP) addresses, and if needed, it will inspect devices down to the interface level to produce a mapping.

This reconciliation is then used for multiple purposes.

- In event notification, it is used to associate device events with the proper Smarts Manager device, even when names or management IP addresses do not match.
- Credential synchronization uses the mapping to ensure that password changes in Network Configuration Manager are propagated to the correct Smarts Manager device.
- It facilitates contextual launch by ensuring that launch points in Smarts Manager lead to the correct devices in Network Configuration Manager.

Once the mapping is complete, devices that are not managed by IP Availability Manager, but are managed by Network Configuration Manager are put on the Smarts Manager pending list. Devices that are managed by IP Availability Manager, but not managed by Network Configuration Manager are scheduled for discovery in Network Configuration Manager.

Also, when batch synchronization is complete, the adapter enables active device synchronization, and credential synchronization.

Batch synchronization can be run at any time if the mapping information becomes outdated for any reason. For example, if the server hosting the adapter was down for a number of days, the device mapping could be out of date, depending on the rate of change in the network.

Run batch synchronization again after rebooting the server to immediately synchronize the systems. Remember, with a large number of devices, this is a long running operation that is computationally expensive, so it is advisable to complete this operation during off-peak hours.

Note Until the initial batch synchronization completes successfully, active synchronization and credential synchronization remain inactive.

Active (device) synchronization

The adapter listens for events from Network Configuration Manager, such as, device create events, and certain device state change events, and also events from Smarts Manager that indicates new devices have been added.

These events trigger the adapter to complete the same reconciliation and “diff” logic as the batch synchronization. As with the batch synchronization operation, devices that are added to Network Configuration Manager that cannot be matched with existing Smarts Manager devices, are put on the Smarts Manager pending list. Devices that are added to Smarts Manager that cannot be matched with existing Network Configuration Manager devices, are set up for discovery operations in Network Configuration Manager.

SNMP credential synchronization

The adapter listens for SNMP credential change events in Network Configuration Manager. Specifically, the password change event is inspected to determine whether the SNMP credential change involves an SNMP community string. If so, calls to change the SNMP community string in Smarts Manager are put in a queue for processing.

The reason the events are queued instead of acted upon real time, is to handle the case of SNMP credential rolls. By design, Network Configuration Manager has a credential roll feature that could result in large numbers of devices having passwords changed at the same time. However, the logistics of changing passwords in Smarts Manager can be expensive if many devices are changed on a one-off basis.

Therefore, SNMP credential changes are run in batch. At the conclusion of the batch operation, a reconfigure command is issued to IP Availability Manager to utilize the new passwords. The time interval between batch SNMP credential synchronization operations is configurable. This information can be located in *"Configuring the Adapter" on page 170*

Note that the Network Configuration Manager manages SNMP credentials as a single pair of one read-only password and one read-write password. In the case where an SNMP credential is modified in Network Configuration Manager in which the read-only password is set to null, the adapter will not update the Smarts Manager SNMP community string. This prevents any interruption in monitoring if Smarts Manager is using a different SNMP community string than Network Configuration Manager to monitor the device.

Event notification

Event notifications start to run before batch device synchronization has run, but notifications may not be associated with the correct devices before the adapter has a chance to reconcile devices between the systems.

The notification console in Smarts Manager typically receives SNMP notifications. The events received from Network Configuration Manager differ only in the delivery method. The adapter processes the events, and uses the mapping generated during reconciliation to associate events with the correct Smarts Manager device. The events are delivered by way of an API. Therefore, the SNMP notification adapter for Network Configuration Manager is not required for this adapter.

Important information about synchronization

Synchronizing devices can potentially be an expensive operation. On new installations, where both Smarts Manager and Network Configuration Manager are new to an environment, performance is much better if the discovery of devices is done in at least one of the systems prior to running batch synchronization. Although the active synchronization can synchronize them, it takes longer and is less efficient.

More importantly, keep in mind that some of the functionality in the adapter depends on synchronization. For example, associating notifications with the proper devices and performing credential rolling depends on the internal mapping.

After running batch synchronization, the respective discovery jobs in Network Configuration Manager and Smarts Manager (the pending list) must be executed for the synchronization to complete. Therefore, it takes some time for the synchronization to settle out unless the pending list and jobs are manually executed and run to completion.

Mapping between networks and IP Availability Managers

The adapter has a mapping feature to route devices into specific networks or IP Availability Managers. The mapping rules allow you to specify a target destination, based on a device's origin and other attributes, such as the IP address or name of the device.

For example, a rule could specify that for a given Network Configuration Manager network, devices coming from that network will end up in a named Smarts IP Availability Manager. For a different network, they could route to a different IP Availability Manager. There are filters available to achieve any granularity necessary for your environment. A full explanation of filters is detailed in *“Configuring the Adapter” on page 170*.

Installation programs

There are two installation programs used to install the adapter. The first installer is for the adapter itself, and the second is for installing the scripts used for contextual launch into the Global Console.

Installing the Integration adapters

Install the adapter on the Network Configuration Manager **Application server**. Use the following steps to install the adapter for Smarts Manager on the Linux environments.

Note If you already have a previous installation of the adapter, uninstall that version before installing the newer version.

To start the installation, you have to run the script **install.sh** in (Linux). When you run the script, the command prompt screen appears with four options:

- Type **1**, and press **Enter** to install NCM Core product, and Device Drivers.
- Type **2**, and press **Enter** to install NCM Smarts Adapters.
- Type **3**, and press **Enter** to install NCM Core product and NCM Smarts Adapters.
- Type **4**, and press **Enter** to exit the installation.

For Linux

Step	Action
1	Type **bash install.sh –i console** to run the installer in the graphical installer mode,and press **Enter**. The command prompt screen appears: ■ Type **3**, and press **Enter** to install NCM Smarts Adapters.
2	At the Introduction window, press **Enter** or click **Next**.
3	At the Important Notice window, read the information, and then press **Enter** or click **Next**.
4	At the Choose Install Folder window, either type the **Install Folder path**, or press **Enter** or click **Next** to view and accept the default for the Install Folder path.
5	At the Summary window, press **Enter** or click **Next**.

The adapter now begins the installation process. Verify the installation using the steps in the URL noted in *“Configuring the Adapter” on page 170*.

Installed services

The installation creates a convenient method for starting and stopping the adapter via services appropriate for the platform on which it is installed.

- On a **Linux** platform, a service named **ncmsmartsadapter** is created in the standard /etc/init.d directory. The commands to start and stop the adapter are as follows:

  ```
  service ncmsmartsadapter start
  service ncmsmartsadapter stop
  ```

Establish a secure connection with the server

For establishing a secure connection to the Network Configuration Manager server:

1 From the Network Configuration Manager Application or Combination server, export the self signed certificate from [Product Directory]/conf/voyence-ssl.keystore to a file using the steps:

2 source /etc/voyence.conf

3 $JAVA_HOME/bin/keytool -export -keystore [Product directory]/conf/voyence-ssl.keystore -alias selfsigned -file <CERTIFICATE>

  To find the location of JAVA_HOME, type the command echo $JAVA_HOME. Ensure that JAVA_HOME is pointing to the right version of Java. For example, <<VOYENCE_HOME>>/java.

  Note <CERTIFICATE> can be any name and it is the file that is created from the export.

  Press **Enter** without entering a password.

4 Import the self signed certificate from the file <*CERTIFICATE*>.

  ```
  $JAVA_HOME/bin/keytool -keystore $JAVA_HOME/jre/lib/security/cacerts -import -file
  <CERTIFICATE> -alias selfsigned
  ```

5 Type the password **changeit** during the prompt.

6 This is the default password, unless otherwise modified.

7 Type **Yes** and click **Enter** when the **Trust the certificate** prompt appears.

  To view the imported certificate, type:

  ```
  $JAVA_HOME/bin/keytool -keystore $JAVA_HOME/jre/lib/security/cacerts -list -alias
  selfsigned
  ```

8 Restart Tomcat service:

  service tomcat restart

9 Restart the adapter, following the instructions in *"Installed services" on page 169*.

Configuring the Adapter

Discovering Network Configuration Manager with Smarts Manager

The Network Configuration Manager system must be discovered by Smarts Manager for the event notifications to function properly. The adapter now checks this during configuration, and will not pass the self-tests if the Network Configuration Manager server cannot be found.

The Smarts Manager provides two options for initiating a manual discovery. Both options are initiated through the Domain Manager Administration Console.

- Option 1: Import a seed file
- Option 2: Using the Add Agent command

> **Note** VMware Smart Assurance IP Manager Concepts Guide and VMware Smart Assurance IP Manager User Guide provides more information for preparing and initiating discoveries.

Network Configuration Manager needs to be discovered in Non-SNMP mode to get it into the system. Once Network Configuration Manager is discovered into Smarts Manager, note the name given by Smarts Manager to the Network Configuration Manager server. This is needed in the next step, configuring the adapter.

Accessing the configuration GUI

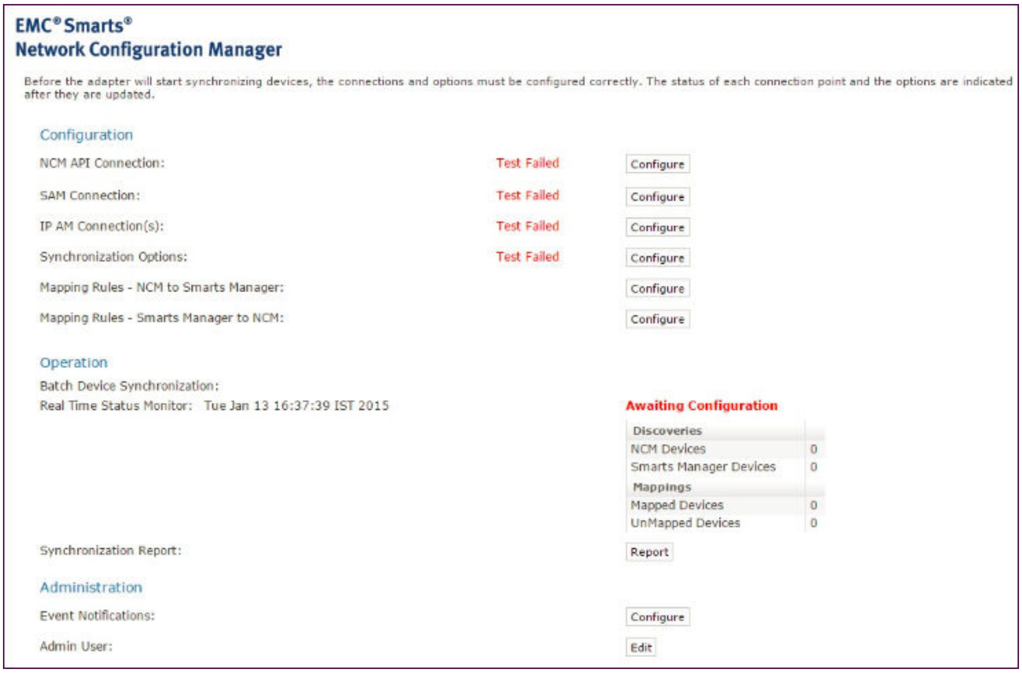
A graphical user interface is provided to guide you through the configuration steps. Go to the URL:

https://[SERVER-IP]:11843/NCMSmartsAdapter-10.1.6.0/

where [**SERVER-IP]**is the server where the adapter was installed, usually the Network Configuration Managerserver.

The main window appears, showing the status of all connections. The status is Failed until the connections are configured, as the following figure shows.

Figure 8-1. Smarts Adapter Configuration Main Screen



EMC® Smarts®
Network Configuration Manager

Before the adapter will start synchronizing devices, the connections and options must be configured correctly. The status of each connection point and the options are indicated after they are updated.

Configuration

NCM API Connection: Test Failed Configure

SAM Connection: Test Failed Configure

IP AM Connection(s): Test Failed Configure

Synchronization Options: Test Failed Configure

Mapping Rules - NCM to Smarts Manager: Configure

Mapping Rules - Smarts Manager to NCM: Configure

Operation

Batch Device Synchronization:

Real Time Status Monitor: Tue Jan 13 16:37:39 IST 2015 Awaiting Configuration

Discoveries	
NCM Devices	0
Smarts Manager Devices	0
Mappings	
Mapped Devices	0
UnMapped Devices	0

Synchronization Report: Report

Administration

Event Notifications: Configure

Admin User: Edit

An overview of the configuration process follows:

- The top four rows indicate the status of each connection.
- To the right of the status is a **Configure** button used to configure each connection.
- Below this, the synchronization options and mapping rules are shown. These are also configured by using the **Configure**button to the right.
- Clicking any **Configure**button produces the login window. Default credentials are:
  - Login ID: admin
  - Password: admin
- When the configuration is valid (indicated by all the Tests Passing), components are enabled, and event notifications begin flowing. However, synchronization does not begin until the **Start** button is selected.

Step 1: Network Configuration Managerpublic API connection configurations

1. On the main screen, select **Configure** next to the NCM API Connection line. The next screen displays the values for which the adapter is currently configured.
2. The following values can be configured for the Network Configuration ManagerPublic API:
   - **Username / Password** – this should be a separate user that has been created through Network Configuration Manager, with full access rights
   - **Host Name** – the IP address of the Network Configuration ManagerApplication server

- **Auth Conf Location**– only modify this field if you are familiar with the authentication mechanism of Network Configuration Manager, or if you are specifically instructed to by a qualified support engineer.
- **Cxn Retries**– once the adapter tests have passed, it is advisable to reset this value to 5 retries
- **Cxn Retry Interval**– this is in milliseconds, so a value of 10,000 is equal to 10 seconds

3. When you are satisfied with the values in the configuration, click **Update** located in the bottom left of the screen.
4. Click **Home** (at any time) to return to the main screen.

   Once you have successfully configured the connections, note that Event Notifications will flow from Network Configuration Managerto Smarts Manager. However, until synchronization is performed, events will not necessarily be associated with devices in SAM.

   The connection is not continuously monitored after the initial synchronization. Therefore, it is possible to see this connection in a Test Failed state if the adapter has been running for a while in Active Synchronization mode. This does not affect the operation of the adapter. If you are performing a batch synchronization operation and find the connection down, update to re-establish the connection.

Step 2: SAM connection configuration

1. From the main screen, select **Configure** next to SAM Connection line. The next screen displays the values for which the adapter is currently configured.
2. The following values can be configured for the SAM connection:
   - **Broker IP Address**– the IP address where SAM is installed.
     - **Broker port**– The port where SAM is running.
     - **User Name / Password**– Account credentials for SAM.
     - **SAM Domain Name**– the name of Service Assurance Manager requested with the Broker, for example, INCHARGE SA.

       Click **Get Available Domain Managers**to receive the list of available domain managers that are registered on the broker that is populated in the SAM Domain Name field.
     - **SAM Username / Password**– this needs to be set to an administrator user with full administrator rights.
     - **Network Configuration Manager System Name**– Not required in version 9.6.1 onwards.

       Note The **NCM System Name** becomes blank after you click the **Get Available Domain Managers** button. The **NCM System Name** is automatically obtained in the backend and you do need not to provide it manually.

3 When you are satisfied with the values in the configuration, click **Update** located in the bottom left of the screen.

4 Click **Home** (at any time) to return to the main screen.

The configuration status is displayed as **Tests Passed** if the following criteria is met:

- Successful connection with the selected domain manager using the provided credentials.
- Selected domain manager is a valid entry, such as SAM
- The NCM host is discovered in Smarts Manager, and the provided name matches with the Display Name on the host that is discovered in the Smarts Manager.

Step 3: Smarts IP Availability Manager connections configuration

1 From the main screen, select **Configure** next to IP availability line.

2 The list of possible IP Availability Manager components must be obtained by selecting the **Refresh from SAM** button near the top of the page. As a reminder, a dummy IP Availability Manager configuration called REFRESH-ME is present by default.

3 After you refresh from SAM, a list of possible Domain Managers are present. Not all of these are valid IP Availability Manager Domain Managers. This is because SAM cannot be queried strictly for IP Availability Managers, only the full list of Domain Managers. Delete any Domain Managers that are not IP Availability Managers that you want to configure. Typically, in addition to IP Availability Managers, you will see the SAM interface and the OI interface listed as Domain Managers. Delete these as well.

Note Deleting all IP Availability Manager configurations could result in unexpected behavior from the adapter. If there are questions about the status of IP Availability Manager connections, refreshing from SAM is the correct method used to address the situation.

The domain manager must comply with one of the following requirements:

- The domain manager is a IP Availability Manager directly configured with SAM.
  - The domain manager is a TSM either directly configured with SAM, or is managing an IP Availability Manager that is configured with SAM.

If the configured domain manager does not meet any of the above requirements, then it is removed from the list.

The list of IP Availability Managers on this page must pass the configuration tests, or the adapter will not pass the self-tests. The adapter does not allow the synchronization operation to start until the configuration is valid.

When configuring IP Availability Managers, the adapter reports one of the following states for each IP Availability Manager:

- **UNCONFIGURED** – the Domain Manager was reported by SAM, but you have not configured it
  - **NOT FOUND IN SAM** –a previously existing Domain Manager was not in the list of Domain Managers reported by SAM, or a Domain Manager connected to the broker, but not reported by SAM, for example, TSM not connected to the SAM and managing an IP Availability Manager reported by SAM.
  - **NOT** IP Availability Manager **DOMAIN** – a Domain Manager that was configured properly is NOT an IP Availability Manager domain, and is invalid for this configuration
  - **COULD NOT CONNECT** – a Domain Manager that was configured could not make a connection
  - **TESTS PASSED** – the Domain Manager is configured, a connection was successfully made, and the Domain Manager was queried and determined to be an IP Availability Manager

4 The following values can be configured for the IP Availability Manager connections:

   - **AM Domain Name** – it is not recommended that this value be changed. Rely on SAM to report the name of the Domain Managers for you, then proceed with the other configuration parameters

      - **Broker IP Address** –the IP address where the IP -M is installed (this may be the same box as SAM)

      - **AM Username / Password** – this needs to be set to an administrator user with full administrator rights.

5 When you are satisfied with the values in the configuration, click **Update** located in the bottom left of the screen.

6 Click **Home** (at any time) to return to the main screen.

Step 4: Synchronization options

1 On the main screen, select **Configure** next to the Synchronization Options line. The next screen displays the values for which the adapter is currently configured.

2 The following options are configurable for synchronization:

   - **Default Network Configuration Manager Network** – This is the network inside Network Configuration Manager into which Smarts Manager devices are discovered if a mapping rule is not present or fired for a device. If you enter a network that does not exist in Network Configuration Manager, it will be created.

      - **Default Network Configuration Manager Device server** – Discovery operations in Network Configuration Manager require a Device server to be specified. This Device server is used as the default if a mapping rule is not present or fired for a device. Once the Network Configuration Manager public API connection is configured properly, the adapter selects a default Device server. This server can be changed here, but it must already exist in Network Configuration Manager.

      - **Network Configuration Manager Job Scheduling** – Discovery operations in Network Configuration Manager are jobs. There are two options for how the adapter schedules the discovery jobs.

      - **Run Upon Approval** – the jobs are put into a Pending Approval state, and begin when the job is approved in Network Configuration Manager.

      - **Run In Maintenance Window** – the jobs are scheduled to run in the next maintenance window in Network Configuration Manager.

      - **Network Configuration Manager Name Filtering** – in the mapping rules, filtering can be accomplished based on the device name. This option specifies which Network Configuration Manager device name the mapping rules will use.

- **Network Configuration Manager Discovery** – Use Global Credentials – selecting this option pulls the accounts and privileged passwords from the global configuration in Network Configuration Manager, when discovering devices are coming from Smarts Manager.
- **Manage Default Mapping** – Deselecting this checkbox disables default mapping from Network Configuration Manager to VMware Smart Assurance manager. This option is enabled by default.
- **Manage Network to be used for Mapping** – Selecting this option allows mapping devices from Network Configuration Manager using only primary networks, or only secondary networks, or from both. The default option is Primary. When you selects the **Secondary** or **Both** option, the default mapping is deselected and disabled message is displayed. You can enable the default mapping.

  Note Use only explicit mapping when Secondary or Both option is used to avoid overloading the pending list entries on Smarts manager.

- **Manage listening to Device Configuration Changes on NCM** – This option can be used to add notifications on device changes in the IP Availability Manager. This option is enabled by default
- **Manage listening to Credential Changes** – This option can be used to update changes in the SNMP (RO community string) credentials on devices in the IP Availability Manager.

  Note Changes in credentials on Network Configuration Manager sends both device change and credential change notifications to the adapter. When both theoptions are selected, the update notifications are added as pending list entries on Smarts Manager, and the credentials are updated. If device configuration change is deselected, then the credential changes are silently updated on Smarts manager and not in the pending list.

- **Default Smarts** IP Availability Manager – This IP Availability Manager is used as the default if a mapping rule is not present or fired for a device flowing from Network Configuration Manager to Smarts Manager. Devices will end up on the pending list of this IP Availability Manager by default if a mapping rule is not used.
- **Smarts Manager Name Filtering** – in the mapping rules, filtering can be accomplished based on the device name. This option specifies which Smarts Manager devices name the mapping rules will use.
- **Active Sync (seconds)** – Although the integration adapter is always listening for events that may trigger device synchronization, it only processes these events at regular intervals. For example, the default setting is five minutes, but can be changed to happen only once a night.

- **Credential Sync (seconds)** – The same concept as with Active Synchronization applies, except this applies to credential synchronization. When a password is changed in Network Configuration Manager, Smarts Manager needs to be notified to continue monitoring the device. Therefore, it is advisable to keep this setting relatively short.

3 When you are satisfied with the values in the configuration, click **Update** located in the bottom left of the screen.

4 Click **Home** (at any time) to return to the main screen.

Mapping Configuration

The mapping of devices from NCM to the Smarts Manager, and the default IP Availability Manager configured in the synchronization page, can be turned off by clicking on **NCM to Smarts Manager Default Mapping**.

The devices from the primary and secondary networks in NCM can be mapped to an IP Availability Manager by selecting **Primary** or **Secondary** or **Both** in the **NCM to Smarts Manager Mapping: Network to be used** tab.

If secondary or both options are selected, the default mapping is turned off automatically, the default mapping can be later selected. Use explicit mapping rules for mapping devices in a secondary network. The primary network of the device is used as a default option.

Device Configuration Change Event

The devices in the pending list of the IP Availability Manager when NCM device configuration is changed, can be disabled by deselecting **NCM to Smarts Manager Pending entries - Use Device Configuration Changes** option. The option is selected by default, hence the devices will be to the pending list when Device Configuration Event is triggered.

Credential Synchronization Configuration

The credential synchronization between the devices in NCM and Smarts Manager can be disabled by deselecting the option NCM to Smarts Manager - Credential Sync option. By default the NCM to Smarts Manager - Credential Sync option is selected and the synchronization occurs.

Step 5: Mapping rules

The purpose of mapping rules is to control the destination of devices into specific IP Availability Managers in Smarts Manager, and specific Networks in Network Configuration Manager. For example, if a device exists in Network Configuration Manager but not in Smarts Manager, then during synchronization, the device must be put on a pending list for discovery in Smarts Manager. The mapping rules can dictate to which IP Availability Managers pending list the device will be placed.

Note When the IP Availability Manager used in the mapping rules or the default IP Availability Manager selected is managed by a TSM, then the devices always get added to the TSM. Mapping with topology split manager (TSM) provides more details on the devices added to the TSM.

Rule structure

There are two sets of rules, both with the same syntactic structure. One set of rules is for devices flowing from Network Configuration Manager to Smarts Manager, and another set of rules is for devices flowing from Smarts Manager to Network Configuration Manager.

The basic rule structure is to define an origin, a filter, and a destination. Origins and destinations are either IP Availability Managers in Smarts Manager, or Networks in Network Configuration Manager. Filters are additional criteria that can be applied.

For an example, assume there are two Network Configuration Manager Networks, NetworkA and NetworkB, and two Smarts Manager IP Availability Managers, InCharge-AM1 and InCharge-AM2. A rule might state that devices coming from NetworkB (origin) with an IP address in the range 192.168.1.1-192.168.1.255 will go to the IP Availability Manager InCharge-AM1 (destination). Syntactically, this would be expressed as follows:

```
NetworkB   IP   192.168.1.1-192.168.1.255   InCharge-AM1
```

Mapping rules are a list of these rules that function much like an access control list (ACL). Rules are executed in sequence until a match is found. The matched rule is then "fired" to control the flow of devices. In the following rule set, a device from NetworkA will end up in InCharge-AM2. Notice that regular expressions can be used in the origin. They cannot be used in the destination for obvious reasons:

NetworkB IP 192.168.1.1-192.168.1.255 InCharge-AM1

```
Netw.*  None      InCharge-AM2
```

The rules execute for each device flowing through the mapping component. In the example above, the first rule does not apply because the origin of the device is NetworkA. The second rule applies because NetworkA matches the regular expression for the origin, and no additional filtering is performed. The device will go onto the pending list of the IP Availability Manager InCharge-AM2.

In the case where no rules match for a device, the destination is determined by the defaults that were set up in the synchronization options. Imagine a default rule at the end of every rule set using the defaults from the synchronization options.

The following table shows some examples of mapping rules for devices flowing from Network Configuration Manager to Smarts Manager. Notice the use of regular expressions. If you are not skilled at using regular expressions, their construction can be counter-intuitive at first. Notice the ".*" syntax for specifying any match or any sequence of characters following an exact match.

Origin (network name)	Filter type	Filter value	Destination (AM name)
Example 1			
.*	IP	192.168.1.1-192.168.1.255	InCharge-AM-PM
.*	IP	10.1.1.1-11.1.1.1	InCharge-AM
Example 2			
Cust1	None		InCharge-AM
Cust2	None		InCharge-AM-PM
Example 3			
Cust.*	Name	abc.*23	InCharge-AM
Cust.*	Name	bbc.*23	InCharge-AM-PM
MSP.*	None		InCharge-MSP-IP-AM

Note Device type is only valid from Smarts Manager to Network Configuration Manager.

Extended rule for Network Configuration Manager Device servers

Devices flowing from Smarts Manager into Network Configuration Manager have a network as their destination. This is functional, but sometimes it is necessary to specify not just the network, but the Device server to which the devices should map.

Note If mapping from Smarts Manager to Network Configuration Manager is configured in the Adapter and if more than one Device server exists, the network created will require one or more Device servers added to the Network Configuration Manager system administration console.

Take the previous example for NetworkA, and further assume there are two Device servers, DS1 and DS2. In this case, you may want to specify the specific Device server to which the device should be managed. The mapping rules handle this case by optionally taking a DS (Device server) filter and DS (Device server) destination.

Examine the following rule, which states that a device named myrouter.* coming from InChargeAM1 should go into NetworkA and be managed by Device server DS1:

```
InChargeAM1    None    NetworkA    Name    myrouter.*    DS1
```

There are actually two filters in this statement but in this case, the first filter is a no-op filter that passes everything. Note that the first filter must pass for it to reach the second filter. For example, a router named myrouter1 with an IP address of 172.x.x.x, would not cause the following rule to fire:

```
InChargeAM1   IP   192.168.1.1-192.168.1.255   NetworkA   Name   myrouter.*    DS1
```

The first filter fails on the check of the IP address range, so the rest of the rule is ignored. With this rule structure, it is possible to route a device into exactly the desired destination by getting very specific with the rule set. The granularity of rules can be as fine or as coarse as needed to achieve a desired result.

In addition to being able to route a device into a specific Device server in Network Configuration Manager, there is a round robin (RR) option. The round robin option is applicable only to Network Configuration Manager Device servers. When specified, the round robin option balances incoming devices onto the set of Device servers for a network. Taking the previous example, say we wanted all devices in the 172 network from IP-AM InChargeAM1 to be distributed evenly across Device servers in NetworkA. That can be specified as follows:

```
InChargeAM1   IP   172.1.1.1-172.255.255.255   NetworkA RR
```

If there are 100 devices in the InChargeAM1 domain manager in the 172 network, then 50 of them will be managed by Device server DS1, and 50 will be managed by Device server DS2 in NetworkA. The following table contains additional examples of mapping rules from Smarts Manager to Network Configuration Manager.

Origin (AM name)	Filter type	Filter value	Destination (network name)	DS Filter Type	DS filter value	DS destination (DS name)
Example 1						
.*	IP	192.168.1.1-192.168.1.255	Cust1	RR		
.*	IP	10.1.1.1-11.1.1.1	Cust2	RR		
Example 2						
InCharge-AM	None		Cust1	IP	192.168.1.1-192.168.1.100	DeviceServer1
InCharge-AM-PM	None		Cust1	IP	192.168.1.101-192.168.1.255	DeviceServer2
Example 3						
In.*-MSP	Name	abc.*23	Network5	IP	10.1.1.1-10.255.255.255	DS1
In.*-MSP	Name	bbc.*23	Network5	IP	172.1.1.1-172.255.255.255	DS2
In.*-AM.*	None		Network6	RR		

Origin (AM name)	Filter type	Filter value	Destination (network name)	DS Filter Type	DS filter value	DS destination (DS name)
Incharge-AM	Device Type	Switch	Network7	Name	Dallas.*	DS3
Incharge-AM	Device Type	Router	Network8	RR		

As previously noted, the rule structure is syntactically the same, whether the mapping is from Network Configuration Manager to Smarts Manager, or vice-versa. The following table lists the full structure of rules, including all the filter options available.

Note that the Device Type filter is only applicable to devices flowing from Smarts Manager to Network Configuration Manager, and refer to the device types in Smarts Manager. The main purpose of this filter type is to eliminate non-network devices, such as servers, from ending up in the Network Configuration Manager discovery jobs. However, it can also be used to separate device types, such as routers and switches, if desired.

Origin IP-Amornetworkname	Filter type	Filter value	Destination IP-AM or networkname	DS filter type	DS filter value	DS Device server name
RegEx Value	IP	IP Range	*No RegEx here	IP	IP Range	*No RegEx here
	Name	RegEx		Name	RegEx	
	Device Type	(Smarts Types) Router | Switch | Host, etc.		Device Type	Smarts Types	
	None	N/A		None	N/A	
				RR (Round Robin)	N/A	

Exclusions

The mapping facility also has the ability to exclude certain devices from being mapped. These rules are also the same syntax as the mapping rules, but are less complex. They do not require a destination, since they specify an exclusion. Here are some examples.

Exclude all devices from the 172 network

```
.*   IP   172.1.1.1-172.255.255.255
```

Exclude all hosts going from Smarts Manager to Network Configuration Manager

```
.*   DeviceType   Host
```

Exclude any device whose name matches the regular expression “edge.*” coming NetworkA.

```
NetworkA   Name   edge.*
```

Exclusion rules only require an origin and a filter, and still follow the syntax for mapping rules previously detailed.

Tips and tricks

The mapping rules can be syntactically checked by selecting the Test Grammar button in the mapping rules configuration. The adapter checks the syntax, reports whether it found any errors, and reports the specific error to the best of its ability.

It is important to understand that the adapter will not check your rules for semantic accuracy, or check whether statements are accurate for your particular environment. For example, if you misspell a network name, the adapter is not going to check the networks in Network Configuration Manager and inform you of the misspelling.

It will only check the structure of the rules, not the meaning of the rules. Remember, in the case where no rule matches, the defaults will be used from the Synchronization Options, so it may not always be obvious there is an error in the mapping rules.

Once the structure is correct, the rules can be saved selecting the Save button. For your convenience, the rules are reformatted in a comma delimited format, making for easy import and export to a spread sheet. It may be easier to work in a spread sheet for complex rule sets, or if you are working offline.

Save the rules as a comma delimited format, and paste them into the text fields when you are ready to use them. The adapter will parse rules either delimited by commas or spaces.

Another aid for developing and debugging rules is the addition of a log file dedicated specifically to rule processing. In the same location as the main log, vc_smarts_adapter.log, you will find a rule processing log named vcsmarts_mapping_rules.log.

An entry in the log is made for every device processed by the rules engine during batch synchronization. It will indicate which rule was fired for each device, and the reason or match values that led to firing the rule. Using this log, you can understand what happened to each and every device during processing. Additionally, the log file is constructed in a strict comma delimited format so that you can import it into a spread sheet for analysis.

The structure is as follows, with the fields listed in order:

1. Date
2. Timestamp
3. Timestamp millisecond counter

4. Rule set or direction - V2S means Network Configuration Manager to Smarts Manager; S2V means Smarts Manager to Network Configuration Manager
5. Device name
6. Origin - IP Availability Manager or Network
7. Destination
8. Match type - No Match, IP, Name, None (no-op), Excluded
9. Match value – the value matched causing the rule to fire
10. Delimiter – indicates that following is the actual rule
11. Actual rule fired (delimited as well)

    For easy examination, import the log into a spread sheet, and drop the first three columns. This view offers a clear re-enactment of the rule firings on a device-by-device basis. Note that NO MATCH and NONE are not the same thing. NO MATCH means that no rule was fired and the default destination was used. NONE means that the no-op filter was defined in the rule that was fired.

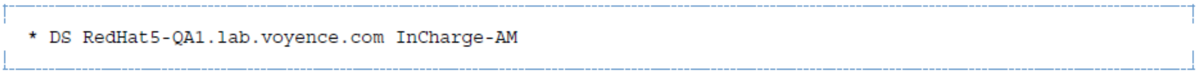
    Finally, if rule configuration and processing seems confusing, take it one step at a time. Remember that when executing the synchronization, devices go into Network Configuration Manager jobs and the pending list for Smarts Manager. You can delete these if they do not appear to be what you want before they execute. In Network Configuration Manager, deleting the actual auto-discovery entry will also delete the job created from it as well. That is the best place to delete unwanted entries. You can execute batch synchronization as many times as you like, provided the data set is not too massive.

    One approach to learning mapping would be to exclude everything but a single IP Availability Manager coming from Smarts Manager, and route that into a couple of practice networks in Network Configuration Manager. Execute the batch synchronization, and get comfortable with the rules and examining the log. Then, remove the pending list entries or auto-discovery entries in Network Configuration Manager, and expand the list of devices. You will find the rules easy to navigate.

Mapping NCM to Smarts

In addition to the existing filters, a new filter DS is added to support mapping from the NCM Device server to the TSM to IP Domains. The filter ensures that devices belonging to a given Device server will be explicitly mapped to the destination. Mapping ruledisplays an example of a mapping rule.

Figure 8-2. Mapping rule



```
* DS RedHat5-QA1.lab.voyence.com InCharge-AM
```

Mapping with topology split manager (TSM)

TSM behaves as both an IP Availability Manager, and a manager of other IP Availability Managers by controlling the distribution of devices to them.

When constructing the mapping, it is recommended you use a TSM as the destination for any of the subordinate IP Availability Managers.

If the mapping rule includes a subordinate IP Availability Manager, the mapping is evaluated against the managing TSM and allows the TSM to add the device to the pending list entries in any of its subordinate IP Availability Managers.

When the IP Availability Manager used in the mapping rules, or the default IP Availability Manager selected is managed by a TSM, then the devices always get added to the TSM.

Configuring Service Assurance Manager (SAM) for contextual launch

Once the scripts have been installed on the SAM server, they must be configured as client tools. Client tools are configured from the Global Manager Administration Console.

The client tools provide contextual launch capability in SAMs from the Notification Browser, the Topology Browser, and the Map View of the Topology Browser.

Before configuring the client tools, there are some items to note on the Network Configuration Manager contextual launch. Contextual launch happens through a URL in a browser. Once fed to the browser, the web start mechanism takes over and begins loading the Network Configuration Manager application from the server. When using the Contextual Launch feature, keep the following in mind.

- Usually, you are required to login for each launch of the Network Configuration Manager application. This contextual launch uses a special launch file that allows use of the “Remember Me” feature, so users do not have to log in each time.
- The Network Configuration Manager application should be closed after each use of the launch so that:
  - The application is ready to launch to the appropriate location on the next use
  - The extra device information readily available from Network Configuration Manager is not left on the screen if the operator leaves their workstation

    Once in the Global Manager Administration Console, ensure that it is attached to the SAM application, by ensuring the drop-down box Manager, is pointing to INCHARGE-SA.

    For each of the client tools the set of steps are the same, but the values are different. See the specific parameters for each client tool located in the *“Client tools” on page 188*, and then follow these steps:

Step	Action
1	Under **Tools > Client** right-click, and select **New Client Tool.**
2	Type the name of the **client tool** in the Client Tool text box, and click **Next**.
3	Select the program from the drop-down list.

4	■ Select the profiles you want to add. The **admin-profile** must be one of the selected profiles. ■ Click **Next**.
5	Select the appropriate **value** for the Context object in the drop-down. For example, ICIM_Notification.
6	■ Use the plus-sign (**+**) to create the context criteria. These are listed below for each client tool. ■ Click **Next**.
7	Ensure that the Context object for the Status criteria is the *same* as the previous screen. Click **Next**.
8	Do not add any parameters. Click **Finish**.

After you enter client tools, read the information in the VMware Smart Assurance Service Assurance Manager Operator Guide on how SAM picks up the changes for the appropriate platform.

Additional Required Configurations

In addition to the configuration console for the adapter, some configuration is required for the following Smarts Manager components:

- Domain Manager Administration Console for IP Availability Manager
- Global Administration Console (SAM)
- Ensure the SAM Adapter Platform is installed and registered with the Smarts SAM module

Installing the contextual launch scripts for Smarts Manager

Users can launch the Smarts Manager GUI from the following related product GUIs:

- From the SAM Manager
- From the EMC M&R User Interface when the SolutionPack for Smart Assurance Manager is installed

  Each method requires some setup, as described in the following sections.

Setup for SAM GUI contextual launch

Note The Contextual Launch Scripts for Smarts Manager must be installed on the Smarts Service Assurance Manager console.

Follow these steps to install the client for the adapter for Smarts Manager on the Linux environment.

1 Run the Smarts Integration adapter client installer. The installer is available in the Adapters directory in the Network Configuration Manager distribution media.

```
bash VMware_Smart_Assurance_Manager_Integration_Module_Client_X.X.X.X.XXX_Linux.bin
```

2 At the Introduction window, press Enter or click Next.

3 At the Choose Install Folder window, type:

For Linux: /opt/InCharge/CONSOLE/smarts/local/actions/client

4 At the Network Configuration Manager IP Address window, type the IP Address or the fully qualified hostname of the Network Configuration Manager Application server. Press Enter or click Next.

5 At the Web Browser window, type the full path to a web browser program on this server. Press Enter or click Next.

For example: If using the Mozilla Firefox web browser, select the default of: /usr/bin/firefox

6 At the Summary window, review the information, then Press Enter or click Next. The client for the adapter for Smarts installation process begins. After installation, the following message appears: Smarts Manager Integration Module Client has been successfully installed.

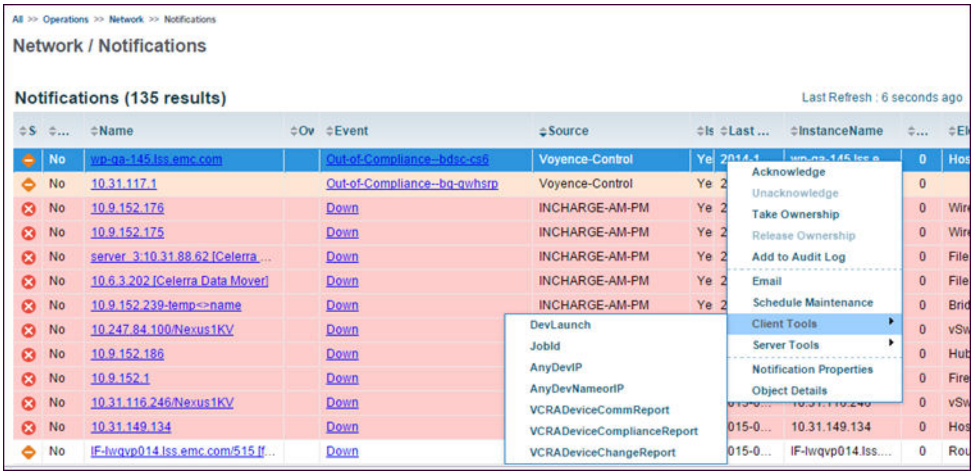
Reinstall the Smarts Manager Integration Module, if:

- There are errors during the installation
- Network Configuration Manager needs to be updated.

Setup for M&R GUI contextual launch

The contextual launch appears under a context menu option Client Tools. The following figure shows the EMC M&R GUI with the Client Tools menu.

Figure 8-3. Launch Smarts Manager from EMC M&R



All >> Operations >> Network >> Notifications

Network / Notifications

Notifications (135 results)

Last Refresh : 6 seconds ago

S	...	Name	Ov	Event	Source	Is	Last ...	InstanceName	...	El
⊖	No	wp-qa-145.lss.emc.com		Out-of-Compliance--bdsc-cs6	Voyence-Control	Ye	2014-1...	wp-qa-145.lss.e...	0	Hos
⊖	No	10.31.117.1		Out-of-Compliance--bq-qwhsrp	Voyence-Control	Ye	2		0	
⊗	No	10.9.152.176		Down	INCHARGE-AM-PM	Ye	2		0	Wir
⊗	No	10.9.152.175		Down	INCHARGE-AM-PM	Ye	2		0	Wir
⊗	No	server_3:10.31.88.62 [Celerra ...		Down	INCHARGE-AM-PM	Ye	2		0	File
⊗	No	10.6.3.202 [Celerra Data Mover]		Down	INCHARGE-AM-PM	Ye	2		0	File
⊗	No	10.9.152.239-temp<>name		Down	INCHARGE-AM-PM	Ye	2		0	Brid
⊗	No	10.247.84.100/Nexus1KV		Down					0	vSw
⊗	No	10.9.152.186		Down					0	Hub
⊗	No	10.9.152.1		Down					0	Fire
⊗	No	10.31.116.246/Nexus1KV		Down					0	vSw
⊗	No	10.31.149.134		Down			015-0...	10.31.149.134	0	Hos
⊖	No	IF-lwqvp014.lss.emc.com/515 [f...		Down			015-0...	IF-lwqvp014.lss....	0	Rou

Use the following steps to configure the information to appear in the Client Tools list for launching the Smarts Manager.

1 Using the EMC M&R GUI, install the SolutionPack for VMware Smart Assurance Manager.

2 Edit the **SmartsTools.json**file: located in the following path:

<MnR Install Dir>/Custom/WebApps-Resources/Default/conf/

For example:

Linux: /opt/APG/Custom/WebApps-Resources/Default/conf/

3 Follow instructions in the file to configure the information to appear in the contextual launch under the Client Tools menu option. An example is included in the file.

Client tools

The following tables contain the settings appropriate for each client tool:

- NCM device Info client tool
- NCM job info client tool
- NCM Query Client Tool
- Device communication report client tool
- Device change report client tool
- Device compliance report client tool
- NCM Device query client tool

Follow the steps in Configuring the Service Assurance Manager (SAM) dashboard (web client) by entering the appropriate values at each step. Note that the program name has a **.sh** suffix for Linux.

NCM device Info client tool

Note The attributes and values have changed for the client tools configuration for contextual launch. Those changes are:

- Attribute: **Source**
- Value: **Voyence-Control**

Name	NCM Device Info
Description	Launches Network Configuration Manager from a notification directly to the device to which the notification was associated
Program	VCDeviceLaunch
Context criteria	**Context object**: ICIM_Notification **Attribute**: User Defined 5 **Value**: [a-zA-Z0-9]* **Attribute**: Source **Value**: Voyence-Control
Status criteria	**Context object**: ICIM_Notification

NCM job info client tool

Note The attributes and values have changed for the client tools configuration for contextual launch. Those changes are:

- Attribute: **Source**
- Value: **Voyence-Control**

Name	NCM Job Info
Description	Launches Network Configuration Manager from a notification directly to the job listed in the notification
Program	VCJobLaunch
Context criteria	**Context object**: ICIM_Notification **Attribute**: User Defined 7 **Value**: [a-zA-Z0-9]* **Attribute**: Source **Value**: Voyence-Control
Status criteria	**Context object**: ICIM_Notification

NCM Query Client Tool

Name	NCM Query
Description	Launches Network Configuration Manager attempting to look up a device based upon device name or IP address. The client tool is named Network Configuration Manager Query, because devices in Network Configuration Manager may or may not match criteria passed into the tool.
Program	VCGenericDeviceLaunch
Context criteria	**Context object**: ICIM_Notification Attribute: Class **Value**: Router|Switch|Firewall|Interface
Status criteria	**Context object**: ICIM_Notification

Device communication report client tool

The attributes and values have changed for the client tools configuration for contextual launch. Those changes are:

- Attribute: **Source**
- Value: **Voyence-Control**

Name	Device Communication Report
Description	This is a record of the communications between Network Configuration Manager and the device. The main purpose of this is to show outages.
Program	VCRADeviceCommReport
Context Criteria	**Context object**: ICIM_Notification **Attribute**: User Defined 6 **Value**: [a-zA-Z0-9]* **Attribute**: User Defined 4 **Value**: [a-zA-Z0-9]* **Attribute**: Source **Value**: Voyence-Control
Status Criteria	**Context object**: ICIM_Notification

Device change report client tool

The attributes and values have changed for the client tools configuration for contextual launch. Those changes are:

- Attribute: **Source**
- Value: **Voyence-Control**

Name	Device Change Report
Description	This shows a history of configuration changes on the device in the last 24 hours. **Note** By editing the unitsBackParam in the script, the number of days covered by the report can be altered.
Program	VCRADeviceChangeReport
Context criteria	**Context object**: ICIM_Notification **Attribute**: User Defined 6 **Value**: [a-zA-Z0-9]* **Attribute**: User Defined 4 **Value**: [a-zA-Z0-9]* **Attribute**: Source **Value**: Voyence-Control
Status criteria	**Context object**: ICIM_Notification

Device compliance report client tool

The attributes and values have changed for the client tools configuration for contextual launch. Those changes are:

- Attribute: **Source**

- Value: **Voyence-Control**

Name	Device Compliance Report
Description	This is a history of the compliance or non-compliance of the device with policies in Network Configuration Manager.
Program	VCRADeviceComplianceReport
Context criteria	**Context object**: ICIM_Notification **Attribute**: User Defined 6 **Value**: [a-zA-Z0-9]* **Attribute**: User Defined 4 **Value**: [a-zA-Z0-9]* **Attribute**: Source **Value**: Voyence-Control
Status criteria	**Context object**: ICIM_Notification

NCM Device query client tool

Name	NCM Device Query
Description	Launches Network Configuration Manager, attempting to look up a device, based upon device name or IP address. This version is for use by the topology browser and the map view. The client tool is named **NCM Device Query**, because devices in Network Configuration Manager may or may not match criteria passed into the tool.
Program	VCGenericDeviceLaunchForTopo
Context criteria	**Context object**: UnitaryComputerSystem
Status criteria	**Context object**: UnitaryComputerSystem

Configuring the Service Assurance Manager (SAM) dashboard (web client)

Instructions on configuring the web client to use client tools are mentioned in the *VMware Smart Assurance Service Assurance Manager Dashboard Configuration Guide .* The guide is the definitive source for configuring client tools. However, a short version is presented here for a standalone client.

Since the dashboard is launched via the browser, the client tool scripts must be located on the machine from where the browser is launched (or accessible through a mapped network drive).

Step	Action
1	Create a **/actions/client** directory under your local directory. For Linux: /opt/InCharge/CONSOLE/smarts. This is where the client tool scripts are copied. **Note** See a complete list of tools in the *"Client tools" on page 188*.
2	Add the following parameters to the dashboard.properties file, located in the directory: For Linux: /opt/InCharge/CONSOLE/smarts/local/tomcat/webapps/templates ■ com.smarts.clientToolsInApplet=true ■ com.smarts.webconsole.sitemod=/mylocaldirectory
3	Add the following parameters to the webconsole.properties file, located in the following directory: For Linux: /opt/InCharge/CONSOLE/smarts/tomcat/webapps/webconsole ■ com.smarts.clientToolsInApplet=true ■ com.smarts.webconsole.sitemod=/mylocaldirectory
4	Copy the client tool scripts from the /opt/InCharge/CONSOLE/smarts/local/actions/client for Linux systems to your local machine, and place them in the directory you created in step 1.

For more information, the “Additional Viewlet Properties” section in the *VMware Smart Assurance Service Assurance Manager Dashboard Configuration Guide* contains additional details.

Advanced configuration

Customizing notifications

The adapter installs a self-contained Tomcat instance. There is an XML file in the webapps directory (where the adapter is deployed) named Smarts Manager_Transform.xml. This file is the mapping definition of raw Network Configuration Manager events to the properties used by the integration adapter.

In this file, there are some fields that could be customizable at the installation site.

- **Severity** – This is the severity level of the event in the notification log console. 5 is the lowest or normal severity, and 1 is the highest or critical severity
- **EventName** – this is the value shown in the Event column in the notification log
- **EventText** – this is the description of the event shown inside the event details
- **Expiration** – expiration time in the notification console
- **Durability** – modify only if you have an understanding of these settings in the notification console
- **Category** - modify only if you have an understanding of these settings in the notification console
- **ClearOnAcknowledge** - modify only if you have an understanding of these settings in the notification console

- **Source** – only time you might want to modify this is if for some reason, multiple adapters are in use for the same SAM instance

  Note Modifying any other field is not advisable.

User-defined fields

There are many user-defined fields in the event notifications populated by the adapter. The adapter requires these fields to be populated for the contextual launch to function correctly. These settings are only needed if there is a possible conflict with user-defined fields in Event Notifications.

By default, the fields are mapped to the same values expected by the client tool launch scripts. These can be changed, however the scripts for contextual launch must also be modified to use the new user defined fields.

Note It is advisable that these user-defined fields remain unchanged. Only in the case of conflicts should the installer take on the additional burden of reconfiguring the contextual launch scripts and the user-defined fields. If you need to change these, use the following chart, which shows the default configuration out of the box.

Field	Value
User Defined 3	Network name (not needed by scripts; can be turned off)
User Defined 4	Network D (needed only for tools that launch reports)
User Defined 5	Device Name
User Defined 6	Device ID (needed only for tools that launch reports)
User Defined 7	Job Number

When changing the user-defined fields, follow these steps:.

Step	Action
1	Using the adapter configuration console, change assignments of the user-defined fields. Complete your own chart for the new values that you configure.
2	On the Smarts Manager client machine, find the directory for client tools. The default location is For Linux: /opt/InCharge/CONSOLE/smarts/local/actions/client
3	For each script that begins with VC, edit the scripts, and reassign the user-defined values according to the chart you create.

Uninstall instructions

Linux

Use the following steps to uninstall the adapter for Smarts Manager on Linux environments:

Step	**Action**
1	Change the Directory to **[Product Directory]/software/Uninstall_NCMSmartsAdapter/**.
2	Type bash **Uninstall_VMware_Smart_Assurance_Manager_Integration_Module**.
3	Press **Enter**.

Uninstall instructions for client tools for Service Assurance Manager (SAM)

Use the following steps to uninstall the adapter for Smarts Manager on Linux environments:

1 To begin the uninstall procedure; delete the following files located in the directory:

For Linux: /opt/InCharge/CONSOLE/smarts/local/actions/client

Note The file extension for Linux the extension is **.sh**.

- VCDeviceLaunch
  - VCGenericDeviceLaunch
  - VCGenericDeviceLaunchForTopo
  - VCJobLaunch
  - VCRADeviceChangeReport
  - VCRADeviceCommReport
  - VCRADeviceComplianceReport

2 Continue with the following steps.

Step	Action
1	Access the Client tools location. Click the **Global Manager Administration Console** tab.
2	Access the Tools listing by selecting **Tools**.
3	Select the Client Tools listing. From Tools, select **C Client**.

4	Right-click on *each* of the following Client Tool names, then click **Delete** to uninstall each Client Tool. ■ Network Configuration Manager Device Info ■ Network Configuration Manager Job Info ■ Network Configuration Manager Query ■ Device Communications Report ■ Device Change Report ■ Device Compliance Report ■ Network Configuration Manager Device Query
5	Now, restart the VMware Smart Assurance Service Assurance Manager Server Service. **Note** The *VMware Smart Assurance Installation Guide for SAM, IP, ESM, MPLS, and NPM Managers* gives details on how to restart the VMware Smart Assurance Service Assurance Manager Server services on other platforms.

Integration modules configuration

9

Read the following topics next:

- Introducing the Integration Adapters
- JMiniX Console
- Supported Events
- Transform Definition File
- Flat File Integration adapters
- Email Integration adapters
- Generic SNMP Integration adapters
- Launching the application through a URL

Introducing the Integration Adapters

The Network Configuration Manager Integration Adapters output data is in the form of events. These are a subset of the events in the event manager used to track all activities occurring in the system. Many of these events are then available to external programs or applications through various transports.

The following integration adapters are available:

- SNMP (Traps or MIBs)
- SMTP (Email)
- JMS (An asynchronous messaging protocol)
- File (Simple file output)

  The integration adapters listen to the internal Network Configuration Manager events, and transform them into a form appropriate for the transport. For example, an event is transformed into a MIB structure for the SNMP adapters, and is also transformed into an XML document for the JMS adapters.

The SNMP, File, and Email adapters have filters that allow an administrator to choose the events that will be output by the adapters. See Updating configuration using the JMiniX Console. This is a common administrative task.

The format of this data can be customized. This is considered an advanced configuration task for experienced users.

The JMS adapter is different than the other adapters, in that there is no filtering or customization, because it is the basis of the other adapters. A listener to the JMS adapter is advised to only acknowledge events in which they are interested. The code samples in the API area show examples of selectively listening to JMS messages.

The following sections on administration and customization apply to the SNMP, SMTP, and File integration adapters, but not to a JMS adapter.

Integration adapters installation

The Network Configuration Manager installation program installs the SNMP, SMTP, and File integration adapters with default configuration settings. No additional installation steps are required.

Integration adapters configuration and management

The configuration MBeans for the adapters are available in the JMiniX Console after the Network Configuration Manager installation completes. The JMiniX Console also provides management functions, including starting and stopping the adapters.

JMiniX Console

All integration adapters use a **common administration mechanism**, based on JMX. The JMX Mini (JMiniX) console provides an interface for changing configuration attributes in MBeans and for invoking management operations, including starting and stopping the adapters.

Accessing the JMiniX Console

To access the JMiniX Console:

1 Supply the following URL to your favorite browser:

```
https://<NCM_server>:8880/ncm-webapp
```

2 Provide a Username and Password on the login screen.

The JMiniX Console uses the Tomcat BASIC authentication, which caches user credentials and roles until you close the browser. If you logged in previously and then closed the tab, but not the browser, you are still authenticated.

3 In the navigation tree, expand the servers node and then expand server 0.

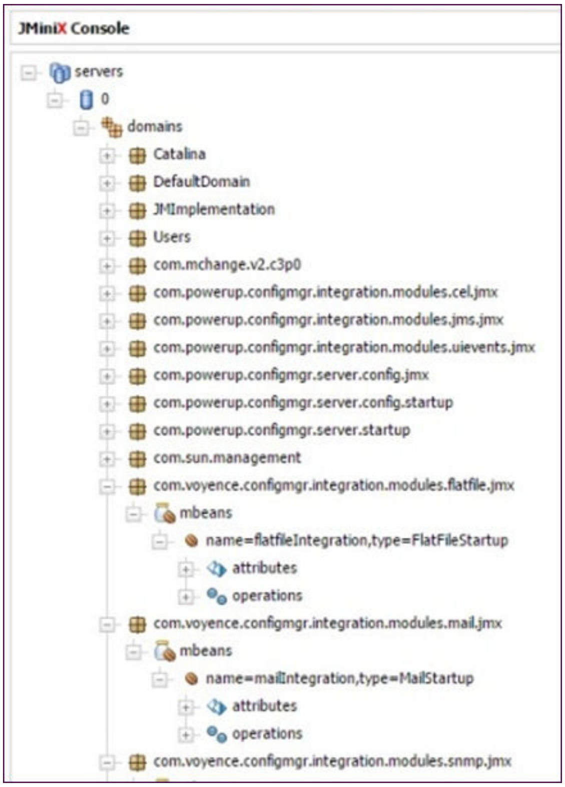
The JMiniX Console can monitor beans for multiple servers. In the navigation hierarchy, each server is numbered, starting with zero (0).

To completely log off of the JMiniX Console, close the browser.

Updating configuration using the JMiniX Console

To change an integration module’s configuration, use the JMiniX Console to access attributes in the MBean.

1 In the navigation tree, expand **servers >0 >domains >com.voyence.configmgr.integration.modules.** *module_name* **.jmx >mbeans**


JMiniX Console
servers
0
domains
Catalina
DefaultDomain
JMImplementation
Users
com.mchange.v2.c3p0
com.powerup.configmgr.integration.modules.cel.jmx
com.powerup.configmgr.integration.modules.jms.jmx
com.powerup.configmgr.integration.modules.uievents.jmx
com.powerup.configmgr.server.config.jmx
com.powerup.configmgr.server.config.startup
com.powerup.configmgr.server.startup
com.sun.management
com.voyence.configmgr.integration.modules.flatfile.jmx
mbeans
name=flatfileIntegration,type=FlatFileStartup
attributes
operations
com.voyence.configmgr.integration.modules.mail.jmx
mbeans
name=mailIntegration,type=MailStartup
attributes
operations
com.voyence.configmgr.integration.modules.snmp.jmx

2 Under mbeans, expand the **name=**node, and then expand **attributes**.

The attributes are the configurable parameters (besides events) specific to each integration adapter.

These may consist of any number of parameters. For example, it is common to find a hostname attribute. Generally, this is the hostname or IP address of the remote system.

3 Change the values of one or more attributes using the table in the right pane.

4 Click **Apply Changes**when you have all the values set properly.

5 Start or restart the integration module as described in Starting or restarting integration modules

Note You must restart the integration module for the changes to take effect.

6 Close the browser (not just the browser tab) to log out of the JMiniX Console.

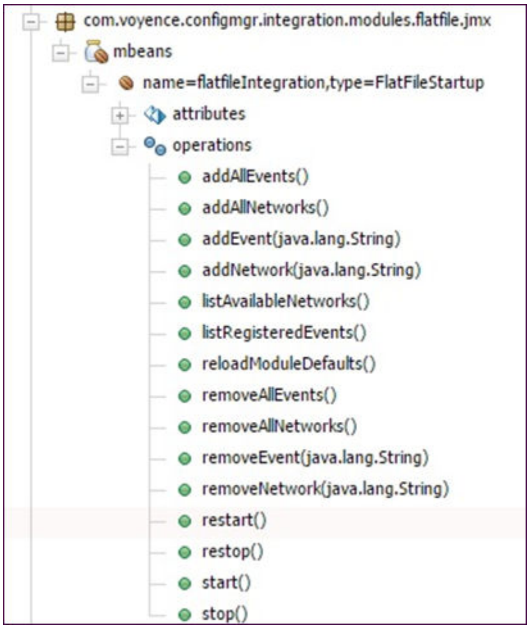
Starting or restarting integration modules

To start, stop, or restart an integration module, access the operation in the module's MBean.

1 In the navigation tree, click **servers >0 >domains >com.voyence.configmgr.integration.modules.** *module_name* **.jmx >mbeans**

2 Under mbeans, expand the **name=**node, and then expand **operations**.

A list of operations appears.



```
com.voyence.configmgr.integration.modules.flatfile.jmx
  mbeans
    name=flatfileIntegration,type=FlatFileStartup
      attributes
      operations
        addAllEvents()
        addAllNetworks()
        addEvent(java.lang.String)
        addNetwork(java.lang.String)
        listAvailableNetworks()
        listRegisteredEvents()
        reloadModuleDefaults()
        removeAllEvents()
        removeAllNetworks()
        removeEvent(java.lang.String)
        removeNetwork(java.lang.String)
        restart()
        restop()
        start()
        stop()
```

3 Click an operation to open it in the right pane. For example, click **restart()**or **start()**.

4 In the right pane, click **Execute**to run the operation.

Integration adapters management operations

The following is a brief description of some of the integration module management operations. Note that preceding the event, you may see java language references to return types. These include the word **void** or **java.lang.String**. Ignore these types. They are a by-product of the automation framework.

Operation	Description
removeEvent()	Used to remove an event from the list of events the adapters is already listening for

start()	Used to start the integration adapters. If the adapters is already running, this operation silently returns.
addEvent()	Used to add an event to the list of events the adapters should listen to
reloadModuleDefaults()	Used to read the integration adapters' configuration file from the disk
restart()	Used to restart the integration adapters. This operation is equivalent to completing a stop() operation, and then a start() operation.
stop()	Used to stop the integration adapters. If the adapters is not running, this operation silently returns.
listRegisteredEvents()	Used to display the core Network Configuration Manager events that the adapters is listening for, and lists all the supported events.

Any changes made through the JMiniX Console take effect only *after* a restart of the Integration adapters.

Managing events

Integration adapters react to events from the Network Configuration Manager. Part of the integration adapters framework includes listeners that can be managed from the JMiniX Console.

1 To see the events that the integration adapters is currently listening to, select the **listRegisteredEvents** management function.

   It is important to understand the scenarios you are interested in configuring *before* making changes to the events. Although there is no harm in adding or removing events to the system, it may have unintended consequences. Not all events supported by a adapters make sense for your system.

   For example, the **AuthorizationSucceededEvent** is supported by a number of integration adapters. However, rarely does it make sense in a normal installation to react to that event.

   If you are administering the Email integration adapters, and select to listen for this event, the Network Configuration Manager gives you a vigorous stream of unwanted spam for a heavily trafficked system.

2 The way to add or remove an event, is to **cut** it from the list of events, and paste it into the **addEvent** or **removeEvent** operation.

3 **Copy** the event from the events list.

4 Locate the **addEvent** or **removeEvent** operation, and **paste** it into the test box.

5 Select **Invoke** after you pasted the event.

6 Do not forget to **restart the integration adapters** after you have finished adding or removing events.

   That completes administering Network Configuration Manager integration adapters. Parameters specific to each integration adapters are covered in the integration adapters guide for your adapters.

Supported Events

The following information details the supported events.

While certain events are fired based on a single, discrete user action, there are other events that can be fired, based on several discrete actions.

The following table is intended to provide additional insight as to the types of actions (user or otherwise) that can cause events to be fired.

Note All integration adapters may not support all the events listed below. Go to the JMX-Console, and check under the list of supported events to get an exact list for a particular integration adapters.

By default, events are not published for backward compatibility to the 3.6 topic, although it can be configured through the JMiniX Console as follows:

1. Scroll down and find the mbean operation **setConfigItem**(), and set the parameters as follows:
   - p1 = config.server
     - p2 = com.powerup.configmgr.eventframework.transformer.event_3_6_transform
     - p3 = true
2. Click **Invoke** to set this parameter. The next page will display a success message:

   ```
   Config item
   config.server:com.powerup.configmgr.eventframework.transformer.event_3_6_transform
   is set to true
   ```

3. Follow the Back to MBean Viewlink.
4. Scroll down, and locate the mbean operation **saveAll().**
5. Click **Invoke** to permanently save your changes.

The types of actions that can cause events to be fired

Event	Stimulus that causes firing
AuthorizationFailedEvent	Unsuccessful authorization check to a protected resource
CommunicationRestoredEvent	When the communication to the device has been restored
CredentialsCreateEvent	When a credential gets created
CredentialsModifyEvent	When a credential gets modified
CredentialsDeleteEvent	When a credential gets deleted

DSIPOverrideEvent	When the Device server’s IP Address is overridden
DSIPRestoreEvent	When the Device server’s IP Address is restored
DataFileCreateEvent	When a datafile is created
DataFileDeleteEvent	When a datafile is deleted
DataFileModifyEvent	When a datafile is modified
DeviceCompliantEvent	When a device is compliant. Includes a list of policies run for compliancy check
DeviceCreateEvent	Device create event
DeviceConfigurationChangeEvent	Device configuration change
DeviceConfigurationUnitChangeEvent	Device configuration unit change
DeviceCutThruInitiatedEvent	When a cut-thru is initiated to a device
DeviceDeleteEvent	When a design device in a workspace is deleted. This does not apply to operational devices.
DeiceLockBreakEvent	When a device lock is broken by a system administrator
DeviceLockSuspendEvent	When a device lock is suspended by a system administrator
DeviceRevisionCreateEvent	Successful auto-discovery completion
DeviceLockingSystemTurnedOffEvent	When the device locking feature is turned off
DeviceLockingSystemTurnedOnEvent	When the device locking feature is turned on
DeviceNameChangeEvent	When the device name is changed
DeviceNonCompliantEvent	When the device goes out of compliant. A List of successful policies and a list of failed policies are included.
DeviceOutOfSyncEvent	When the configuration of a device in a network is out-of-sync with the same device in a Workspace
DevicePWChangeEvent	When a device password is changed
DeviceReturnToSyncEvent	When the configuration of a device in a network is back in sync with the same device in a Workspace
DevicePolicyCheckFailedEvent	When a policy check fails on a particular device
DevicePolicyCheckSuccessful	When a policy check is successful on a particular device
DeviceNewConfigurationStateEvent	When a new revision is created on a device

DeviceServerModifyEvent	When a Device server is modified
DeviceStartConfigOutOfSyncEvent	When a configuration on the device is out-of-sync with the run config.
DeviceStatusChangeEvent	When the status of the device changes
DuplicateIPEvent	When the IP address being used is already in use
FailedCommunicationEvent	When communication fails to a particular device
GroupCreateEvent	When a new user group gets created
GroupDeleteEvent	When a group gets deleted
GroupImportedEvent	When a group gets imported into the system
GroupModifyEvent	When a group gets modified
JobApprovedEvent	When a job gets approved
JobCancelledEvent	When a job gets cancelled
JobCompletedEvent	When a job completes successfully
JobFailedEvent	When a job fails to execute
JobHeldEvent	When a job is put on hold
JobPartiallyFailedEvent	When a job fails partially
JobRemovedEvent	When a job is deleted
JobRunEvent	When a job goes to running state
JobRunManuallyEvent	When a job is run manually
JobScheduledEvent	Reaction of a push, pull, or auto-discovery job (that is not spot-approved), via UI
JobUpdateEvent	Approval of a scheduled push, pull, or auto-discovery job, or creation of a spot-approved push, pull, or auto-discovery job
JobConflictEvent	When there are conflicting jobs already scheduled on a particular device
NetworkCreateEvent	Creation of a network
NetworkUpdateDevicesEvent	Successful completion of auto-discovery job, and by managing devices, via the UI
NetworkModifyEvent	Modification of a network
NetworkDeleteEvent	Deletion of a network
PolicyCreateEvent	When a new compliance policy is created
PolicyDeleteEvent	When a compliance policy is deleted

PolicyModifyEvent	When a compliance policy is modified
PullCompletedEvent	When a pull has successfully completed
PullSpecsCompletedEvent	When a hardware pull has successfully completed
PushCompletedEvent	When a push job has completed successfully
RunQuickCommandEvent	When a quick command is run on a device
RunSavedCommandEvent	When a save command is run on a device
SavedCommandCreateEvent	When a save command is created
SavedCommandModifyEvent	When a save command is modified
SavedCommandDeleteEvent	When a save command is deleted
SiteAccessEvent	When a site is accessed
SiteCreateEvent	When a new site is created
SiteDeleteEvent	When a new site is deleted
SiteAddDevicesEvent	Addition of devices to a site, via the UI
SiteDeleteDevicesEvent	Removal of device from a site, via the UI
SiteUpdateDevicesEvent	Devices have been added/removed from a site
SiteNameChangeEvent	When the name of a site is changed
SiteImportedEvent	When a list of devices are imported into a site
JobCompletedEvent	When a push, pull, or auto-discovery job completes without errors
JobConflictEvent	When a push job is scheduled or spot-approved, and that job contains one or more devices referenced in one or more other currently scheduled push jobs
JobFailedEvent	When all the tasks of a push, pull, or auto-discovery job fail
JobPartiallyCompletedEvent	When one or more-but not all- tasks of a push, pull, or auto-discovery job fail
TaskCompleteEvent	When a task associated with a push, pull, or auto-discovery job completes without errors
TaskFailedEvent	When a task associated with a push, pull, or auto-discovery job fails
TaskHeldEvent	When a task moves to Hold status
TaskRemovedEvent	When a task is removed
TaskRunEvent	When a task is run

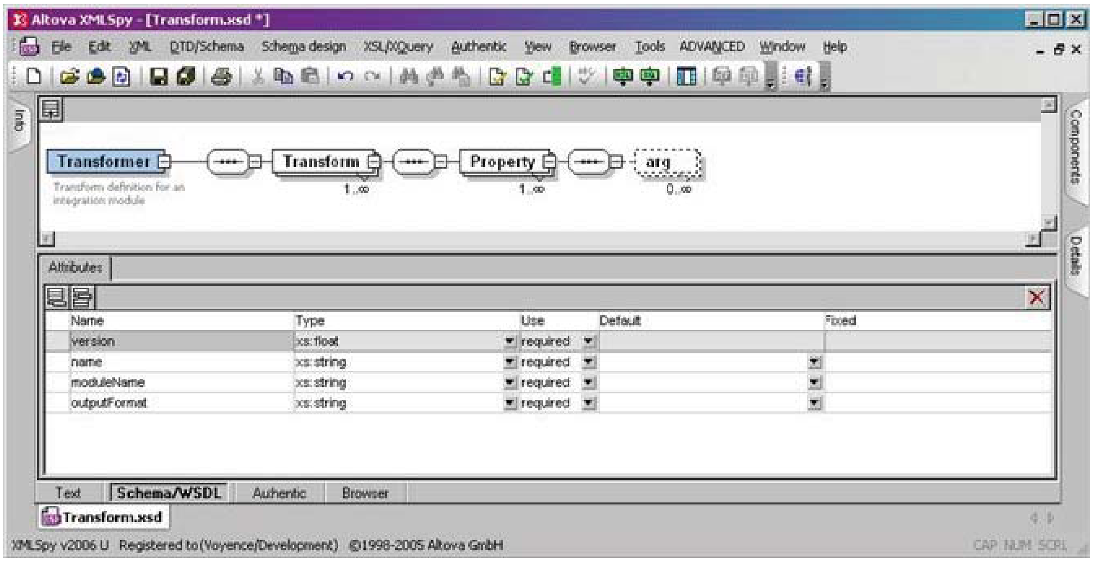
TemplateCreateEvent	When a new template is created
TemplateModifyEvent	When a template is modified
TemplateDeleteEvent	When a template is deleted
TestCreateEvent	When a config audit test is created
TestDeleteEvent	When a config audit test is deleted
TestModifyEvent	When a config audit test is modified
UserCreateEvent	When a new user is created
UserDeleteEvent	When a user is deleted from the system
UserImportedEvent	When a user is imported into the system
UserLockedOutEvent	When a user gets locked out because of too many unsuccessful login attempts
UserLoginEvent	Successful user login
UserLoginExpiredEvent	When a user’s login expires after a period of inactivity
UserLoginFailedEvent	Unsuccessful user login
UserLogoutEvent	When a user logs out of the system
UserModifyEvent	When a user is modified
ViewAccessEvent	When a view is accessed
ViewCreateEvent	When a new view is created
ViewDeleteEvent	When a view is deleted
ViewModifyEvent	When a view is modified
VersionCreateEvent	Creation of a version, via the UI
VersionChangeEvent	When version changes on a device
VersionRemoveEvent	When a version is removed on a device
voyenceEventDeviceConfigurationChangeEvent	When a change has been made to a device's configuration
voyenceEventDeviceConfigurationUnitChangeEvent	When a Configuration Unit is changed on a new Device State
WorkspaceAccessEvent	When a workspace is accessed
WorkspaceCreateEvent	When a new workspace is created
WorkspaceDeleteEvent	When a workspace is deleted
WorkspaceModifyEvent	When a workspace is modified

Transform Definition File

This section details information for the transform definition file.

The Flat file integration adapters, Mail integration adapters, and SNMP integration adapters use a transform definition file that converts the Network Configuration Managerevent into an integration adapters specific format (such as, to a string for Flat file, a set of properties for Mail, and a Trap for SNMP).

Following is the schema for the Transform Definition.


Altova XMLSpy - [Transform.xsd *]
File Edit XML DTD/Schema Schema design XSL/XQuery Authentic View Browser Tools ADVANCED Window Help
Info
Components
Details
Transformer
Transform definition for an integration module
Transform
1..∞
Property
1..∞
arg
0..∞
Attributes
Text Schema/WSDL Authentic Browser
Transform.xsd
XMLSpy v2006 U Registered to (Voyence/Development) ©1998-2005 Altova GmbH
CAP NUM SCRL

Name	Type	Use	Default	Fixed
version	xs:float	required		
name	xs:string	required		
moduleName	xs:string	required		
outputFormat	xs:string	required		

- Each Transformer has one or more transforms, depending on the number of events supported by the integration adapters.
- Each Transform has one or more property nodes. Each property node can have key, value, type, and formatter attributes.
- The attribute “key” is returned as the key in the output Properties object. The value for this key is dependent on the type of attribute.

  The following information is a brief explanation on each of the valid types, and how the other property attributes relate to that type.

XPATH

When the type attribute is XPATH, the value attribute has an **XPath** used to evaluate its value from the incoming event. You can specify a formatter (a Java class, which is accessible through classpath) to format the value returned through the XPath evaluation.

Typical use cases for a formatter are:

- Format a collection of nodes into a string
- Format a Date into a different format

- Format a Map into a string

  For Example:

  ```
  <Transform eventName="DeviceDeleteEvent">
  <Property name="deviceName" type = "XPATH"
                   value = "/VoyenceEvent/Device/DeviceDeleteEvent/DeviceId/OID"/>
  </Transform>
  ```

CONSTANT

When the type attribute is CONSTANT, the value attribute is the constant value itself. This type is used mostly to pass static values to your Transport. For example, the trap name for a particular event in SNMP.

For Example:

```
<Transform eventName = "DeviceDeleteEvent">
  <Property name="ORIGINATOR" type="CONSTANT" value="NCM"/>
</Transform>
```

VARSTRING

When the type attribute is VARSTRING, the value attribute is a String with predefined variables that is substituted using the “arg” node. For example, you could have a Property with a type equal to VARSTRING, and a value equal to “Device {0} deleted from Network {1}”.

The “arg”s defined inside the property node defines how attributes {0} and {1} are evaluated. Arguments follow the same style as property nodes. The types that are allowed for Arg nodes are CONSTANT and XPATH.

For Example:

```
<Transform eventName = "DeviceDeleteEvent">
      <Property name="EVENTSTRING" type="VARSTRING"
value="Device {0} deleted from Network {1}">
<arg key="0" value="/VoyenceEvent/Device/DeviceDeleteEvent/DeviceId/Name"/>
<arg key="1" value="/VoyenceEvent/Device/DeviceDeleteEvent/NetworkId/Name"/>
        </Property>
</Transform>
```

VELOCITY

When the type attribute is VELOCITY, the value attribute corresponds to the name of the Velocity Template. “Arg” nodes can be used to pass values from the event to the Velocity Template. For example, you could have a velocity template for a DeviceDeleteEvent, (for instance, device_delete.vm), which contains the text Device $deviceName deleted from Network $networkName.

You could pass the values for deviceName and networkName as arguments to this template by defining two “arg” nodes with type = XPATH and value = <the xpath to the deviceName/ networkName node>

For Example:

```
<Transform eventName = "DeviceDeleteEvent">
      <Property name="body" type="VELOCITY"
value="device_delete_body.vm">
<arg key="0" value="/VoyenceEvent/Device/DeviceDeleteEvent/DeviceId/Name"/>
<arg key="1" value="/VoyenceEvent/Device/DeviceDeleteEvent/NetworkId/Name"/>
        </Property>
</Transform>
```

Flat File Integration adapters

The Network Configuration Manager Flat File Integration adapters is a component providing the ability to listen for Network Configuration Manager events, transforming them into a formatted string, and writing them to a flat file.

The primary use of this integration adapter is to provide a serialized stream of events to a file that can then be read and used by systems external to the Network Configuration Manager. This would typically be the case where a messaging type infrastructure is not available, but messaging style integration is desired.

Flat file Integration adapters assembly

For each event that can be fired by the core the Network Configuration Manager server, there is a corresponding transform definition inside an XML file that takes the native event and transforms it into a formatted string representing the event handled. This formatted string represents the information that is written to the flat file.

The format of the event string is defined inside the transform file **Flatfile_Transform.xml** located in the following directory:

$VOYENCE_HOME/ncmcore/webapps/ncm-webapp/WEB-INF/classes

This file is set up to map one Network Configuration Manager event to a set of name-value pairs. The Generic Flatfile Transformer reads the transform definition for a particular event, and builds a Properties object. In case of a flat file, the resulting Properties object would contain an entry with a key as EVENTSTRING, and value as the transformed event.

The flat file transport takes the transformed event, and writes it to the end of a file. The file name is specified by the Flat File Integration adapters XML configuration file.

Data written to a file by the flat file transformer, is done in a concurrent, access-safe manner. This allows the consumer of data contained in the file to adopt a locking strategy that ensures there are no race conditions, with respect to reading and/or modifying data from the file.

Flat file integration adapters configuration

The installation program of the Flat File Integration adapters prompts for the values, as listed in the following table.

Element	Description	Required or optional	Default value
<filename>	Specifies the fully qualified file name that events are written to	required	/opt/smarts-ncm/logs/flat_file.log
<enable-file-rolling>	Specifies whether to roll the event file, based upon a file line count threshold	optional	True
<permissions>	Specifies the permission of the flat file the events are being written to	required	755
<roll-threshold>	Number of lines that are written to the flat file before rolling over a new file	required	10000

After the initial installation, the configuration parameters can be edited using the JMX console. Transform Definition File provides more information.

Note You must restart the integration module for the changes to take effect.

Tailoring the flat file integration adapters

The initial configuration of the Flat File Integration adapters is setup to **listen** for the following events:

- AuthorizationFailedEvent
- DeviceNewConfigurationStateEvent
- DeviceConfigurationChangeEvent
- DevicePWChangeEvent
- DeviceRevCreateFailedEvent
- JobFailedEvent
- JobPartiallyFailedEvent
- TaskFailedEvent
- UserLoginFailedEvent

  When these events are fired by the core Network Configuration Manager service, the Flat File Integration adapters receives the event, converts the event into a properly formatted string, and writes the event to the file specified by the configuration.

The most common form of tailoring functionally includes adding new events, removing existing events, updating the event file name, enable file rolling, roll threshold, and file permissions. The tailoring can be accomplished through the JMX console.

Note You must restart the integration module for the changes to take effect.

Modifying the transform definition

Although not recommended, a power user who understands XML and the Transform Definition (XSD) could customize the format of the data written to the event file. Transform Definition File provides more information. Ensure that you **restart the Flat File Integration adapters** for your changes to take effect.

Flat file integration adapters administration

Administration of the Flat File Integration adapters is completed through the JMX-Console. See *"Updating configuration using the JMiniX Console" on page 199* for more information.

Default file format

The following information illustrates the default format of the events file. Each line represents what each event displays as, when written to the file.

```
NetworkCreateEvent: networkId=<OID>, networkName=<name>, networkCreator=<user name>,
timestamp=<long datetime>
NetworkDeleteEvent: networkId=<OID>, networkName=<name>, networkDeleter=<user name>,
timestamp=<long datetime>
NetworkUpdateDevicesEvent: networkId=<OID>, networkName=<name>, addedDevices=[<deviceId=OID/
deviceName=name, deviceId=OID/deviceName=name, ...>], removedDevices=[<deviceId=OID/
deviceName=name, deviceId=OID/deviceName=name, ...>], networkUpdator=<user name>,
timestamp=<long datetime>
DeviceCreateEvent: networkId=<OID>, networkName=<name>, deviceId=<OID>, deviceName=<name>,
deviceCreator=<user name>, timestamp=<long datetime>
DeviceDeleteEvent: networkId=<OID>, networkName=<name>, deviceId=<OID>, deviceName=<name>,
deviceDeleter=<user name>, timestamp=<long datetime>
DevicePWChangeEvent: networkId=<OID>, networkName=<name>, deviceId=<OID>, deviceName=<name>,
timestamp=<long datetime>
DeviceRevisionCreateEvent: networkId=<OID>, networkName=<name>, deviceId=<OID>,
deviceName=<name>, revisionId=<OID>, revisionNumber=<long>, timestamp=<long datetime>
DeviceRevCreateFailedEvent: networkId=<OID>, networkName=<name>, deviceId=<OID>,
deviceName=<name>, timestamp=<long datetime>
InternalDeviceRevChangeEvent: networkId=<OID>, networkName=<name>, deviceId=<OID>,
deviceName=<name>, previousRevisionId=<OID>, previousRevisionNumber=<long>,
currentRevisionId=<OID>, currentRevisionNumber=<long>, jobNumber=<long>,
jobSchedulerName=<user name>, timestamp=<long datetime>
DeviceRevChangeFailedEvent: networkId=<OID>, networkName=<name>, deviceId=<OID>,
deviceName=<name>, taskId=<OID>, taskNumber=<long>, jobSchedulerName=<user name>,
timestamp=<long datetime>
ExternalDeviceRevChangeEvent: networkId=<OID>, networkName=<name>, deviceId=<OID>,
deviceName=<name>, previousRevisionId=<OID>, previousRevisionNumber=<long>,
currentRevisionId=<OID>, currentRevisionNumber=<long>, timestamp=<long datetime>
```

```
ExternalDeviceRevChangeFailedEvent: networkId=<OID>, networkName=<name>, deviceId=<OID>,
deviceName=<name>, timestamp=<long datetime>
DeviceStatusChangeEvent: networkId=<OID>, networkName=<name>, deviceId=<OID>,
deviceName=<name>, previousStatus=<status>, currentStatus=<status>, timestamp=<long datetime>
SiteCreateEvent: networkId=<OID>, networkName=<name>, siteId=<OID>, siteName=<name>,
siteCreator=<user name>, timestamp=<long datetime>
SiteDeleteEvent: networkId=<OID>, networkName=<name>, siteId=<OID>, siteName=<name>,
siteDeleter=<user name>, timestamp=<long datetime>
SiteUpdateDevicesEvent: networkId=<OID>, networkName=<name>, siteId=<OID>, siteName=<name>,
addedDevices=[<deviceId=OID/deviceName=name, deviceId=OID/deviceName=name, ...>],
removedDevices=[<deviceId=OID/deviceName=name, deviceId=OID/deviceName=name, ...>],
siteUpdater=<user name>, timestamp=<long datetime>
SiteAddDevicesEvent: networkId=<OID>, networkName=<name>, siteId=<OID>, siteName=<name>,
addedDevices=[<deviceId=OID/deviceName=name, deviceId=OID/deviceName=name, ...>],
siteUpdater=<user name>, timestamp=<long datetime>
SiteDeleteDevicesEvent: networkId=<OID>, networkName=<name>, siteId=<OID>, siteName=<name>,
removedDevices=[<deviceId=OID/deviceName=name, deviceId=OID/deviceName=name, ...>],
siteUpdater=<user name>, timestamp=<long datetime>
DataFileCreateEvent: folderId=<OID>, folderName=<name>, dataFileName=<name>,
dataFileCreator=<user name>, timestamp=<long datetime>
DataFileModifyEvent: folderId=<OID>, folderName=<name>, dataFileName=<name>,
dataFileModifier=<user name>, timestamp=<long datetime>
DataFileDeleteEvent: folderId=<OID>, folderName=<name>, dataFileName=<name>,
dataFileDeleter=<user name>, timestamp=<long datetime>
JobScheduledEvent: jobId=<OID>, jobNumber=<long>, jobName=<name>, jobScheduler=<user name>,
comments=<string>, timestamp=<long datetime> JobApprovedEvent: jobId=<OID>, jobNumber=<long>,
jobName=<name>, jobScheduler=<user name>, jobApprover=<user name>, comments=<string>,
timestamp=<long datetime>
JobConflictEvent: jobId=<OID>, jobNumber=<long>, jobName=<name>, conflictingJobs=[<jobId=OID/
jobNumber=number, jobId=OID/jobNumber=number, ...>], timestamp=<long datetime>
JobUpdateEvent: jobId=<OID>, jobNumber=<long>, jobName=<name>, jobScheduler=<user name>,
jobApprover=<user name>, comments=<string>, timestamp=<long datetime>
JobRemovedEvent: jobId=<OID>, jobNumber=<long>, jobName=<name>, jobScheduler=<user name>,
jobDeleter=<user name>, timestamp=<long datetime>
JobCompletedEvent: jobId=<OID>, jobNumber=<long>, jobName=<name>, jobScheduler=<user name>,
jobUpdater=<user name>, comments=<string>, timestamp=<long datetime>
JobFailedEvent: jobId=<OID>, jobNumber=<long>, jobName=<name>, jobScheduler=<user name>,
jobUpdater=<user name>, comments=<string>, timestamp=<long datetime>
JobPartiallyFailedEvent: jobId=<OID>, jobNumber=<long>, jobName=<name>, jobScheduler=<user
name>, jobUpdater=<user name>, comments=<string>, timestamp=<long datetime>
JobStatusChangeEvent: jobId=<OID>, jobNumber=<long>, jobName=<name>, jobScheduler=<user
name>, jobUpdater=<user name>, comments=<string>, oldStatus=<status>, newStatus=<status>,
timestamp=<long datetime>
TaskCompletedEvent: jobId=<OID>, jobNumber=<long>, taskId=<OID>, taskNumber=<long>,
comment=<string>, timestamp=<long datetime>
TaskFailedEvent: jobId=<OID>, jobNumber=<long>, taskId=<OID>, taskNumber=<long>,
comment=<string>, timestamp=<long datetime>
ReportRemoveTemplateEvent: reportTemplateId=<OID>, reportTemplateName=<name>,
templateDeleter=<user name>, timestamp=<long datetime>
UserLoginEvent: userId=<OID>, userName=<user name>, loginTimestamp=<long datetime>,
timestamp=<long datetime>
UserLoginFailedEvent: userId=<OID>, userName=<user name>, loginTimestamp=<long datetime>,
timestamp=<long datetime>
AuthorizationSucceededEvent: resourceType=<string>, resourceId=<OID>, resourceName=<name>,
accessorName=<user name>, accessDate=<long datetime>, timestamp=<long datetime>
```

```
AuthorizationFailedEvent: resourceType=<string>, resourceId=<OID>, resourceName=<name>,
accessorName=<user name>, accessDate=<long datetime>, timestamp=<long datetime>
VersionCreateEvent: networkId=<OID>, networkName=<name>, versionId=<OID>, versionName=<name>,
versionCreator=<user name>, timestamp=<long datetime>
VersionChangeEvent: networkId=<OID>, networkName=<name>, versionId=<OID>, versionName=<name>,
versionUpdater=<user name>, timestamp=<long datetime>
VersionRemoveEvent: networkId=<OID>, networkName=<name>, versionId=<OID>, versionName=<name>,
versionDeleter=<user name>, timestamp=<long datetime>
```

File locking considerations

The flat file transport strategy uses the Java 1.5 File Channel feature to facilitate locking the events file when writing events. This strategy allows for external programs to adopt a file locking strategy when accessing this file.

Since the **java.nio.FileChannel** and **java.nio.FileLock** classes make use of native system concurrent file access capabilities, the external programs can make use of system-level, concurrent access methods, without concern as to whether these are compatible with the locking used by the FlatFile transport.

For those programs that are Java-centric, the **java.nio.FileChannel** and **java.nio.FileLock** classes are recommended when reading events from the event file.

The following code fragment illustrates a suggested approach.

```
. . .
FileOutputStream fos = new FileOutputStream("<eventfilename>");
DataOutputStream dos = new DataOutputStream(new BufferOutputStream(fos));
FileChannel channel = fos.getChannel();
FileLock lock = channel.lock();
try {
    . . . read and/or write data . . .
} catch (Exception e) {
    . . . handle exceptions . . .
} finally {
    lock.release();
}
. . .
```

File rolling considerations

- The FlatFile transport strategy is capable of performing file rolling, based on a file line count threshold. Once the event file exceeds the line count threshold, it is renamed, and a new empty file is created for subsequent events. The process of rolling continues for the life of the integration adapters.
- When file rolling is enabled, an optional file line count threshold can be specified. If file rolling is enabled and no threshold is specified, a default value of 100000 is used. This means that when an event file contains 100000 lines, the file is rolled.

- If a threshold is supplied, this value is used. It is advisable that very small threshold values not be used, as this causes a proliferation of small files on the Network Configuration Manager system, increase I/O activity, and overall degrades the performance of the system.
- When a file is rolled, the rolled file name is **<filename>.timestamp**, where **timestamp** is a long value that represents the number of milliseconds since 12:00a.m. January 1st, 1970. This timestamp value can be used to determine the age of the rolled files.
- To disable file rolling, either the **<enable-file-rolling>** element can be specified with a false value in the **<FlatFile>** transport strategy block of the integration adapters configuration file, or by removing the **<enable-file-rolling>** element.

Email Integration adapters

The Network Configuration Manager Email Integration adapters is a component that provides the ability to listen for events, transforming them into a formatted string, and delivering them via email.

Email integration adapters assembly

For each event that can be fired by the core Network Configuration Manager server, there is a corresponding transform definition inside an XML file that takes the native event, and transforms it into a set of well defined name-value pairs. These name-value pairs correspond to the subject line and the body of the email to be sent.

The subject line and the body of the email message for each event are defined inside the transform file **Mail_Transform.xml** located in the following directory:

$VOYENCE_HOME/ncmcore/webapps/ncm-webapp/WEB-INF/classes

This file is set up to map one event to a set of name-value pairs. The Generic Mail Transformer reads the transform definition for a particular event, and builds a Properties object. In the case of Mail integration adapters, the resulting Properties object would contain entries for “subject” and “body”.

The JavaMail transport takes the transformed event, and creates a JavaMail-compliant multi-part MIME message out of:

- The name-value pairs that represent the “transformed” event
- The to_address and from_address. The to_address and from_address values are specified via the E-Mail Integration adapters XML configuration file, but can be overridden on an individual basis by adding property nodes to the transform with keys as **to_address** and **from_address**.

  Once the MIME message is created, it is sent to the specified JavaMail session object.
  As with the to_address and from_address, this configuration parameter is specified in the XML configuration file. This JavaMail session object is found through the JNDI name of the JavaMail session object specified in the configuration file.

The JavaMail object referenced by this JNDI name is configured as part of Network Configuration Manager installation. The type of transport this JavaMail session uses depends on how it is configured during installation. Currently, supported outgoing mail transports are SMTP and IMAP.

Email Integration adapters configuration

The installation program of the Email Integration adapters prompts for the values as listed in the following table.

Element	Description	Required or optional	Default value
<Email Recipients>	Email address of the recipients. If more than one recipient is to be specified, they can be separated by using a comma.	required	N/A
<Return Email Address>	Email address from where the mail was sent	required	N/A
<Email Subject>	Default Subject	required	N/A

- After the initial installation, the configuration parameters can be edited using the JMX-Console.
- Refer to *“Updating configuration using the JMiniX Console” on page 199* for more details.

Tailoring the email integration adapters

The initial configuration of the email Integration adapters is setup to **listen** for the following events:

- DeviceNewConfigurationStateEvent
- DeviceConfigurationChangeEvent
- JobFailedEvent
- JobPartiallyFailedEvent
- TaskFailedEvent
- UserLoginFailedEvent

When these events are fired by the core Network Configuration Manager service, the Email Integration adapters receives the event, converts the event into a properly formatted string, and delivers the event via Email.

The most common form of tailoring functionally includes adding new events, removing existing events, recipient email address, sender email address, and email subject. The tailoring can be accomplished through the JMX-Console.

Generic SNMP Integration adapters

This section describes the features of the Network Configuration Manager Generic SNMP Integration adapters (hereafter referred to as SNMP Integration adapters). Specifically, Installing SNMP Integration adapters Server-side Components is detailed.

The SNMP Integration adapters server-side component provides the capability of listening for events, transforming the events into SNMP traps, and sending traps to a SNMP trap listener.

Note Refer to the Vendor-Specific document for Client-Side component installation.

Generic SNMP integration adapters assembly

For each event that can be fired by the core Network Configuration Manager server, there is a corresponding transform definition inside an XML file that takes the native event, and transforms it into an SNMP trap.

These traps conform to the MIB that is defined in the core Network Configuration Manager product.

This file is located in the following directory:

$VOYENCE_HOME/ncmcore/webapps/ncm-webapp/WEB-INF/classes/SNMP_Transform.xml

The SNMP transport takes the transformed event and sends it, via the SNMP protocol, to the configured vendor installation.

Generic SNMP integration adapters configuration

The installation program of the Generic SNMP Integration adapters prompts for the vendor product you are integrating with, along with the values listed in the following table.

Element	Description	Required or Optional	Default Value
<snmp-host>	Specifies the hostname or IP address of the SNMP host	required	N/A
<snmp-trap-port>	Specifies the port to send SNMP trap to	optional	162
<mib-file>	Specifies the name of the MIB definition file	required	N/A
<snmp-version>	Specifies the version of the SNMP protocol to use	optional	V1

Should the values of either of these fields change after installation and deployment, the configuration file must be updated using the **jmx-console**.

Refer to *“Updating configuration using the JMiniX Console” on page 199* for more information.

Tailoring the generic SNMP integration adapters

The initial configuration of the SNMP Integration adapters is setup to **listen** for the following events:

- AuthorizationFailedEvent

- DeviceNewConfigurationStateEvent
- DeviceConfigurationChangeEvent
- JobFailedEvent
- JobPartiallyFailedEvent
- TaskFailedEvent
- UserLoginFailedEvent

  When these events are fired by the core Network Configuration Manager service, the SNMP Integration adapters receives the event, converts the event into an SNMP trap, and sends the trap to the SNMP Trap listener.

  The trap listener has a rules file that understands the SNMP trap and formats it to their predefined format.

  The most common form of tailoring functionally includes adding new events, removing existing events, MIB file name, SNMP hostname, SNMP trap port, and SNMP version. The tailoring can be accomplished through the JMX console.

  Note You must restart the integration module for the changes to take effect.

Launching the application through a URL

The system has the ability to launch the application in context via a URL. You are directed to the information for specific jobs or devices, based on the parameters of the URL. This is especially useful in integrations.

One example is where an external system receives an event or SNMP trap about a network device. Users in the external system can click a URL that launches into the Network Configuration Manager system directly to the device for detailed information.

Another example is where job warnings or failures are issued. A URL can launch you directly to the offending job for a detailed description of the problem.

The URL is constructed as follows:

https://<server-ip>:8880/contextual-launch/launch?<param_name=value>

Or,

https://<server-ip>:8880/contextual-launch/launch?<param_name=value>

where <server-ip> is the IP Address of the machine where the server is installed.

Check *Section "List of allowed query strings" on page 219* for a list of allowed param_names. For example, a URL to launch to job number **10005** would be as follows:

https://<server-ip>:8880/contextual-launch/launch?jobId=10005

Many parameters are available as query strings. In the case where multiple entities could be returned from the query, you can select the entity in which they are interested.

The URL query can also further restrict the scope of the launch by including a network parameter. It must be used in conjunction with one of the above parameters. For example, to launch to any device that contains an IP address of 192.168.1.1 in a network called MyNetwork, the URL would be as follows:

https://<server-ip>:8880/contextual-launch/launch?networkId=

MyNetwork&anyDeviceIP=192.168.1.1

The contextual launch capability was specifically designed to give the integration developer a great deal of flexibility. It is intended to allow tighter integrations between disparate systems with less effort.

List of allowed query strings

Parameter	Launches to...
jobId	Specific job number
deviceHostname	Device with host name
deviceFQDN	Device with FQDN
deviceIP	Device with management IP as specific
deviceAlias	Device with indicated alias
deviceName or derivedName	Device whose name has been derived by the method specified by the system administrator
anyDeviceName	Any device where the FQDN, alias, derived name or hostname match the parameter
anyDeviceIP	A device where any of the device’s interfaces match the given IP Address
anyDeviceNameOrIP	A combination of the previous two – the system checks any name or IP Address on the device
Value	The system will determine whether the value is a job number, device name, or IP Address, and launch to the appropriate entity

Upgrade procedures (Linux platform)

10

Read the following topics next:

- Overview
- Upgrading using the graphical installer mode
- Upgrading using the console installer mode
- Updating the privLevels.xml
- Post upgrade procedures

Overview

The Network Configuration Manager can be upgraded using the graphical installer mode or the console installer mode.

The following table lists the products that are supported for upgrade to version 10.1.6:

Task	Upgrade to
Upgrade from Network Configuration Manager 9.6 or 9.6.1	Network Configuration Manager 10.1.6
Upgrade from Network Configuration Manager 10.1.0, 10.1.1, 10.1.3 or 10.1.4.	Network Configuration Manager 10.1.6

Note A downgrade path is not supported. After upgrading to Network Configuration Manager 10.1.6, you cannot revert to the previously installed version.

Upgrading using the graphical installer mode

This section describes how to use the graphical installer mode to upgrade the Network Configuration Manager.

When upgrading the Network Configuration Manager, the servers must be upgraded in the following order:

- Stand-alone Database Server (if applicable)
- Combination Server or Application Server

- Device Server (if applicable)

  The upgrade must be repeated for each server. If you are upgrading a distributed server configuration, with separate Application Server and Device server, you must first upgrade the Network Configuration Manager on the Application Server, and then upgrade it on the Device Servers.

  Note At setup, the Device server registers itself with the Application server. Before upgrading the Device server, ensure the Application or Combination servers have the same date and time as the candidate Device server. If not, the Device server cannot communicate with the Application server, this step fails, and you must reinstall the Device server.

Upgrading an existing version using the graphical installer mode

Note This procedure must be completed for each Network Configuration Manager server.

To upgrade an existing version of Network Configuration Manager using the graphical installer mode, follow these steps:

Step	Action
1	Log into the server as a user with administrator privileges.
2	Type **bash install.sh –i gui** to run the installer in the graphical installer mode, and press **Enter**.
3	The installer will install the prerequisites if the software prerequisites need to be installed.
4	The installer will attempt to stop the product processes if the server is an Application or Combination server. The database process NCM_Controldb will be started. A prompt to backup the product data (DB) will be seen before the upgrade process, if the server is an Application or Combination server. ■ Select Y (Yes) or N (No) for the product data (database) backup. ■ Select Y (Yes) if there has not been a data backup done before the upgrade. Type the appropriate passwords. The backup file will be in the [Product directory]\data-image directory. Save the backup file if data needs to be restored later.
5	An Important Notice Window appears in a command prompt window. Click, **Enter** in the Important Notice window. The installer begins to load.
6	The Introduction window appears. Click **Next** in the Introduction window.
7	The License Agreement window appears. Read the license agreement, select **I accept the terms of the License Agreement**, and click **Next**. **Note** The installer checks if the correct versions of Tomcat and Perl have been installed.
8	The Watch4net configuration requirement check window appears. ■ Select **Yes** to configure the Network Configuration Manager Reporting SolutionPack and click **Next**. ■ Select **No** to continue without configuring Network Configuration Manager Reporting SolutionPack. *“Configuring EMC M&R server”* provides instructions on configuring Watch4net server post Network Configuration Manager installation.

Step	Action
9	The Watch4net Server IP address window appears. Type the Watch4net Server IP address and click **Next**. **Note** Do not enter the server name or FQDN.
10	The Lockbox passphrase window appears. Type the passphrase and click **Next**.
11	The Security Questions windows appears. Type the answers for the security questions and click **Next**.
12	The Encryption Key store option window appears. Choose a location where NCM should store the encryption key that is used to encrypt and decrypt data. The options are: ■ 1 for Standard Security – Key stored encrypted in a flat file ■ 2 for Advanced Security – Key stored in RSA Lockbox **Note** If you return to this window later during the installation process, the option you selected will be displayed in encrypted format (not in clear text).
13	Another backup warning appears to ensure that a data backup is created before the upgrade begins. Select, **Continue the Upgrade** if the data backup is created.
14	The Summary window opens and displays the product information before installation, and the required disk space. **Note** If there is insufficient disk space, the installer displays an error message until the disk space is free. Click **Install** to start the installation. This portion of the installation may take several minutes. **Note** If the database resides on the server during upgrade, the upgrade process may take much longer to complete. There is an internal database backup and restore when you upgrade to a new version of PostgreSQL. For large databases, the upgrade process could take an hour or more.

Next step, go to Post upgrade procedures.

Upgrading using the console installer mode

This section describes how to use the **console-based installer** to upgrade the Network Configuration Manager. When upgrading the Network Configuration Manager, the servers must be upgraded in the following order.

- Stand-alone Database Server (if applicable)
- Combination Server or Application Server
- Device Server (if applicable)

  The upgrade must berepeated for each server. If you are upgrading a distributed server configuration, with separate Application server and Device server, you must first upgrade the Network Configuration Manager on the Application server, and then upgrade the Network Configuration Manager on the Device servers.

  Note At setup, the Device server registers itself with the Application server. Before upgrading the Device server, ensure the Application or Combination servers have the same date and time as the candidate Device server. If not, the Device server cannot communicate with the Application server, this step fails, and you must reinstall the Device server.

Upgrading an existing version using the console based installer mode

Note This procedure must be completed for each Network Configuration Manager server.

To upgrade an existing version of Network Configuration Manager using the console-based installer, follow these steps:

Step	Action
1	Log into the server as the root user.
2	Type **bash install.sh –i console** to run the installer in the graphical installer mode, and press **Enter**.
3	An Important Notice appears. Press **Enter** at the Important Notice window. The installer begins to load.
4	The **install.sh** script checks for the Network Configuration Manager Prerequisites and automatically installs any that are missing. VMware Smart Assurance Network Configuration Manager Support Matrix document provides more information.
5	A message appears indicating the system is extracting resources from archives. When complete, the introduction to the installer appears. Press **Enter** to continue.
6	The License Agreement appears. Read the license agreement. Press **Enter**, and continue to press **Enter** to move through each page of the license agreement until you reach the final page.
7	On the final page of the license agreement, type **Y**, and press **Enter** to accept the terms of the license agreement.
8	The installer prompts you for Watch4net configuration requirement check. ■ Select **Yes** to configure the Network Configuration Manager Reporting SolutionPack and press **Enter**. ■ Select **No** to continue without configuring Network Configuration Manager Reporting SolutionPack. *"Configuring EMC M&R server"* provides instructions on configuring Watch4net server post Network Configuration Manager installation.
9	The installer prompts you for the Watch4net server IP address. Type the Watch4net server IP address and press **Enter**.
10	The installer prompts for the lockbox passphrase. Type the passphrase and press **Enter**.
11	The installer prompts for answers to the security questions. Type the answers for the security questions and press **Enter**.
12	The installer prompts you to select an Encryption Key store option. Type a location where NCM should store the encryption key that is used to encrypt and decrypt data. The options are: ■ 1 for Standard Security – Key stored encrypted in a flat file ■ 2 for Advanced Security – Key stored in RSA Lockbox **Note** If you return to this window later during the installation process, the option you selected will be displayed in encrypted format (not in clear text).
13	Another backup warning appears to ensure that a data backup is created before the upgrade begins. Select, **Continue the Upgrade** if the data backup is created.

Step	Action
14	The Pre-Install Summary Screen displays all of your selections to this point in the installation process. ■ Review the information for the Pre-Install Summary Screen, including the required disk space. ■ Press **Enter** to start the installation. It may take several minutes for the next prompt to appear. **Note** If there is not enough available disk space, the installer displays an error message until sufficient disk space is free. You can continue once enough disk space is available.
15	The installer displays the installation complete message. Press **Enter**. **Note** If the database resides on the server during upgrade, the upgrade process may take much longer to complete. There is an internal database backup and restore when you upgrade to a new version of PostgreSQL. For large databases, the upgrade process could take an hour or more to complete.

Note In certain distributed upgrade scenarios, the Tomcat logs might contain ClassFormatException exception errors. There is no functionality impact due to this exception.

Next step, go to *"Post upgrade procedures"*.

Updating the privLevels.xml

Once Network Configuration Manager has been fully upgraded to version 10.1.6, the privLevels.xml file can be updated to maintain your Network Configuration Manager settings. This file allows you to customize the default multi-level enable mode configuration of network devices that are managed by NCM. These steps are optional.

Note The Network Configuration Manager privLevels.xml file is located in the **[Product Home]/package/pkgxml/privLevels.xml** directory after upgrading to Network Configuration Manager 10.1.6.

To update the privLevels.xml file, follow these steps:

Step	Action
1	Log into the server as a user with administrative privileges.
2	Create a directory for the customized privLevels.xml file. Type **mkdir -p [Product Home]/custompackage/pkgxml**, and then press **Enter**.
3	Copy the privLevels.xml to the new directory. Type **cp [Product Home]/package/pkgxml/privLevels.xml [Product Home]/custompackage/pkgxml/privLevels.xml**, and then press **Enter**.
4	Run the following command: **chown -R ncm:voyence [Product Home]/custompackage/pkgxml**
5	Use a text editor to edit the new Network Configuration Manager 10.1.6 version of the privLevels.xml file with the changes from the older Network Configuration Manager version of privLevels.xml.

Post upgrade procedures

After performing an upgrade installation, follow the steps in this section:

- Add distributed system hosts for remote servers (standard or advanced security)
- Establish a secure connection with Report server

Add distributed system hosts for remote servers (standard or advanced security)

Use the following steps to add distributed system hosts:

1. If you choose Standard Security mode during AS installation, copy **lockb.ekey** from [product directory]/data in the AS to [product directory]/data on the remote server (DS or Database).
2. If you chose Advanced Security mode during AS installation:
3. On the Application server, go to [Product directory]/bin directory.
4. Source the voyence.conf file

   ```
   source /etc/voyence.conf
   ```

5. Add distributed system hosts to the lockbox using the **cstdriver** utility:

   ```
   ./cstdriver -lockbox  [Product directory]/data/lockb.clb
   -passphrase <passphrase> -addHost <FQDN of Database server>
   ./cstdriver -lockbox [Product directory]/data/lockb.clb
   -passphrase <passphrase> -addHost <FQDN>
   ./cstdriver -lockbox [Product directory]/data/lockb.clb
   -passphrase <passphrase> -addHost <FQDN of Device server>
   ```

6. Go to [Product directory]/data directory.
7. Copy the lockbox file to any directory on each of the distributed system hosts.
8. For example:

   ```
   scp lockb.clb Host2_DB_Server:/root/
   scp lockb.clb Host3_Device_Server:/root/
   ```

9. Change the lockb.clb file permission to ncm:voyence using the command:

   ```
   chown ncm:voyence [Product directory]/data/lockb.clb
   ```

10. Restart all Network Configuration Manager services.

Reset the JMX password

An upgrade to NCM version 10.1.6 cannot retain the JMX password that was set in the previous version of the software. After the upgrade, you must manually reset the JMX password.

Reapply customizations to the system-config.xml file

An upgrade to NCM version 10.1.6 does not retain any customizations that were made to values in the system-config.xml file in previous versions of the software. After the upgrade, you must manually reapply any changes that were made in the file.

Retain RSA users after the NCM upgrade

After the NCM upgrade, RSA users are not retained that were added before the upgrade due to the change in JAVA_HOME. To retain RSA users, import the RSA certification again.

To import the RSA certificate, do the following:

1 Run the following commands in the Application server:

```
$VOYENCE_HOME/java/bin/keytool -keystore       $VOYENCE_HOME/java/jre/lib/security/cacerts
-import -file /RSA.cer -alias       VCRSA
/opt/smarts-ncm/java/bin/keytool -keystore       $VOYENCE_HOME/java/jre/lib/security/
cacerts -import -file c:/RSA.cer -alias       VCRSA
```

2 When prompted for a password, enter **changeit**.

3 Restart vcmaster service.

Backup and recovery

11

Read the following topics next:

- Overview
- Network Configuration Manager distributed architecture
- Data locations
- Backup utilities
- Customer responsibilities
- Hot spare scenario
- Backing up clustered and distributed database environments

Overview

The first and most important part of any good disaster recovery plan is to ensure your critical application data is completely backed up on a regular basis, and the data is ready for restoration in the event of data loss, data corruption, or disaster recovery.

Your installation of Network Configuration Manager comes with a set of backup and restoration utilities pre-configured to backup the critical data in your environment. These utilities are set up during installation on your Application server to create nightly backups consisting of all information within the Network Configuration Manager application needed to fully recover your environment.

Information contained here introduces you to these utilities, their use in the Network Configuration Manager distributed architecture environment, and their integration into your overall corporate disaster recovery plan.

Note It is not within the scope of this document to discuss the backup or disaster recovery for the operating systems or any application software within the Network Configuration Manager server environments. Your corporate disaster recovery processes are unique to your environment, and are based on your overall IT process needs. The Network Configuration Manager back up and restore utilities are constructed to compliment your existing sever OS and application software restoration processes, and not attempt to replace them.

Network Configuration Manager distributed architecture

Your implementation of Network Configuration Manager is designed to scale to the needs of your network environment, supporting a separate Application server and one or more Device servers. Depending on the size of your network, your Application server and Device server may exist on a single hardware platform, or be dispersed geographically across multiple hardware platforms.

Regardless of your environment, the data management capabilities of Network Configuration Manager will ensure that the backup and restore utilities collect all the data required to fully recreate your network environment in the case of data loss.

While both your Application server and Device servers store data about your network environment, only the Application server needs to be part of your data backup strategy, saving untold hours and resources required to backup Device servers that may be distributed across your network and the globe.

This is accomplished by storing configuration data about your Device servers within the Application server itself. In the unforeseen instance when a Device server is lost or corrupted, a clean Device server can download the identity of the lost Device server from your Application server, and take over all device management for the lost Device server.

Information about your Device servers is stored in the Network Configuration Manager Application server Database, and is captured along with all other application data using your pre-installed Network Configuration Manager backup and restore utilities.

Data locations

The Network Configuration Manager back up and restoration utilities gather all your critical application data to be stored in a preset backup location. This frees you from worrying about which data files within the Application server are important to back up, and which data files can be ignored.

Your network configuration data is stored essentially in three forms:

- Relational database tables
- XML data
- Flat file data

  All files needed for a successful backup of your Application server data are stored under [Product directory], and include:

  ```
  [Product directory]/data
  [Product directory]/db
  ```

When a backup of your system takes place, the files in these directories are copied into a backup bundle, compressed, given a time-stamped name, and stored in a separate directory within your application environment, [Product directory]/data-image. By default, the data-image directory is on a filesystem local to the Application server.

When integrating the Network Configuration Manager backup process into your existing corporate backup, it is imperative that this backup data be stored off of the Application server (on a daily basis) to prevent an Application server hardware failure from corrupting both the application data and the backups.

There are several options to transfer your backup files onto a system other than the Network Configuration Manager Application server. The best option for your environment depends on your corporate IT backup, and your disaster recovery policy, but can include installing a third-party storage backup utility on the Network Configuration Manager Application server. Follow these steps:

a Use the UNIX®® cron utility to rcp, scp, or ftp the backup file to a different server other than the Network Configuration Manager Application server.

b Create an NFS mount point for the [Product directory]/data-image directory that resides on a remote server.

c Copy the backup file to a removable storage device installed on the Network Configuration Manager Application server, such as tape or CD.

Backup utilities

The backup and restore utilities have been updated to require a valid database password.

Note The nightly database backup cronjob using the [Product Directory]/tools/backup.pl script is disabled, as it would fail with the new database password that was added. The backup has to be done manually or a script needs to be created that will create the database backup using the database password provided during the installation. The rotation of these database backup files needs to be taken under consideration, since the file system space will be used up if the backups performed on daily or regular basis.

The installation process for the Network Configuration Manager Application server automatically installs the utilities required to perform a nightly backup of your network data, placing them in the [Product directory]/tools directory. These tools are:

- [Product directory]/tools/backup.pl — Creates a compressed backup bundle of all critical data files on an active server, storing the resulting backup file in [Product directory]/data-image
- [Product directory]/tools/restore.pl — Given a name of a backup bundle in [Product directory]/ data-image, restores the network image on the Network Configuration Manager Application server

- [Product directory]/ tools/rotate-backups.pl — Given an integer, such as 7, maintains a list of the seven most recent backup files in the [Product directory]/data-image directory, based on file timestamps

  These utilities provide full backup and full restoration. Since the Network Configuration Manager application is not transactional in nature, there is no provision for incremental backups or transaction rollback. This greatly simplifies the restoration process and management of backups in your environment.

  The [Product directory]/tools/restore.pl utility is run manually in the event that a full data restore of the Network Configuration Manager Application server is required. To run the command, you must log in to the Network Configuration Manager server as user 'root' and execute the following command:

  # [Product directory]/tools/restore.pl

  [Product directory]/data-image/<filename>

  <filename> indicates the name of the backup file to be restored from the [Product directory] / data-image directory.

  Logs are created for database related scripts to show the progress or display errors encountered. When you run any of these scripts, logs are generated in the same folder. The logs generated are archive.log, backup.log, and restore.log. These logs will help you to analyze the progress of these scripts or analyze any errors occurring while they were run.

Steps to backup and restore database in NCM

The following are the steps to backup and restore database in NCM.

Steps to backup and restore database in NCM Combination setup

1. Login to NCM server from which you want to take the backup of database, and then set the VOYENCE_HOME environment variable.

   For example, in Linux, execute the following command:

   ```
   source /etc/voyence.conf
   ```

2. Take the backup of database by using the backup.pl script under the <VOYENCE_HOME>/ tools directory.

The script creates a “backup-image-.*.tgz” file under the VOYENCE_HOME>/data-image directory.

Note

- If you have Smarts Adapter configured with SMARTS IP and SAM, the backup.pl script will also backup the Smarts Adapter data.
- If you are taking backup from lower version of NCM (10.1.3 and below) then before taking the backup run the database-changes.pl script present under Utils directory of 10.1.6 installer.

3 Copy the “backup-image-.*.tgz” file to a host where a new NCM Combination setup is installed. The backup file can be copied under any directory.

4 Login to the new NCM server setup, and then execute the following command:

```
source /etc/voyence.conf
```

5 Execute the following command from the <VOYENCE_HOME>/tools directory if you are restoring database across the same NCM version:

```
perl restore.pl <Absolute path to backup image file /backup-image-.*.tgz>
```

6 Execute the following command from the <VOYENCE_HOME>/tools directory if you are restoring database on higher NCM version:

```
perl restore.pl <Absolute path to backup image file /backup-image-.*.tgz>
--force
```

Note This step is required for the backups taken from NCM 9.6 version onwards.

7 Update the InfraDB entry with the Device server host name. To update the InfraDB entry, perform the following steps:

a From the <VOYENCE_HOME>, execute the following command:

```
\cgi-bin\cflist.cgi > cflist.txt
```

b Edit the cflist.txt to change the Device server FQDN to the new Device server FQDN (Same as Combination server FQDN).

For example, POP 1000 “<hostname>”

c Execute the following command. It must return 'Status: 200 Success'.

```
\cgi-bin\cfwrite.cgi < cflist.txt
```

8 To update the Device server FQDN in cm_device_server table in the database, do the following:

a Login to NCM UI, and then navigate to **Tools > System Administration > Global > Access > Device Servers**.

b Select the Device server, and then click **Edit**.

c In the **Edit Device Server** window, click **OK**.

Or,

Run the following command from [Product directory]\db\controldb\bin:

```
psql.exe -h -d voyencedb -U pgdba -p 5435 -c "update cm_device_server set
device_server_name='Device_Server_name';"
```

9 Change the ownership of <VOYENCE_HOME>/data directory to ncm:voyence using the command:

```
chown -R ncm:voyence <VOYENCE_HOME>/data
```

10 Change the ownership of <VOYENCE_HOME>/conf/key and <VOYENCE_HOME>/conf/iv files to ncm:voyence using the command:

```
chown ncm:voyence <VOYENCE_HOME>/conf/key
chown ncm:voyence <VOYENCE_HOME>/conf/iv
```

11 Restart the vcmaster service.

12 If you have Smarts Adapter configured in your previous NCM setup, follow these steps:

On Linux

a Stop the NCM Smarts Adapter service.

```
service ncmsmartsadapter stop
```

b Change the directory to $VOYENCE_HOME/NCMSmartsAdapter/.

c Open and edit the prodDb.script file, so that VOYENCE_CONFIGURATION table and SMARTS_CONFIGURATION table is populated with actual AS host name, as follows:

d Search for

INSERT INTO VOYENCE_CONFIGURATION VALUES (1,4,TRUE,'auth.conf','2','10000','linbgh125.lss.vmware.com','jUpFF0M5HQuOdJUqIYKo0w==','sysadmin')

e Replace the old Application server host name with new Application server host name.

For example, replace 'linbgh125.lss.vmware.com' with '<new Application server host name>'.

f Search for

INSERT INTO SMARTS_CONFIGURATION VALUES (1,5,'aced0005757200135b4c6a6176612e6c616e672e537472696e673badd256e7e91d7b4702000078700000000274000e494e4348415247452d414d2d504d74000353414d','10.31.202.131',426,NULL,'z/RS9si+EWVsdA8kxzEovg==','SAM','linbgh131.lss.vmware.com','10.31.202.131','z/RS9si+EWVsdA8kxzEovg==','46499','admin',TRUE,'admin','linbgh125.lss.vmware.com')

g Replace the old Application server host name with new Application server host name.

For example, replace 'linbgh125.lss.vmware.com' with '<new Application server host name>'.

h Open and edit the prodDb.script file, so that TOPOLOGY_SYNC table is populated with actual DS host name, as follows:

i Search for

INSERT INTO TOPOLOGY_SYNC VALUES (1,43,120,300,TRUE,TRUE,200,'INCHARGE-AM-PM','DisplayName','Active Sync On',NULL,TRUE,FALSE,TRUE,TRUE,TRUE,TRUE,FALSE,'linbgh127.lss.vmware.com','1000',' Derived','IP Devices','Run Upon Approval')

j Replace the old device server host name with the new device server host name.

For example, replace 'linbgh127.lss.vmware.com' with '<new Device server host name>'.

Steps to backup and restore database in NCM distributed setup

1 Login to NCM Application server from which you want to backup database, and then set the VOYENCE_HOME environment variable.

For example, in Linux, execute the following command:

source /etc/voyence.conf

2 Stop the tomcat service running on the remote RA server.

3 Take the backup of database by using the backup.pl script under the <VOYENCE_HOME>/tools directory.

The script creates a “backup-image-.*.tgz” file under the VOYENCE_HOME>/data-image directory.

Note

- If you have Smarts Adapter configured with SMARTS IP and SAM, the backup.pl script will also backup the Smarts Adapter data.
- If you are taking backup from lower version of NCM (10.1.3 and below) then before taking the backup run the database-changes.pl script present under Utils directory of 10.1.6 installer.

4 Copy the “backup-image-.*.tgz” file to a host where a new NCM Application server is installed. The backup file can be copied under any directory.

5 Login to the new NCM Application server setup, and then execute the following command:

source /etc/voyence.conf

6 Execute the following command from the <VOYENCE_HOME>/tools directory if you are restoring database across same NCM version:

perl restore.pl <Absolute path to backup image file /backup-image-.*.tgz>

7 Execute the following command from the <VOYENCE_HOME>/tools directory if you are restoring database on higher NCM version:

   perl restore.pl <Absolute path to backup image file /backup-image-.*.tgz> --force

   Note This step is required for the backups taken from NCM 9.6 version onwards.

8 Update the InfraDB entry with Device server host names and IP addresses. To update the InfraDB entry, perform the following steps:

   a From the <VOYENCE_HOME>, execute the following command:

      \cgi-bin\cflist.cgi > cflist.txt

   b Edit the cflist.txt to change all Device server FQDN and IP address to the new Device server FQDN and IP address.

      For example, POP 1000 "<HOSTNAME>" NetList= RsrcList= DevList=1001,1002 EmsList= : ADDR="<IPADDRESS"

   c Execute the following command. It must return 'Status: 200 Success'.

      \cgi-bin\cfwrite.cgi < cflist.txt

9 On the new Application server, go to the <VOYENCE_HOME>/bin directory, and then add all distributed Device servers to the lockbox using cstdriver utility:

   a cstdriver -lockbox <VOYENCE_HOME>/data/lockb.clb -passphrase <passphrase> -addHost <FQDN of Device server>

   b cstdriver -lockbox <VOYENCE_HOME>/data/lockb.clb -passphrase <passphrase> -addHost <FQDN>

10 Change the ownership of <VOYENCE_HOME>/data directory to ncm:voyence using the command:

```
chown -R ncm:voyence <VOYENCE_HOME>/data
```

11 Change the ownership of <VOYENCE_HOME>/conf/key and <VOYENCE_HOME>/conf/iv files to ncm:voyence using the command:

```
chown -R ncm:voyence <VOYENCE_HOME>/conf/key
chown -R ncm:voyence <VOYENCE_HOME>/conf/iv
```

12 Restart the vcmaster service in the Application server host.

13 Copy and replace the <VOYENCE_HOME>/data/lockb.clb file from Application server host to all Device server host under <VOYENCE_HOME>/data/lockb.clb.

14 Change the ownership of the lockb.clb file to ncm:voyence using the command:

```
chown ncm:voyence lockb.clb
```

15 Change the file permissions of the lockb.clb file to 640 using the command:

```
chmod 640 lockb.clb
```

16 Copy and replace the following from the old Device server to new Device server:

- <VOYENCE_HOME>/data/devserver/configuration/ad_nextIdx
  - <VOYENCE_HOME>/data/devserver/configuration/ad_numIdxIHavefiles

17 Change the ownership of both the files to ncm:voyence using the commands:

```
chown ncm:voyence ad_nextIdx
chown ncm:voyence ad_numIdxIHavefiles
```

18 Change the file permissions of both the files to 660 using the commands:

```
chmod 660 ad_nextIdx
chmod 660 ad_numIdxIHavefiles
```

19 Restart the vcmaster service in all distributed Device server hosts.

20 To update all Device server FQDN in cm_device_server table in the database, do the following:

a Login to NCM UI, and then navigate to **Tools > System Administration > Global > Access > Device Servers**.

b Select each Device server, and then click **Edit**.

c In the **Edit Device Server** window, click **OK**.

Or,

Run the following command from [Product directory]\db\controldb\bin:

```
psql.exe -h -d voyencedb -U pgdba -p 5435 -c "update cm_device_server set
device_server_name='Device_Server_name';"
```

21 If you have Smarts Adapter configured in your previous NCM setup, follow these steps:

On Linux

a Stop the NCM Smarts Adapter service.

service ncmsmartsadapter stop

b Change the directory to $VOYENCE_HOME/NCMSmartsAdapter/.

c Open and edit the prodDb.script file, so that VOYENCE_CONFIGURATION table is populated with actual AS host name, as follows:

d Search for

INSERT INTO VOYENCE_CONFIGURATION VALUES (1,4,TRUE,'auth.conf','2','10000','linbgh125.lss.vmware.com','jUpFF0M5HQuOdJUqIYKo0w==','sysadmin') e Replace the old Application server host name with new Application server host name.

For example, replace 'linbgh125.lss.vmware.com' with '<new Application server host name>'.

f Start the NCM Smarts Adapter service.

service ncmsmartsadapter start

Customer responsibilities

While the Network Configuration Manager installation will automatically create a nightly rotation and backup of your network data, this is merely the first step of your complete data backup and disaster recovery plan.

As discussed earlier in the *"Data locations" on page 223* the next step in the backup process is to ensure the safekeeping of your backup data by sending the data to a remote corporate storage device or a server as dictated by your IT backup policy.

Finally, your data backup, application software restoration, and server OS imaging requirements all need to be documented in a corporate disaster recovery plan to guarantee business continuity in the event of a major outage or failure. These tasks, while important, are beyond the scope of this document.

Hot spare scenario

Many customers have expressed an interest in maintaining a **hot spare Application server** in case of a catastrophic hardware failure in their Network Configuration Manager production Application server. Because of the distributed architecture of Network Configuration Manager software, and hot backup capabilities of the backup utilities, a hot spare server can be maintained in a ready standby state, able to take over the production application role in a matter of minutes.

To set up a hot spare scenario, two identical Application servers are required to be installed withunique IP addresses on the same subnet. Both servers should have identical versions of the Network Configuration Manager Application (or combination) Server software installed. However, only the primary, or production server, is configured to communicate with any distributed Device servers.

Once the primary and hot spare Application servers are configured and running, the root crontab can be edited on the primary server to copy the nightly backup bundle to the [Product directory] /data-image directory on the hot spare server using rcp or scp commands. (Note that there are a variety of ways you can copy the backup file from one server to the other, originating the command from either the primary or the hot spare server. This is only one example).

Once the backup bundle is on the hot spare server, it can be restored using the [Product directory] /tools/restore command (see the *"Backup utilities" on page 224*) making the network environment on the hot spare identical to the production server. This process can be repeated nightly through the use of cron, so that the two servers stay in sync.

The refresh rate of the sync process is up to your requirements. You may choose to sync the network data every four hours, or more frequently. There is a performance penalty on the production server during a backup, and large environments should take care when determining the frequency of backups.

Once the sync process is in place, if the primary server ever goes down, it is a simple process of executing a ‘takeover’ script on the hot spare sever that will change its IP address to that of the primary, and restart network services. Once the hot spare server has successfully obtained the IP address of the primary, it will communicate with all Device servers and user clients.

Backing up clustered and distributed database environments

For customers that have very high availability (HA) requirements, the Network Configuration Manager software supports operations in clustered and distributed database environments. In general, the backup and recovery utilities in such environments will work as described in this document.

However, due to the custom requirements of HA clustered and distributed environments, it is recommended that you contact Customer Support before implementing a backup and disaster recovery plan for your Network Configuration Manager HA environment.

Getting Started with Network Configuration Manager

12

Read the following topics next:

- Accessing additional Network Configuration Manager publications
- After installation—getting started using Network Configuration Manager
- Lightweight Directory Access Protocol (LDAP)

Accessing additional Network Configuration Manager publications

The related publications for this product are available online in Portable Document Format (PDF). To locate product publications in the Network Configuration Manager Reference Library:

Step	Action
1	Click the **Help** option on the Network Configuration Manager menu bar.
2	Select **Help Contents**. The Online User's Guide will open. Help Contents can be downloaded as pdf document.

After installation—getting started using Network Configuration Manager

After installing Network Configuration Manager, the first task you need to accomplish is to create a Network. After creating a Network, the following tasks are recommended, in the order shown:

- Assign Device servers
- Add Credentials
- Schedule an Auto Discovery
- Create Users and Groups
- Manage Users and Groups Permissions
- Set Network Permissions

- Manage Network Devices

> **Note** The ability to create networks and work with users and groups is reserved for System Administrators, or those with System Administrator privileges.

Step	Task
1	■ Once the Network Configuration Manager application launches and you successfully log in, go to the Online User's Guide(**Help -> Help Contents**). ■ Use the **Search** feature to locate and view the **Creating a New Network** help, and complete those steps.
2	Next, associate Device servers to the Network. Use the **Search** feature to enter **Network – Device servers**, and complete the steps for **Assigning Device servers**.
3	■ Continue to use **Search** to locate the **Auto Discovery Overview** help, and then click the **Creating Auto Discovery Jobs** link within that Help. ■ Once linked, complete the steps to **Add Credentials**, and then **Schedule** and complete the **Auto Discovery**.
4	Continue using **Search** to locate the procedures for **Creating Users**, and then **Creating Groups**. Complete those procedures.
5	Using **Search**, review **Setting User and Group Permissions** help, then complete the steps needed to **Manage the permissions for Users and Groups**.
6	Assign Users and Groups to Networks, by locating and then completing the steps in **Setting Network Permissions**.
7	Use Search to locate and access the **Manage Network Devices** help. **Note** To review other tasks and functions you can complete, search for **SYSTEM ADMINISTRATORS – Getting Started**, or **NETWORK ADMINISTRATORS – Getting Started**.

Tips:

- To locate specific information within the *Online User's Guide*, click the **Search** tab, and type a search word or phrase in the entry box, then click **Go**.
- To search through the complete listing of topics in the *Online User's Guide*, click the **Index** tab.
- Depending on your job title and responsibilities, select the **End Users**, **System Administrator**, or **Network Administrator** section to get started using Network Configuration Manager. Within each of these sections information and step-by-step procedures for job-specific tasks are detailed.

Lightweight Directory Access Protocol (LDAP)

This section describes how to set up LDAP server on Network Configuration Manager.

1 Configure Network Configuration Manager to point to LDAP or Active Directory server

2 Log into Network Configuration Manager as system administrator.

3 Go to **System Administration** > **Global** > **User Management** > **Authentication Servers** > **LDAP**

4 Enter your settings. Click **Apply**.

5 In the left pane, go to **User Management > System Users** and add your LDAP/Active Directory users. Ensure that the **User ID** and **Email** fields match with what you have in the LDAP/AD server.

6 Under **Authentication Method**, select **External LDAP**.

7 Verify LDAP/Active Directory settings (optional)

8 Logout of Network Configuration Manager.

9 Login with an LDAP/Active Directory user credentials.

Note If you experience problems logging in, check the LDAP/Active Directory logs.

10 Flip the secure switch on your LDAP/Active Directory server. Configure your LDAP/Active Directory server to use SSL. Make a note of the secure port number used by LDAP/Active Directory server.

11 Retrieve the SSL certificate from LDAP/Active Directory server.

12 Download InstallCert.java from internet to your desktop. If InstallCert.java is not available, skip to Step 16.

13 Run the command,

```
C:\Users\Administrator\Desktop>"%JAVA_HOME%\bin\javac" InstallCert.java
C:\Users\Administrator\Desktop>"%JAVA_HOME%\bin\java" InstallCert LDAP-SERVERIP:<secure
port>
```

14 You will be prompted to enter certificate to add to trusted keystore. Press **Enter**.

15 From your desktop, copy the file **jssecacerts** to NCM Application Server or Combination Server at $JAVA_HOME/lib/security.

Note Execute step 16 and 17, if steps 12 – 15 are not executed.

16 On NCM Application Server or Combination Server, generate PEM file from LDAP server with below command:

```
openssl s_client -showcerts -connect LDAP-SERVERIP/DNS:secure-port </dev/null 2>/dev/null|
openssl x509 -outform PEM > LDAP_DNS.pem
```

For example:

```
openssl s_client -showcerts -connect AD01:636 </dev/null 2>/dev/null|openssl x509 -outform
PEM > AD01.pem
```

Here AD01 is the LDAP server and 636 is the secure port.

17. Go to $JAVA_HOME/bin and import the pem file to jssecacerts with below command::

    ```
    $JAVA_HOME/bin#./keytool -import -trustcacerts -alias LDAP_DNS -file <Path>/LDAP_DNS.pem
    -keystore $JAVA_HOME/lib/security/jssecacerts
    ```

    When prompted for password, enter "*changeit*".

    For example:

    ```
    $JAVA_HOME/bin#./keytool -import -trustcacerts -alias AD01 -file $JAVA_HOME/bin/AD01.pem
    -keystore $JAVA_HOME/lib/security/jssecacerts
    ```

    Note The above command creates the jssecacerts file at $JAVA_HOME/lib/security.

18. Go to JMiniX console and type the login credentials:

    Username: **jmx-user**

    Password: **sysadmin**

19. Go to **servers -> 0 -> domains -> com.powerup.configmgr.server.config.jmx -> mbeans -> name=VoyenceControlConfig,type=JMXSystemConfig -> operations**

20. In the **listAll** operation, click **Execute**. In the **CONFIG NAME** column, look for **0.ldap.server.securityprotocol** and **1.ldap.server.securityprotocol**. You will change the values of these configuration names from **none** to **ssl**.

21. To change the values of configuration names, follow these steps:

    - In the **setConfigItem** operation,
        - For **p1**, set the parameter value to **config.security.ldap-auth**
            - For **p2**, set the parameter value to **0.ldap.server.securityprotocol**
            - For F, set the parameter value to **ssl**
            - Click **Execute**.
            - For the same **setConfigItem** operation,
            - For **p1**, set the parameter value to **config.security.ldap-auth**
            - For **p2**, set the parameter value to **1.ldap.server.securityprotocol**
            - For **p3**, set the parameter value to **ssl**
            - Click **Execute**.
            - In the **saveAll** operation, click **Execute**.

22. Change the port number in your Network Configuration Manager installation to communicate with LDAP/Active Directory server. To change the port number, follow these steps:

23. Login to Network Configuration Manager as **sysadmin**.

24. Go to **System Administration** > **Global** > **User Management** > **Authentication Servers -> LDAP**

25 Change the port number to secure port number used in step 3.

26 Click **Apply**.

27 Click **Close**.

28 Logout of Network Configuration Manager.

29 Login to Network Configuration Manager using one of your LDAP/Active Directory server users.

Maintaining the server

13

Read the following topics next:

- Licensing
- Command-line utilities
- Backup and restore
- Purging device revisions and audit history
- System services
- Log files
- Certificates
- Changing the default from address
- Changing the department and company name in the client Dashboard
- Changing the default pull operation
- Database vacuum
- Disabling TCP Fusion
- Password management
- Archiving data
- Performance tweaks
- Switch between advanced and standard security modes
- Location of IP addresses in Servers

Licensing

Obtaining a new license key

For existing Network Configuration Manager customers, you must obtain a new vmware license key for the Network Configuration Manager application. This key can be obtained by emailing your request for a new license key to *licensekeys@vmware.com*. Within your email request you must mention you need to acquire this new license key for Network Configuration Manager.

Note Without this new license key, you will not be able to install Network Configuration Manager.

Installing a license key

The Network Configuration Manager license key is initially installed during the installation process. You cannot install Network Configuration Manager without a valid license key.

Note If you receive a “License Key Invalid” error, upgrade the license key using the License utility. *“Upgrading a license key ” on page 240* provides more information.

Upgrading a license key

Use the License utility to upgrade the license key:

Using the runLicenseCmd script

- From the [Product directory]/tools/license directory, run the command:
  - For Linux,

    ```
    ./runLicenseCmd.sh
    ```

- Type **help** for a list of options.
- Type **Show-license** to display the values for the current license.
- Type **update-license “LicenseFilename.key”** to prompt for a valid system login and then update the license.

The product serial number

Each key has a product serial number associated with it. This serial number appears in the Network Configuration Manager Launch window, and can be used to reference your particular license. You might be requested to provide your serial number when opening an issue with Network Configuration Manager Support.

Handling an expired license key

If you encounter one or more of the following scenarios, the warning lock all accounts or disable the product might display. This indicates one of the following scenarios:

- More devices are managed than are licensed.

- The time limit of license key has expired.
- The IP address of the server has changed.

  If you receive any of the above messages, upgrade the license key using the License utility as described in *"Upgrading a license key " on page 240*.

Command-line utilities

Extract config

This tool extracts the latest revision of a device in the system (and outputs it to a file) to a specified directory.

	Linux
Location	[Product Directory]/tools/extract_config.sh Replace [Product Directory] with the path to the directory you installed Network Configuration Manager to initially. For example, /opt/smarts-ncm/tools/extract_config.sh.
Usage	perl extract_config.sh -network NETWORK -user USER -password ****** -outputdir /OUTPUT/DIR/ -ext FILE-EXT

Parameters	Description
network	Name of the network in the application
user	Valid username in the application
password	Valid password in the application for the user entered above
outputdir	Directory where config files will be placed. The script will create a subdirectory with the network specified
ext	File name extension

Security

The tool uses Network Configuration Manager Security. If a user entered in the tool does not have view password privileges, the passwords and SNMP community strings will be hidden from that user.

Backup and restore

The following information details the backup and restore processes.

Creating a data image

To create a Network Configuration Manager Data Image:

- Run the *backup.pl* script located in the *[Product Directory]/tools* directory using the **perl backup.pl** command. The backup.pl script must be run on the Network Configuration Manager Application server.

  Replace *[Product Directory]* with the path to the directory where Network Configuration Manager is installed.

  For Linux, */opt/smarts-ncm/tools/backup.pl*

- A Data Image is a compressed, time stamped archive, of both the data files and database. The backup script creates a *backup-image-VERSION.AS|DS|CS.DATE.tgz* file in [Product Directory]/data-image/.

  Replace *[Product Directory]* with the path to the directory where Network Configuration Manager is installed.

  For Linux, */opt/smarts-ncm/data-image/backup-image-VERSION.AS|DS|CS.DATE.tgz*

Note If you are taking backup from lower version of NCM (10.1.3 and below) then before taking the backup run the database-changes.pl script present under Utils directory of 10.1.6 installer.

Restoring a data image

To restore a Network Configuration Manager Data Image:

- Run the restore.plscript located in [Product Directory]/tools/ directory using the **perl restore.pl** command. The restore.pl script must be run on the Network Configuration Manager Application server.

  Replace [Product Directory] with the path to the directory where Network Configuration Manager is installed.

  For Linux, */opt/smarts-ncm/tools/restore.pl*

- Pass the full path of the Data Image file to the script using the *perl restore.pl [Product Directory]/data-image/backup-image-10.1.6.0.50.CS.Dec-02-2020-02.00.tgz*

  Replace [Product Directory] with the path to the directory where Network Configuration Manager is installed.

- The version and configuration of the Network Configuration Manager products that are installed when a Data Image is created must match the version and configuration of the Network Configuration Manager Products that are installed when the Data Image is restored.

  For example, if Network Configuration Manager 10.1.6 is installed when a Data Image is created, then Network Configuration Manager 10.1.6 must be installed when the Data Image is restored.

Purging device revisions and audit history

Two tools are available for managing data:

- The **database-utility.pl** script. This script allows you to archive, restore, and purge particular types of data that may grow to a very large size under normal operating conditions. Archiving and/or purging improves application performance by lowering the amount of data that needs to be processed. For detailed usage information for this utility, including argument descriptions and examples, see Database Archive Utility.
- The **purge_audit_history.pl script.** It accepts the number of days as an input and retains the audit data for a given number of days. It also deletes the rest of the data from cm_device_audit_history.

  Note Deleting audit history may lead to data inconsistency in RA reports.

System services

The following service files can be found in the [Product Directory]\bin directory:

- vcmaster status—displays the status of Network Configuration Manager services
- vcmaster start—starts Network Configuration Manager services
- vcmaster stop— stops Network Configuration Manager services
- vcmaster restart— restarts Network Configuration Manager services

Log files

The Network Configuration Manager application log files are located in **[Product Directory]/logs/**. Replace [Product Directory] with the path to the directory you installed Network Configuration Manager to initially.

For Linux, */opt/smarts-ncm/logs/*

The following table provides a brief description of the common log files.

Log File Command	Description
Autodisc	Output from an Auto Discovery
CommMgr	(Device \ Combination server only) output from device communication
Error	Collection of error messages
Logfile	General log file containing top level information

Application server logs

The Application server logs are located in **[Product Directory]/ncmcore/logs**. Replace [Product Directory] with the path to the directory you installed Network Configuration Manager to initially.

For Linux, */opt/smarts-ncm/ncmcore/logs*

Debug logging

By default, debug logging is disabled (turned off). Debug logging might consume a significantly large amount of disk space. It is advisable that debug logging be turned on only when needed.

Step	Action
1	To enable (turn it on) debug logging, edit **[Product Directory]/conf/logs.cfg**. Replace [Product Directory] with the path to the directory you installed Network Configuration Manager to initially. For Linux, **/opt/voyence/conf/logs.cfg**.
2	■ For debugging, locate and uncomment the following line. (Remove the **number sign (#)** at the beginning of the line.) ***:log(0-9):file(10x50000000)**. ■ **Save**, and exit.
3	For Linux, run the **/etc/init/voyence restart** command.

Certificates

Installing Root CA certificate on the client

Note The following applies to configurations where SSL is enabled on the Network Configuration Manager Application or Combination server, using the Network Configuration Manager Self-signed Certificate.

The Network Configuration Manager provides the ability to install the Network Configuration Manager *root CA certificate* on client machines, which is required for accessing the API over an SSL connection.

The Network Configuration Manager root CA certificate is located on the Application or Combination server at **[Product Directory]/conf/CA/voyenceca.crt**.

To install the Network Configuration Manager Root CA Certificate on the Client:

Step	Action
1	Copy **voyenceca.crt** to your client machine.
2	Import **voyenceca.crt** into your browser root certificate store, and the Java Web Start root certificate store.

Note The self-signed certificates that are part of this release are valid for ten years and expire in the year 2027.

SSL Configuration—CA-signed certificates

The Network Configuration Manager provides the ability to use certificates that are signed by a Certificate Authority (CA). An automated utility is available for generating a private key and certificate signing request (CSR), as well as installing and configuring the CA-signed certificate into Tomcat and Apache.

Use the following steps to enable the CA-signed SSL certificate on Network Configuration Manager.

Step	Action
1	Log into the server as a user with administrator privileges. If you have already received the CA-signed certificate, skip to **step 3**.
2	Use the following steps to generate a Private Key and Certificate Signing Request (CSR). ■ Type the following command to change directories to **[Product Directory]\tools\ssl**, and then press **Enter**: cd [Product Directory]\tools\ssl Replace [Product Directory] with the path to the directory you installed Network Configuration Manager to initially. ■ Type the following command, and press **Enter**: **perl ssl-utility.pl –keygen** ■ Follow the screen prompts. You will be asked for general security information about the location of the server, and the hostname; such as country, state, locality, and organization name. Any field you do not want to complete can be left blank, or you can enter a period (.) into that field. The utility generates the following files: ■ **server.key** – the private key ■ **server.csr** – the certificate signing request (CSR)
3	Send the CSR file to your preferred **Certificate Authority** (CA). The CA then returns the signed certificate.
4	**Save** this file to [Product Directory]\tools\ssl\.

Installing the private key and certificate

Use the following steps to install the private key and certificate on Network Configuration Manager.

Step	Action
1	Log into the server as a user with administrator privileges.
2	■ Type the following command to change directories to **[Product Directory]\tools\ssl**, and then press **Enter**: cd [Product Directory]\tools\ssl ■ Where [Product Directory] is the path to the directory you installed Network Configuration Manager to initially.
3	Type the following command and press **Enter**: **perl ssl-utility.pl –install <private key file> <certificate file>** For example: perl ssl-utility.pl –install server.key certnew.cer
4	The installer prompts you to confirm that you want to install the private key and certificate. Type Y, and press **Enter**.

Step	Action
5	Partially through the certificate install, you are prompted to enter a password to protect the private key and Java keystore. This password must be at least six characters. Enter a **password**, and press **Enter**. Once the utility completes, the ncm-as and Apache services are restarted, and a message displays indicating the SSL configuration is complete.
6	Place the **Certificate Authority** (CA) root certificate on each Device server.
7	Download the **CA root certificate** in *base64 format*, and **save** the file as **ca-root-cert.crt**. The root certificate is available from the Certificate Authority's website.
8	**Copy** this file to each Device server, and place it into the **[Product Directory]\conf\CA\** directory.
9	Run the **perl [Product Directory]\conf\CA\cert_hash.pl** utility on each Device server.

Changing the default from address

To change the email address used by Network Configuration Manager from which the job notifications are sent, follow these steps:

Step	Action
1	Login to the Jminix Console. ■ Open a browser. ■ Navigate to the following address: **https://<serverip>:8880/ncm-webapp** ■ Type the **username** and **password** for the Jminix Console. The default username is *jmx-user* and the default password is *sysadmin.*
2	Go to **servers** > **0** > **domains** > **com.powerup.configmgr.server.config.jmx** > **mbeans** > **name=VoyenceControlConfig,type=JMXSystemConfig** > **operations**
3	Locate the **setConfigItem()** operation and provide the following values for the parameters: ■ For parameter 1: **config.server** ■ For parameter 2: **com.powerup.configmgr.server.services.scheduler.email_contact** ■ For parameter 3: Type the *email address* where the job notifications will be sent from. Click **Execute**. **Note** This will temporarily change the value. If ncm-as is restarted, the value will be restored to its default. See below to make the change permanent.
4	To make the new value permanent: ■ Locate the **saveAll()** operation. ■ Click **Execute**.
5	To verify your setting: ■ Locate the **listAll()** operation. ■ Click **Execute**.

Changing the department and company name in the client Dashboard

To change the department and company name using the Network Configuration Manager client dashboard follow these steps:

Step	Action
1	Open the **license.properties** file located here: ■ For Linux: **/opt/smarts-ncm/ncmcore/webapps/ncm-webapp/WEB-INF/classes/license.properties**
2	Inside the license.properties file, you will see: ■ license.licensee=DEPARTMENT ■ license.company=COMPANY Change the values of the **DEPARTMENT** and **COMPANY** properties. **Note** Do not modify any of the key names left of the equal signs.
3	**Save** the file.
4	For Linux,restart the ncm-as service using the **/etc/init.d/ncm-as restart** command.

Changing the default pull operation

To change the default pull operation used by the Network Configuration Manager to pull all known device information, follow these steps:

Step	Action
1	Login to the Jminix Console. ■ Open a browser. ■ Navigate to the following address: **https://<serverip>:8880/ncm-webapp** ■ Type the **username** and **password** for the Jminix Console. The default username is *jmx-user* and the default password is *sysadmin.*
2	Go to **servers** > **0** > **domains** > **com.powerup.configmgr.server.config.jmx** > **mbeans** > **name=VoyenceControlConfig,type=JMXSystemConfig** > **operations.**

Step	Action
3	Locate the **setConfigItem()** operation and provide the following values for the parameters: ■ For parameter 1: **config.server** ■ For parameter 2: Set the value to one of the following: **com.powerup.configmgr.server.services.scheduler.pullafterpush** This is the default option for *pull after a push*. **com.powerup.configmgr.server.services.scheduler.pullafterautodisc** This is the default option for *pull after an auto discovery*. **com.powerup.configmgr.server.services.scheduler.pullafterdevservernotif** This is the default option for *pull after a cut-through*. **com.powerup.configmgr.server.services.scheduler.pullaftersingledeviceautodisc** This is the default option for *pull after a single device auto discovery*. **com.powerup.configmgr.server.services.scheduler.pullafterremedy** This is the default option for *pull after a remedy*. ■ For parameter 3: Set the value to one of the following: **NONE** - A value of *NONE* indicates the default post operation will perform no pull. **PULL_CONFIGS** - A value of *PULL_CONFIGS* indicates the default post operation will perform a pull of the configuration files. **PULL_ALL** - A value of *PULL_ALL* indicates the default post operation will perform a pull of all known device information. Click **Execute**. **Note** This will temporarily change the value. If ncm-as service is restarted, the value will be restored to its default. See below to make the change permanent.
4	To make the new value permanent: ■ Locate the **saveAll()** operation. ■ Click **Execute**.
5	To verify your setting: ■ Locate the **listAll()** operation. ■ Click **Execute**. **Note** For a change to pull after push or a change to pull after auto discovery, the Java Swing Client must be closed and reopened in order to view the changes to future jobs.

Database vacuum

To recover lost disk space created by updating or deleting rows in a database table, a database vacuum must be performed on a regular basis.

Searching for database tables to cleanup

To search the Network Configuration Manager database for tables to cleanup, follow these steps:

Step	Action (Linux)
1	Log into the Database server as a user with administrator privileges.
2	Log into the database as the pgdba user using the **su – pgdba** command.
3	Navigate to the psql prompt. Type **psql voyencedb voyence** to navigate to the psql prompt, and press **Enter**.
4	Run a database query (Query1). Type **select** * **from voyence.cm_calculate_table_sizes;** to run Query1, and press **Enter**.
5	Run a database query (Query2). Type **select** * **from voyence.cm_total_db_size;** to run Query2, and press **Enter**.
6	Compare Query1 and Query2. The first few tables in Query 1 account for most of the size of the database returned by Query 2. If the first few tables in the output of Query1 appear to be very large, these tables must be cleaned using a database vacuum. While running the database vacuum on the first few tables is the most beneficial, it is advisable to clean the entire database. *"Running a full database vacuum" on page 186* provides information for running a database vacuum.

Running a full database vacuum

Note For a full database vacuum, it is advisable to stop all application services and run the database vacuum during a period of down time.

To run a database vacuum on all database tables, follow these steps:

Step	Action (Linux)
1	Log into the Database server as a user with administrator privileges.
2	Log into the database as the pgdba user using the **su – pgdba** command.
3	Navigate to the psql prompt. Type **psql voyencedb voyence** to navigate to the psql prompt, and press **Enter**.
4	Run the database vacuum. Type **vacuum full;** to run the database vacuum, and press Enter. **Note** The database vacuum may take several minutes/hours depending on the size of your database. If "vaccum full" hangs, then go to $VOYENCE_HOME/db/controldb/data and make **autovacuum = off** in postgresql.conf file.

Running a partial database vacuum

To run a database vacuum on one database table, follow these steps:

Step	Action (Linux)
1	Log into the Database server as a user with administrator privileges.
2	Log into the database as the pgdba user using the **su – pgdba** command.
3	Navigate to the psql prompt. Type **psql voyencedb voyence** to navigate to the psql prompt, and press **Enter**.
4	Run the database vacuum. Type **vacuum <table_name>;**, where *<table_name>* is the name of the table to be vacuumed, and press Enter. **Note** The database vacuum may take several minutes/hours depending on the size of your database.
5	Repeat step 4 for each table you want to cleanup.

Disabling TCP Fusion

TCP Fusion can slow down network traffic if your applications are not properly optimized.

To disable TCP Fusion, follow these steps:

Step	Action
1	Log into the server as the root user.
2	Navigate to the **/etc/system** directory. Use a file editing program to open the *system* filefor editing.
3	Add the following line to the end of the *system* file. set ip:do_tcp_fusion = 0
4	Restart the server.

Password management

Changing passwords in Network Configuration Manager

To automatically generate new passwords for all accounts in Network Configuration Manager, follow these steps:

Step	Action
1	Log into the server as a user with administrator privileges.
2	Navigate to the **[Product Directory]/tools** directory. Type **perl password-change.pl** to run the password change utility, and press **Enter.**
3	Type **A** to automatically generate new passwords for all accounts and then press **Enter**.

To change a password for a single account in Network Configuration Manager, follow these steps:

Step	Action
1	Log into the server as a user with administrator privileges.
2	Navigate to the **[Product Directory]/tools** directory. Type **perl password-change.pl** to run the password change utility, and press **Enter.**
3	Type **C** to change a single password and then press **Enter**. A list of usernames displays.
4	Press the number corresponding to the user you want to change the password for and then press **Enter**.
5	Type the new password and press **Enter**.

To synchronize all passwords for the Network Configuration Manager Application server, follow these steps:

Step	Action
1	Log into the server as a user with administrator privileges.
2	Navigate to the **[Product Directory]/tools** directory. Type **perl password-change.pl** to run the password change utility, and press **Enter.**
3	Type **S** to sync all passwords for the Application server and then press **Enter**.

Archiving data

The **database-utility** script performs database maintenance operations. This script allows you to archive, restore, and purge particular types of data that may grow to a very large size under normal operating conditions. Archiving and/or purging improves application performance by lowering the amount of data that needs to be processed.

There are four types of data to archive in Network Configuration Manager.

- **events**: Common Event Log (CEL) events
- **jobs**: Scheduler Jobs
- **revisions**: Device Configuration Revisions
- **auditHistory**: Audit data

  For detailed usage information for this utility, including argument descriptions and examples, see Database Archive Utility.

Performance tweaks

Disclaimer

The following tweaks were tested on 64-bit Red Hat Enterprise Linux 5 and 6 only. Although untested and unsupported, it may be possible to achieve similar benefits on other supported platforms when the system has at least 8 GB of total memory.

Note Making the changes below, on a server with less than 8 GB of memory, can cause a decrease in system performance.

By increasing the number of revision processing threads and the amount of shared memory available to the database, it is possible to improve the device configuration revision processing rate and the overall database performance.

To increase the number of revision processing threads and the amount of shared memory available to the database, follow these steps:

Note If you have installed NCM in a distributed environment,

– perform Step 1 – Step 10 on the Database server and

– perform Step 11 – Step 13 on Application server..

Step	Action
1	Log into the Application server as the **root user**.
2	Stop the Network Configuration Manager services using the following command: service vcmaster stop
3	**Open** the [Product directory]/db/controldb/data/postgresql.conf file for editing.
4	Locate the line **shared_buffers = 32MB**. Replace the above line with **shared_buffers = 512MB**.
5	**Save,** and then **Exit** the [Product directory]/db/controldb/data/postgresql.conf file.
6	Set the shared memory max for Linux to 600MB using the following command: echo 600000000 > /proc/sys/kernel/shmmax
7	**Open** the /etc/sysctl.conf file for editing.
8	Locate the line **kernel.shmmax = 100000000**. Replace the above line with **kernel.shmmax = 600000000**.
9	**Save,** and then **Exit** the /etc/sysctl.conf file.
10	**Open** the [Product directory]/cm/daemon/conf/cdaemon-config.properties file for editing.
11	Locate the line **devsvc.daemon.deviceupdate.max_notif_threads=2**. Replace the above line with **devsvc.daemon.deviceupdate.max_notif_threads=8**.
12	**Save,** and then **Exit** the [Product directory]/cm/daemon/conf/cdaemon-config.properties file.
13	Start the Network Configuration Manager services using the following command: service vcmaster start

Switch between advanced and standard security modes

A security mode is selected during installation. Use these procedures to change the security selection after installation.

Switch from Standard Security to Advanced Security

1 Delete **lockb.ekey** file from NCMBase/data directory. (AS or CS setup)

2 Restart vcmaster services. (AS or CS setup)

Linux: service vcmaster restart

3 If Device server or RA is deployed in different machines, delete existing **lockb.ekey** file from NCMBase/data directory

4 In Application Server m/c, add Device Server and RA hostnames to lockbox (**lockb.clb**) and copy it to respective machines under NCMBase/data directory.

Add distributed system hosts to the lockbox using the cstdriver utility:

```
./cstdriver -lockbox [Product directory]\data\lockb.clb
-passphrase <passphrase> -addHost <FQDN>
./cstdriver -lockbox [Product directory]\data\lockb.clb
-passphrase <passphrase> -addHost <FQDN of Device server>
```

5 Change permissions to ncm:voyence (chown ncm:voyence lockb.clb)

6 Restart vcmaster services in Device Server m/c

On the Device Server:

Linux: service vcmaster restart

Switch from Advanced Security to Standard Security

1 On the Combination Server m/c or Application Server m/c, create the **ekey** file by executing the following command:

```
NCMBase/bin/cstdriver -lockbox ../data/lockb.clb -passphrase <Passphrase> -createKeyFile
```

2 Copy the **lockb.ekey** file from the NCMBase/bin directory to the NCMBase/data directory.

3 Change permissions to root:cst:

chown ncm:voyence lockb.ekey

4 Restart vcmaster services.

Linux : service vcmaster restart

5 If the Device server or RA is deployed on different machines, then copy the **lockb.ekey** file to the respective machines under the NCM Base\data directory.

6 Change permissions to root:cst (chown root:cst lockb.ekey)

7 Restart vcmaster services on Device Server m/c and tomcat service on RA machine.

   On the Device Server:

   Linux: service vcmaster restart

   On the RA Server:

   Linux: service tomcat restart

Location of IP addresses in Servers

This section contains the location of the IP addresses in Servers.

Application server

The following locations contain the IP address in an Application server:

- [Product Directory]/ui/html/index.html contains IP address of the reporting server
- $VOYENCE_HOME/ncmcore/webapps/voyence/powerup.jnlp contains the IP address of the reporting server and the IP address of the Application server.
- Infrastructure Database contains the IP addresses of the Device servers.

  Use [Product Directory]/cgi-bin/cflist.cgi > tmpfile to export the database to a file, and edit the IP addresses on the lines that begin with POP.

  Import the database by running [Product Directory]/cgi-bin/cfwrite.cgi < tmpfile.

Device server

The following location contain the IP address in an Device server:

[Product Directory]/data/devserver/master.addr contains the IP address of the Application server

Database server

The following locations contain the IP address in an Database server:

- [Product Directory]/db/controldb/data/pg_hba.conf contains access list entries for all servers that require access to the database, and the Application server and reporting server
- [Product Directory]db/controldb/data/postgresql.conf contains the external IP address of the Database server on the “listen_addresses” line if the Application server or reporting server is remote from the Database server.

Utilities

14

Read the following topics next:

- Database Archive Utility
- Lockbox utility
- Change NCM passwords

Database Archive Utility

The **database-utility** script performs database maintenance operations. This script allows you to archive, restore, and purge particular types of data that may grow to a very large size under normal operating conditions. Archiving and/or purging improves application performance by lowering the amount of data that needs to be processed.

Here are the types of data to archive in Network Configuration Manager:

- **auditHistory : Audit Data**
- **events**: Common Event Log (CEL) events
- **jobs**: Scheduler Jobs
- **revisions**: Device Configuration Revisions

  The modes of operations for **database-utility** are:

- **Archive**: Moves selected data from the application schema to the archive schema, resulting in better application performance.
- **Purge**: Removes selected data from the archive schema, resulting in smaller database backups.

  The command **purge ra** is also supported; it does not need any arguments. It removes excess data from report tables (cm_rpt_*). It is equivalent to the RA purge script.
- **Restore**: Moves selected data from the archive schema back into the application schema.
- **Prune**: Removes selected data directly from the application schema, resulting in better application performance and smaller database backups.

- **Delete:** Deletes selected revisions directly from the voyence schema. (This mode is equivalent to the vc_purge_revisions_timebased script.) This mode accepts the time_interval for which to retain the data and also the minimum number of revisions to maintain per device

Usage

The pathname to the **database-utility** script is:

/< *product-directory* **>/tools/db-utility/database-utility.pl**

To run the script, follow these steps:

Step	Action
1	Open a command prompt and navigate to **/<** *product_directory* **>/tools/ db-utility/**. For example: **cd /opt/smart-ncm/tools/ db-utility/**
2	Run the **database-utility.pl** script using the following syntax: **./database-utility.pl <COMMAND> <TYPE> <ARGUMENTS>** Where <COMMAND> is **archive**, **delete**, **purge, prune**, **retain**, or **restore**.Where <TYPE> is **auditHistory**, **events**, **jobs**, **latestRAAuditTrail**, or **revisions**.Where <ARGUMENTS> contains the required arguments defined below.

Arguments

The following are the required arguments for the <ARGUMENTS> value, when using the perl **database-utility.pl** script.

- The **events** type requires two arguments:
  - Type of event (device, system, security, or all)
  - Number of days to retain (for example, 1, 2, 3)
- The **jobs** type requires one argument:
  - Number of days to retain (for example, 1, 2, 3)
- The **revisions** type requires one argument:
  - Number of revisions to retain per device (for example 1, 2, 3)
- If the <COMMAND> <TYPE> is **delete revisions**, it needs two arguments:
  - Time interval for saving data enclosed in quotation marks. For example:
    - Linux: ‘2 years’ or ‘3 days’
  - Number of revisions to retain per device (for example 1, 2, 3).
- If the <COMMAND> <TYPE> is **purge ra**, no arguments are required.
- If the <COMMAND> <TYPE> is **retain latestRAAuditTrail**, no arguments are required.
  - This option deletes all the old Audit Trail records from RA tables like cm_rpt* and retains only the latest Audit Trail record.

- If the <COMMAND> <TYPE> is **purge auditHistory**, it needs one argument:
  - Number of days to retain the audit data (for example, 1,2,3)

  Note Event Pruning retains last Nx24 hours of events, whereas Job Pruning retains last N days of jobs.

Examples

The following examples show the usage for the **database-utility.pl** script.

- database-utility.pl archive events all 14
- database-utility.pl archive jobs 30
- database-utility.pl archive revisions 5
- database-utility.pl purge jobs 90
- database-utility.pl purge events system 30
- database-utility.pl prune revisions 10
- database-utility.pl purge ra
- database-utility.pl delete revisions '2 years' 10

  This example retains 2 years of revision data and also maintains 10 revisions per device. It deletes all other revisions from the voyence schema.
- database-utility.pl delete revisions '30 days' 5
- database-utility.pl delete revisions '6 months' 5
- database-utility.pl purge auditHistory 30
- database-utility.pl retain latestRAAuditTrail
- database-utility.pl delete revisions "2 years" 10
- database-utility.pl delete revisions "30 days" 5
- database-utility.pl delete revisions "6 months" 5

Lockbox utility

Lockbox utility provides increased security for data. The lockbox is a file that serves as a local repository for storing the passphrase which is used for encryption of sensitive data such as user credentials. The encryption algorithm is upgraded from Blowfish to AES. The lockbox file can be opened only on the machine on which it is created.

Lockbox utility features

Each lockbox is associated with a Network Configuration Manager component. If you remove the lockbox from a component, the lockbox is rendered unusable.

Encrypting functionality

This encrypts the lockbox passphrase, security questions and answers, and stores them on the server in different locations. This is called by the installer.

Decrypting functionality (for system administrators only)

You can retrieve the lockbox passphrase by running the **decrypt** script.

For Linux, [Product directory]/tools/passphrase/decrypt.sh

This can be run only by the system administrator. After authentication of the system administrator, it provides the lockbox passphrase on the screen.

Unlocking functionality

You can unlock the lockbox internally by running the **unlockLockbox** script.

For Linux, [Product directory]/tools/passphrase/unlockLockbox.sh

This can be run by any user. It prompts for the security answers. If the answer to any one question is correct, it internally unlocks the lockbox. It does not provide the lockbox passphrase to the user. If the answer is incorrect, then the user has to contact the system administrator who can use the “Decrypting functionality” to get the lockbox passphrase.

Unlocking the lockbox using the passphrase

To unlock the lockbox, run the following command:

For Linux,

```
[Product directory]/bin/cstdriver -lockbox [Product directory]/data/lockb.clb -passphrase
<passphrase>
```

Changing the lockbox passphrase

Use the *changePassphrase.pl* utility to change the lockbox passphrase. This utility will save the passphrase in an encrypted file.

Passphrase rules

The passphrase must contain at least:

- One letter in upper case
- One letter in lower case
- One special character

- One numerical
- Minimum fifteen characters

  The special characters that can be used for the lockbox passphrase are:

- Tilde (~)
- At (@)
- Number (#)
- Percent (%)
- Exclamation (!)

Note It is recommended that the passphrase must not start or end with a special character.

Steps to change the passphrase for Linux platform

1 From the [Product directory]/tools/passphrase directory, run the commands:

2 source /etc/voyence.conf

3 perl changePassphrase.pl

The script prompts for old and new passphrase.

4 Type the old passphrase and press Enter.

5 Type the new passphrase and press Enter.

6 Type the new passphrase again and press Enter.

7 Answer the security questions.

8 Restart the ncm-as service.

Change NCM passwords

This section describes how to change the passwords for the Network Configuration Manager database, lockbox, and PKCS certificate to a minimum of 15 characters.

Before upgrading in silent mode, follow the steps to change these passwords to 15 characters.

Procedure

1 Steps to update database password:

   a Execute below commands in NCM Application server:

      1 Run the `$VOYENCE_HOME/tools/password-change.pl` script to update the database password.

      ```
      # type the letter 'C' to change a password  ([C]hange Single Password)
      # type the number '7' to change the database password (7. database)
      # enter the old (9 char long) password when prompted for 'Current Password'
      # enter the new  password when prompted for 'New Password'
      ```

      2 The encrypted password was generated using the NCM java utility. It takes the plain text password as an argument and outputs the encrypted password.

      ```
      source /etc/voyence.conf
      $JAVA_HOME/bin/java -cp "$VOYENCE_HOME/tools" NCM -e PLAIN_TEXT_PASSWORD
      ```

      3 Restart *vcmaster* service.

   b Update Encrypted password in NCM Database server.

   The database password is saved in `/opt/smarts-ncm/conf/setup/install.properties` in an encrypted form in the NCM database server. This file is used by the NCM installer during the NCM database upgrade.

   After changing the password on the Application server, copy the encrypted database password (as mentioned in step **1 > a > 2**) from Application server to the database server.

      1 Open `$VOYENCE_HOME/conf/setup/install.properties` file.

      2 Search for the word *DBPW*.

      3 Replace the old encrypted password with the new encrypted password generated:

      DBPW=<ENC>-395cce2abe818dbee0f4fadaae6c7657</ENC>

2 Steps to update lockbox password.

   a Execute the below commands in NCM Application server:

      1 Run `$VOYENCE_HOME/tools/passphrase/changePassphrase.pl`, and change the new lockbox passphrase to 15 characters.

      2 To unlock the lockbox with new passphrases, run the following command:

      ```
      cd $VOYENCE_HOME/bin
      ./cstdriver -lockbox ../data/lockb.clb -passphrase NEW_LOCKBOX_PASSPHRASE
      ```

      3 Restart *vcmaster* service.

b Execute the below commands in NCM Device server:

1 Run the following commands:

```
source /etc/voyence.conf
cd $VOYENCE_HOME/bin
./cstdriver -lockbox ../data/lockb.clb -passphrase OLD_LOCKBOX_PASSPHRASE -change-
passphrase NEW_LOCKBOX_PASSPHRASE
```

2 Copy the updated *lockb.clb* file from Application server to the Device server and update LOCKBOX FILE location in the *silent-install.properties* accordingly.

3 Restart *vcmaster* service.

3 Steps to update PKCS password:

a Execute the below commands in NCM Application server:

```
source /etc/voyence.conf
cd $VOYENCE_HOME/bin
perl exportcertsintopkcs.pl NEW_PKCS_PASSWORD
```

b Change the ownership privilege, by running the command:

```
chown ncm:voyence $VOYENCE_HOME/conf/bundle.p12
```

c Copy the updated *bundle.p12* file from Application server to the device server and update *CERT_FILE* location in the *silent-install.properties*.

d Restart *vcmaster* service.