RELEASE NOTES

EMC® Smarts®
Network Configuration Manager

Version 9.4.2.0

Release Notes

P/N 302-003-132
REV 01

September, 2016

These release notes contain supplemental information about EMC Smarts Network Configuration Manager. Topics include:

Revision history

Table 1 lists the revision history of this document.

Table 1 Revision history

Revision	Date	Description of changes
01	September, 2016	First release of NCM Version 9.4.2.0.

Product description

EMC Smarts Network Configuration Manager (NCM) is:

- An automated compliance, change and configuration management solution that delivers industry-recognized best practices.
- A collaborative network infrastructure design that controls change processes, provides network device and service configuration transparency, and ensures compliance with corporate and regulatory requirements — to enable you to ensure the security, availability, and operational efficiency of your network.
- An automated support for all facets of the network infrastructure lifecycle, seamlessly integrating critical design, change, and compliance management requirements.

These release notes apply to:

- The core NCM product
- Optional Report Advisor and Compliance Advisor
- NCM Integration Adapter for Smarts Manager
- Smarts NCM Device Services Support

Related Products

The following products are related to Network Configuration Manager 9.4.2.0.

- EMC Smarts 9.4.2 Release Notes for SAM, IP, ESM, MPLS, NPM, OTM, and VoIP Managers
- SolutionPack for EMC Network Configuration Manager
- SolutionPack for EMC Smarts

For information about these products, go to:

https://community.emc.com/community/connect/smarts or https://support.emc.com

Usage Notes

In this document, 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] does not have spaces.

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

For Windows, you can determine your product installation directory and server configuration by accessing the Registry keys at:

- HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Voyence\Control\Configuration \VOYENCE_HOME
- HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Voyence\Control\Configuration \SERVER_CONFIG

NCM Advisors — Report Advisor and Compliance Advisor

Report Advisor (RA) and Compliance Advisor (CA) are included with NCM 9.4.2.0. The NCM installers present options for installing the advisors on the same server with the NCM or on a remote server.

For platform-specific installation instructions, see the *EMC Smarts Network Configuration Manager Installation Guide*.

NOTICE

When the remote server configuration is used, the two servers must have the same operating system type. (Both servers must be Linux, or both must be Windows.)

NCM Integration Adapter for Smarts Manager

This section contains supplemental information about EMC Smarts Network Configuration Manager Integration Adapter.

The integration adapter provides the following functionality:

- Device Synchronization – The adapter ensures that devices found in Network Configuration Manager are also in Smarts Manager, and those found in Smarts Manager are also in Network Configuration Manager. In addition, the adapter has reconciled devices between Smarts Manager devices and Network Configuration Manager devices 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 change into Smarts Manager.
- 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

Table 2 lists the terminologies used in the document.

Table 2 Terminology used in this document

Term	Refers to
SAM	EMC Smarts Service Assurance Manager.
IP AM/PM	IP Availability Manager/Performance Manager
Smarts Manager	Refers to the system with a minimum configuration of one SAM, the Broker, and any associated IP AM.
Adapter	EMC Smarts Network Configuration Manager Integration Adapter for Smarts Manager.

EMC Smarts Network Configuration Manager Device Services Support (DSr)

Device Services Support is a functionality in Network Configuration Manager that provides support to new devices and enhancements to existing device drivers, thus enabling the Network Configuration Manager to access and manage new devices on the network.

Upgrade and migration overview

The following table lists the NCM versions that are supported for upgrade and migration to version 9.4.2.0.

Task	From	To
Upgrade	• Network Configuration Manager 9.3.x or 9.4.x • For Linux, Network Configuration Manager 9.3.x with 9.2.2a Report Advisor • You must first upgrade to 9.4 and then upgrade to 9.4.2.0 if using Network Configuration Manager 9.1.x, 9.2.x, or 9.3.x with 9.2.2a Report Advisor for Windows.	Network Configuration Manager 9.4.2.0
Migration	You must first migrate to 9.4 and then upgrade to 9.4.2.0 if using Network Configuration Manager 4.1.x.	Migrate to version 9.4 and then follow the upgrade instructions to install 9.4.2.0.

For upgrade instructions, see the *EMC Smarts Network Configuration Manager Installation Guide*. For migration instructions, see the *EMC Smarts Network Configuration Manager Migration Guide*.

New features and changes

These release notes describe features and changes associated with 9.4.2.0, 9.4.1.0, 9.4.0.0, and 9.3.x.

New features and changes in Network Configuration Manager 9.4.2.0, 9.4.1.0, and 9.4.0.0

New 9.4.2.0 updates and applicable features introduced with 9.4.0.0 are described in this section.

Third-party software upgrades for 9.4.2.0

- All Apache Common Collections libraries in 3.x version (prior to 3.2.2) which were impacted by remote code execution vulnerability (during de-serialization) have been upgraded to version 3.2.2 where the vulnerability is fixed.
- Oracle Java SE is upgraded to 1.8u91. The Java update includes fixes for multiple security vulnerabilities. All NCM components are updated to Oracle Java 8 update 91, including the Integration Adapter for Smarts Manager.
- For Windows, OpenSSL is upgraded to Win32OpenSSL-1_0_2h.
- Postgres is upgraded to 9.4.7.

EMC Security Advisory "ESA-2016-116" provides more information about the fixed vulnerabilities for Java and Apache Common Collections. EMC Security Advisory "ESA-2016-117" provides more information about the fixed vulnerabilities for OpenSSL.

Migration and upgrade to 9.4.2.0

If using version 9.1.x, 9.2.x, or for Windows, 9.3.x with 9.2.2a Report Advisor, you must first upgrade to Network Configuration Manager 9.4. Then you can upgrade to 9.4.2.

Migration of customizations is supported from NCM 4.1.x (excluding 4.1.0) to NCM 9.4.0.0. You must follow the upgrade procedures to install 9.4.2.0. Migration procedures are described in the *EMC Smarts Network Configuration Manager 9.4 Migration Guide*.

Upgrade is supported from NCM 9.3.x, 9.4.0 or for Linux, 9.3.x with 9.2.2a Report Advisor to NCM 9.4.2. The *EMC Smarts Network Configuration Manager Installation Guide* provides information on upgrade procedures.

NCM version numbering for 9.4.2.0

All NCM chargeable and non-chargeable components hold the following numbering scheme:

- Network Configuration Manager 9.4.2.0 (base application)
- Report Advisor 9.4.2.0
- Compliance Advisor 9.4.2.0
- API 9.1.0 (embedded as a base sub-component)
- NCM Integration Adapter for Smarts Manager 9.4.2.0 (base sub-component add-on)
- DSr (Device Driver) release continues under the current numbering scheme as this is not tied to a NCM version number in the release naming.

  - DSr version for the NCM 9.4.2.0 is DSr 22.0

New features introduced with 9.4.2.0

These features are applicable to 9.4.2:

- For DSr (Device Driver), changes have been made not to show the warning if the attribute model data (OSPF, ACL, VLAN, ARP, Routes) are not configured for the device.
- With this release, you can add the CACHE_ENCRYPT parameter to the NCM Infrastructure Database to encrypt the configuration data. By default, configuration data is not encrypted in the Device Server cache. It appears as plain text. Enabling encryption only takes effect if there is a change in the configuration data (if a new Device Configuration State is created). The *EMC Smarts Network Configuration Manager Security Configuration Guide* provides information about the CACHE_ENCRYPT parameter.

Third-party software upgrades for 9.4.1.0

- All NCM components are updated to Oracle Java 8 update 51
- OpenSSL 1.02d (for Windows only)
- Apache Tomcat 8.0.23

Note: Refer to EMC Security Advisory **ESA-2015-156** for more information.

Migration and upgrade to 9.4.1.0

Migration of customizations is supported from NCM 4.1.x (excluding 4.1.0) to NCM 9.4.0.0. You must follow the upgrade procedures to install 9.4.1.0. Migration procedures are described in the *EMC Smarts Network Configuration Manager 9.4 Migration Guide*.

Upgrade is supported from NCM 9.2.x, 9.3.x, and 9.4.0.x to NCM 9.4.1. The *EMC Smarts Network Configuration Manager Installation Guide* provides information on upgrade procedures.

NCM version numbering for 9.4.1.0

All NCM chargeable and non-chargeable components hold the following numbering scheme:

- Network Configuration Manager 9.4.1.0 (base application)
- Report Advisor 9.4.1.0
- Compliance Advisor 9.4.1.0
- API 9.1.0 (embedded as a base sub-component)
- NCM Integration Adapter for Smarts Manager 9.4.1.0 (base sub-component add-on)
- DSr (Device Driver) release continues under the current numbering scheme as this is not tied to a NCM version number in the release naming.
  - DSr version for the NCM 9.4.1.0 is DSr 21.0

New features introduced with 9.4.0.0

These features are applicable to 9.4.0.0 onwards.

- "Reintroduction of Report Advisor and Compliance Advisor" on page 7
- "Replacement of JBOSS with Spring framework" on page 7
- "SSLv3 POODLE vulnerability (CVE-2014-3566) mitigation" on page 7
- "Alternate storage for the key used to encrypt/decrypt data in Advisors" on page 8
- "Encryption key inaccessible notification from Application Server" on page 8
- "New features and changes in NCM Device Services Support (DSr)" on page 9
- "Performance and scalability" on page 9

NOTICE

To view the release notes for earlier versions, go to Online Support, and navigate to the specific version of the product documentation.

Reintroduction of Report Advisor and Compliance Advisor

Report Advisor and Compliance Advisor are optional components included in NCM. The advisors can be installed using the NCM installer.

Replacement of JBOSS with Spring framework

NCM 9.4.x uses Spring as the underlying Java framework. Accordingly, the JMX Console is replaced by the JMiniX Console for configuring and managing product MBeans.

SSLv3 POODLE vulnerability (CVE-2014-3566) mitigation

NCM 9.4.x includes the fix to disable SSLv3 connections. NCM components are not vulnerable to Poodle attack. For details on this vulnerability refer to:

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566

As a fix, the SSL connections to NCM components (Application server, Report Advisor, MSA, Apache) are disabled and only TLS connections are allowed.

The SAS Security KB reference is https://support.emc.com/kb/194044

NOTICE

To enable connection to the NCM server, SSLv2 and SSLv3 must be disabled on each client machine. For instructions, see the "Client-side required configuration to disable SSLv3" section in the *EMC Smarts Network Configuration Manager Installation Guide.*

Alternate storage for the key used to encrypt/decrypt data in Advisors

With this release, you can choose to use either Advanced security (storing encryption key in RSA lockbox) or Standard security (storing the encryption key in an encrypted format in a flat file) for the Report and Compliance Advisors. In earlier releases, this option was available only for the NCM Core Product.

To use the Standard option for encryption, copy the **[Product directory]/data/lockb.ekey** file from the Application server to the same location on the Report Advisor servers.

Linux

1. Change the permission of the **lockb.ekey** file to **root:cst**.
2. Restart the Tomcat services.

Windows

1. Restart the Tomcat8 service.

Encryption key inaccessible notification from Application Server

Prior to this release, the `Encryption key Inaccessible` notification event was generated only from Device Servers. Now this event is extended to the Application Server as well. This type of event is created when the encryption key becomes inaccessible in the Application or Device servers, and jobs hang. The event also details the possible cause, and will include details of the server IP address.

To resolve a problem:

1. If the lockbox is locked — unlock the lockbox with the following command:

   ```
   $VOYENCE_HOME/bin/cstdriver -lockbox
   $VOYENCE_HOME/data/lockb.clb -passphrase <PASSPHRASE> (for
   Linux)
   $VOYENCE_HOME\bin\cstdriver.exe –lockbox
   $VOYENCE_HOME\data\lockb.clb -passphrase <PASSPHRASE> (for
   Windows)
   ```

2. If filestore is corrupted or not available — re-generate the lockb.ekey using the following command:

   ```
   $VOYENCE_HOME/bin/cstdriver -lockbox
   $VOYENCE_HOME/data/lockb.clb -passphrase <PASSPHRASE>
   -createKeyFile (for linux)
   $VOYENCE_HOME\bin\cstdriver.exe –lockbox
   $VOYENCE_HOME\data\lockb.clb -passphrase <PASSPHRASE>
   -createKeyFile (for windows)
   ```

   Copy the lockb.ekey to the [Product directory]/data of the Application server and copy the same to the same location on the Device server.

3. Restart vcmaster services.

New features and changes in NCM Device Services Support (DSr)

Refer to the *Network Configuration Manager Device Services (DSr) Support Matrix* document.

NOTICE

Some device drivers support only a limited number of models.

Performance and scalability

The *EMC Smarts Network Configuration Manager Version 9.4.1.0 Support Matrix* document provides an overview of the performance and scalability testing as well as system limits when deploying the NCM system and allocating devices that NCM will be managing.

Performance and scalability highlights are:

- The compliance audit of devices recommendation has improved to 1000 devices (config size of ~1MB)
- The policy enforcement of devices recommendation has improved to 1000 devices (config size of ~1MB)
- The time taken to extract the config files has improved significantly with good response time (time taken to extract 180 config files took a minute)

New features and changes in NCM Integration Adapter

There are no new features or changes in NCM Integration Adapter.

New features and changes in Network Configuration Manager 9.3

The following features were introduced in NCM 9.3 and are still applicable to 9.4.x. They are included here for your reference.

- "Alternate storage for the key used to encrypt/decrypt data" on page 9
- "Database Utility for working with NCM data" on page 11
- "Pre-Post Configuration Analysis" on page 13
- "Transformer service" on page 14
- "Masking of Saved Command variables" on page 15
- "MSA authentication using CAS server" on page 16

Alternate storage for the key used to encrypt/decrypt data

With this release, you are provided with an option to choose Advanced security (storing encryption key in RSA lockbox) or Standard security (storing the encryption key in an encrypted format in a flat file).

During fresh install and upgrade

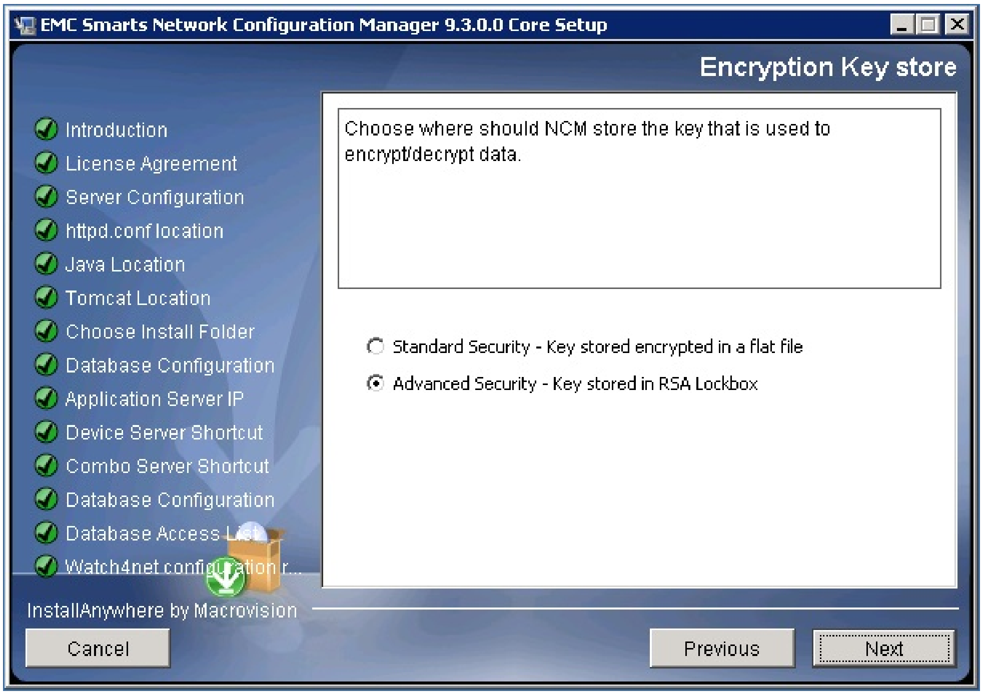
You are prompted with an option for standard or advanced security. Advanced security is the default option.

During a CLI mode installation

You are prompted to choose the location where NCM stores the key that is used to encrypt/decrypt data:

1. Standard Security – Key stored in a flat file
2. Advanced Security – Key stored in RSA Lockbox

Windows GUI mode installation



EMC Smarts Network Configuration Manager 9.3.0.0 Core Setup

Encryption Key store

Choose where should NCM store the key that is used to encrypt/decrypt data.

○ Standard Security - Key stored encrypted in a flat file

● Advanced Security - Key stored in RSA Lockbox

Silent installation

A new property is added to the silent-installer.properties file.

Default is **Advanced Security**. To choose **Standard Security,** change the value to:

```
KEY_STORE="Standard Security"
```

Copying the encrypted flat file to remote device servers

To use the Standard option for encryption, copy the [Product directory]/data/**lockb.ekey** file from the Application server to the same location on all the Device servers.

Linux

1. Change the permission of the lockb.ekey file to root:cst
2. Restart vcmaster services.

Encryption Key inaccessible notification

A new security event notification – Encryption Key inaccessible – is created in Event manager. This type of event is created when the encryption key becomes inaccessible in the Device servers, and jobs hang.

The event also details the possible cause, and will include details of the Device server IP address and IDX. To resolve the problem:

1. If the lockbox is locked — unlock the lockbox with the following command:

   ```
   $VOYENCE_HOME/bin/cstdriver -lockbox $VOYENCE_HOME/data/lockb.clb
   -passphrase <PASSPHRASE> (for linux)
   $VOYENCE_HOME\bin\cstdriver.exe -lockbox
   $VOYENCE_HOME\data\lockb.clb -passphrase <PASSPHRASE> (for windows)
   ```

2. If filestore is corrupted, or not available — copy the **lockb.ekey** from the [Product directory]/data of the Application server to the same location in Device server.
3. Restart vcmaster services.

Database Utility for working with NCM data

A new Database Utility is introduced in NCM 9.3. The utility available in the [Product directory]\tools\db-utility directory, allows you to quickly work with NCM data. It enables fast and easy data transfer, maintenance, and database administration of the application schema and archive schema.

NOTICE

EMC recommends that you use the newly introduced Database Utility (database-utility.pl) instead of the Archive Utility (archive-utility.pl) that continues to be available in the tools directory.

Using the utility, you can archive, restore, purge, prune, and delete particular types of data that may grow to a very large size under normal operating conditions. Archiving, purging, or pruning improves application performance by lowering the amount of data that needs to be processed. There are three types of data that you can work with in Network Configuration Manager.

- Common Event Log (CEL) events
- Scheduler Jobs
- Device Configuration Revisions

Usage

The utility is located in the [Product directory]/tools/db-utility directory. To run the utility, follow these steps:

Step	Action
1	Open a command prompt and navigate to the [Product directory]/tools/db-utility directory.
2	Run the perl database-utility.pl script using the following command: `perl database-utility.pl <COMMAND> <TYPE> <ARGUMENTS>` Where *<COMMAND>* is archive, purge, or restore. Where *<TYPE>* is events, jobs, or revisions. Where *<ARGUMENTS>* contains the required arguments defined below.

Commands

Command	Description
archive	Moves selected data from the application schema to the archive schema, resulting in better application performance.
restore	Moves selected data from the archive schema back into the application schema.
purge	Removes selected data from the archive schema, resulting in smaller database backups.
prune	Removes selected data directly from the application schema, resulting in better application performance and smaller sized database backups.
delete	Deletes selected revisions directly from the voyence schema (It is equivalent to vc_purge_revisions_timebased script), it accepts the time_interval for which to retain the data and also to maintain minimum number of revisions per device

Types

Type	Description
events	Application CEL events. Requires two arguments: • type of event (DEVICE, SYSTEM, SECURITY, all) • number of days to retain
jobs	Scheduler jobs, requires one argument: • number of days to retain
revisions	Device configuration revisions, requires one argument: • number of revisions to retain per device If you use *delete revisions*, you must provide two arguments.
ra	Removes excess data from report tables (cm_rpt_*). RA purge does not require any arguments. **Notice:** This is equivalent to RA purge script available in earlier releases of NCM.

Examples

- Move all events from the application schema to the archive schema, and retain 14 revisions per device:

  ```
  database-utility.pl archive events all 14
  ```

- Retain two years of revision data and also maintain 10 revisions per device. And deletes the rest of revisions from voyence schema:

  ```
  database-utility.pl delete revisions '2 years' 10
  ```

  NOTICE

  On Windows, the time interval input must be provided in double quotes.

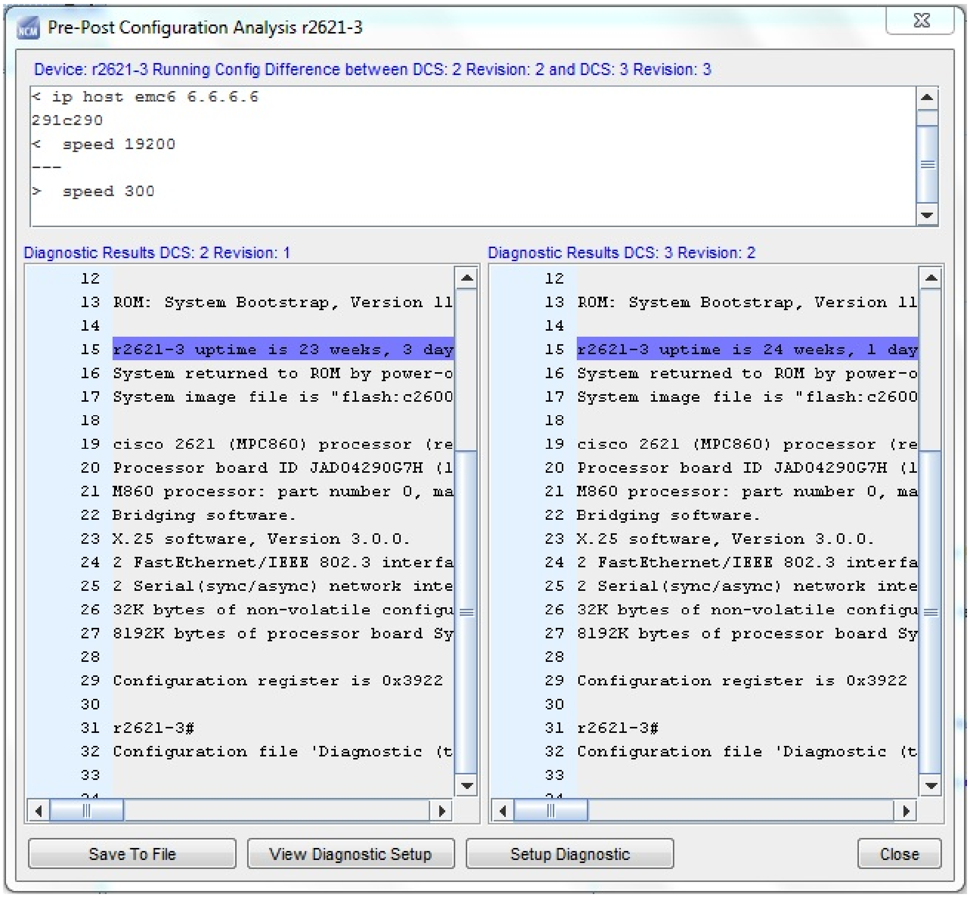
Pre-Post Configuration Analysis

A new feature is introduced in NCM 9.3 by enhancing the Diagnostic Utility of NCM, which:

- Provides network administrator a validation of the configuration changes made to device
- Allows the network administrator to create a report which functions as a proof of changes made to devices. You can download the comprehensive report which details the diagnostic results between the current and previous configuration revisions. To generate the report:

1. Right-click a device
2. Select **Pre-Post Configuration Analysis**

   A comprehensive report is displayed.
3. You can perform these operations:
   - Save to File (saves the results of the diagnostics to a Microsoft XLS file)
   - View Diagnostic Setup
   - Diagnostic Setup



Device: r2621-3 Running Config Difference between DCS: 2 Revision: 2 and DCS: 3 Revision: 3

```
< ip host emc6 6.6.6.6
291c290
<  speed 19200
---
>  speed 300
```

Diagnostic Results DCS: 2 Revision: 1

```

ROM: System Bootstrap, Version 11

r2621-3 uptime is 23 weeks, 3 day
System returned to ROM by power-o
System image file is "flash:c2600

cisco 2621 (MPC860) processor (re
Processor board ID JAD04290G7H (1
M860 processor: part number 0, ma
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interfa
2 Serial(sync/async) network inte
32K bytes of non-volatile configu
8192K bytes of processor board Sy

Configuration register is 0x3922

r2621-3#
Configuration file 'Diagnostic (t

```

Diagnostic Results DCS: 3 Revision: 2

```

ROM: System Bootstrap, Version 11

r2621-3 uptime is 24 weeks, 1 day
System returned to ROM by power-o
System image file is "flash:c2600

cisco 2621 (MPC860) processor (re
Processor board ID JAD04290G7H (1
M860 processor: part number 0, ma
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interfa
2 Serial(sync/async) network inte
32K bytes of non-volatile configu
8192K bytes of processor board Sy

Configuration register is 0x3922

r2621-3#
Configuration file 'Diagnostic (t

```

Transformer service

A new service named Transformer has been introduced. The service is integrated with the core NCMmaster (Windows) or vcmaster (Linux) service of NCM. The service allows you to perform the following intensive database operations in the background:

- When a compliance enforcement is performed, the audit trail data is split and updated in the respective reporting tables. The table names are suffixed with a cm_rpt*
- When a configuration revision is created, the cm_config_diff table is updated with the configuration difference between the n and n-1 revisions
- When you perform a bulk device deletion activity, the service deletes devices and the associated data in batches in the background.

Configuration files

The following configuration files are available in [PRODUCT DIRECTORY]/Transformation/conf/

File name	Property name	Default value	Description
transformer.properties	transformer.interval	30	This is the interval in which the transformer thread runs to poll for any new revision created or enforcement done. To edit change the value and restart the transformer service. Value is in seconds.
	configDiffDT.batchSize	500	Data transformer batch sizes - these are the max number of records picked for processing per run by each transformer
	dcsDiffDT.batchSize	500	Data transformer batch sizes - these are the max number of records picked for processing per run by each transformer
	auditTrailDT.batchSize	500	Data transfomer batch sizes - these are the max number of records picked for processing per run by each transformer
devicedeletion.properties	deviceDeletion.interval	1800	This is the interval in which the device deletion thread will poll for any new devices in the REMOVED state. The value is in secs. Default is 1800 secs.
	deviceDeletion.batchSize	5	Number of devices to be deleted in every batch

Log files

To troubleshoot problems with the Transformer service, review the log file available at: ‹PRODUCT_HOME›/Transformation/logs/transformer.log

How to stop and start the transformer service

On Linux

```
Service transformer stop
Service transformer start
```

On Windows

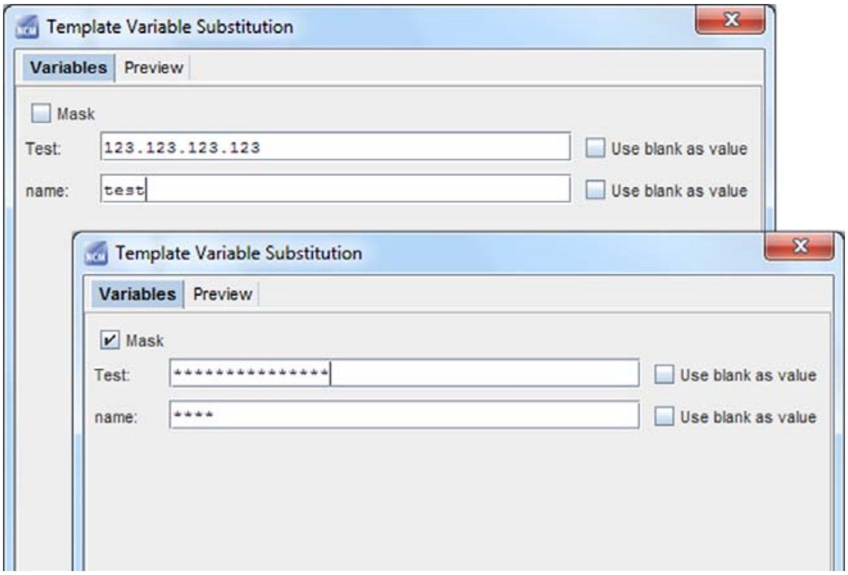
Go to Service Manager and click on the NCM_Transfomer service to stop/start manually.

Masking of Saved Command variables

An enhancement has been made to Saved Command, to mask the values of the template variables.

1. If you had created a Saved Command using template variables, and then you run the saved command, a *Template Variable Substitution* dialog appears.
2. Enter the values of the Template variables.
3. Select the Mask check box:

   If Mask is selected, the template values entered are masked with **** characters.


Template Variable Substitution
Variables
Preview

□ Mask

Test: 123.123.123.123 □ Use blank as value

name: test □ Use blank as value

Template Variable Substitution
Variables
Preview

☑ Mask

Test: *************** □ Use blank as value

name: **** □ Use blank as value

MSA authentication using CAS server

The change reports that contain the configuration differences, and the audit trail reports are displayed using an external URL. The data is displayed in the EMC M&R browser frame.

The external web application is hosted on the MSA tomcat server of NCM. The data required for the reports are retrieved using the MSA interface.

To allow authentication to this application, a CAS authentication server is deployed along with ncm-msa service. When you try to access the web application URL, the UI prompts you for the MSA username and password. The default password for the user (msa-user) is listed in the *EMC Smarts Network Configuration Manager Security Configuration Guide*.

To change the password for the MSA user

1. Run [Product directory]/tools/password-change.pl.
2. Choose msa-user and change the password.
3. Restart vcmaster service.

Fixed problems

This section lists the problems that are fixed in the 9.4.2.0 release. The table includes the following information for each fixed problem:

- CQ or SR number is a unique ClearQuest (CQ) or Service Request (SR) number that is used to track the problem. Each problem is assigned a CQ number. A problem is also assigned an SR number if the problem is reported by a customer.
- Problem summary is a short description of the problem.
- Description of fix is a short explanation of how the problem was addressed.

All NCM releases are cumulative; each successive release includes all fixes from earlier releases.

This release contains the following fixed problems:

- "Network Configuration Manager fixed problems" on page 17
- "NCM Integration Adapter for Smarts Manager fixed problems" on page 27

Network Configuration Manager fixed problems

Table 3 lists the problems that have been fixed in EMC Smarts Network Configuration Manager 9.4.2.0.

Table 3 Fixed problems in NCM 9.4.2.0 (page 1 of 6)

CQ or SR number	Problem summary	Description of fix
IS-4821, 74207732	The ncm_monitor.sh script doesn't generating hibernate statistics anymore in 9.4.	Code has been modified.
IS-6104	_svn directories under Apache web server should be made read-only for root.	Code has been modified to remove _svn directories.
IS-5535, 76022710	Java Deserialization Vulnerability	All Apache Common Collections libraries in 3.x version (prior to 3.2.2) which were impacted by remote code execution vulnerability (during de-serialization) have been upgraded to version 3.2.2 where the vulnerability is fixed. EMC Security Advisory "ESA-2016-116" provides more information.
IS-5418, 75936262	Need update in NCM 9.4.1 Install guide. The text on Page 20 is not clear. Customers who are on 9.2.2a or 9.3 think that they can directly install 9.4.1 on new host, take backup of 9.2.2a/9.3 from old host and perform restore on the 9.4.1 install, which will fail.	In the *EMC Smarts Network Configuration Manager 9.4.2 Installation Guide*, the revised text is on Page 19. The text states which NCM versions cannot be directly upgraded to 9.4.2 and must be upgraded to 9.4 first. Also, there is a description about using the backup.pl tool.
IS-5825 75931452	While purging jobs on database "foreign key constraint" exception is received.	Code has been modified to handle the exception.
IS-6413, 79268092	Not able to schedule recurring jobs in NCM using JAVA API.	Code has been modified to use the correct timezone.
IS-5998 77800082	Clear text passwords are visible in xml files.	Code has been modified to mask the keystore password.
IS-5266, 75559516	While taking the backup using the back.pl script, if the database is remote, the "controldb:unrecognized service" error is thrown.	Changed the code to execute checkDBStatus() function only in case of local Database.
IS-5763	Selection lists don't scale when windows is resized.	Modified the selection list panel to use BorderLayout instead of Gridbaglayout.
IS-5744	postgresql upgrade is required as 9.0 version is not supported anymore.	Upgraded postgresql to the supported 9.4.7 version.
IS-5899	Data left in some tables after removal of all devices.	Code has been modified to ensure that dm_vlan and dm_vlan_trunk_protocol data is deleted whenever the devices are deleted.
IS-2484, 68590928	The physical/virtual classification of interfaces is broken.	Code has been modified.

Table 3 Fixed problems in NCM 9.4.2.0 (page 2 of 6)

CQ or SR number	Problem summary	Description of fix
IS-5269, 75865678	Device configurations encrypted in database but stored clear text in the device server cache.	Add the CACHE_ENCRYPT parameter to the NCM Infrastructure Database to encrypt the configuration data as described in the *EMC Smarts Network Configuration Manager Security Configuration Guide*.
IS-6751	The created pgadb user have illegal uid's.	Code has been modified to ensure that pgdba user uid values are legal (greater than 500).
IS-6090, 78197912	Clear text passwords in uninstall log files	Code has been modified.
IS-6081, 78932304	NCM unable to forward TACACS user credentials on cut-through.	Changed the code to ensure credentials are encrypted correctly, so that decryption happens successfully.
IS-6543, 67245178	Hibernate/EHCache will produce warnings about unconfigured classes on startup.	Warnings are no longer produced.
IS-5738	Transformation engine will check existence of the cm_config_diff and cm_rpt_dcs_diff tables, but not the other cm_rpt* tables.	Modified the code and have put the check for existence of other tables as well.
SND-3764	Creating/updating checks through the API throws exception if data field filter has value as "any".	Handled null value in the code.
IS-6672	Device removal failed halfway and caused major differences between AS and DS.	Modified the code to handle the exceptions correctly.
IS-5751	cm_device_comments table cannot be cleaned up.	Overloaded getOperationalDeviceInfo() and getDesignDeviceInfo() APIs and added getDeviceComments flag as a parameter. If the getDeviceComments flag is true, device comments are included in return parameter. If false, return parameter will not contain device comments.
IS-5900	database-utility.pl cannot remove old report table data.	For entries deleted from cm_device_audit_history, the corresponding entries from the cm_rpt_enforment_trail table are deleted, except for entries with state_number 1 which do not have corresponding cm_device_audit_history entry.
IS-6757, IS-7191	TFTP shouldn't be enabled on the AS, only on the DS. This is a security issue.	For an Application Server, a new NCM 9.4.2 installation will ensure that the TFTP status will not be altered. The TFTP is not needed in the Application Server. For an upgrade from an older release on the Application Server, you need to change the TFTP setting according to your security requirements prior to performing the upgrade.
IS-7073, 80845096	Massive Security Risk msa-user default password "sysadmin" still works on GUI after changing it in with the password-change.pl.	Changed the code to ensure Application Server is not validating msa-user against default sysadmin password. Also, changes are done to update the password of msa-user after the change.
IS-6089 77405840	Clear text passwords in log files when silent install or upgrade is done.	Code has been modified to mask the passwords shown in plain text.
IS-5839l, 67245178	default values used for ehcache classes	Handled the warnings which were shown for default values.

Table 3 Fixed problems in NCM 9.4.2.0 (page 3 of 6)

CQ or SR number	Problem summary	Description of fix
SND-2159, 71258936	Running ldconfig generates errors about NCM libraries.	Changed the code to make sure duplicate libraries are not present.
IS-4822 74208180	Multiple underscores are not working for Device Data field names.	The issue was due to similar patterns not being handled in the Code. Changes have been made to handle the similar patterns.
IS-4828 74207240	When adding/editing credentials, copy/paste of the password was not working.	This was due to paste option not being allowed for password fields. Changes have been made to allow to paste in the password fields.
IS-4732 73899906	Server logs has a lot Errors.	This was due to the translation table not having the mappings for all the encapsulation types. The translation table is updated with all the mappings.
IS-4818 74186050	Device cached data is not always deleted when a device is deleted.	The device deletion is a two-step activity. During 1st step the device is moved to unclassified state and the device cache data deletion is started. During the second step devices are moved to unmanaged state and removed. The issue was due to the same field being updated in both the steps which was stopping the cache data deletion once the second step is initiated. Code is changed and now for deletion of device cached data a separate field is maintained which makes sure that the cache deletion is continued in the second step as well if it's not completed in the first step.
IS-5015 72045486	Discovery of a large number of devices causes device server restart.	This was due to devices sending an abnormal communication disconnect during Pull operations. This situation was not handled in the driver code and triggered a TIMEOUT after the usual wait period. Although the session was disconnected from the device for Device Server the Session was still active. On subsequent operations when Device Server tried to use the same corrupted session handler, it crashed. Changes has been made to remove the corrupted session handlers from the SSH session cache. This will ensure that there are no further interactions with the device using the corrupted session.
73828704	PermSize and MaxPermSize options need to be removed from the JVM settings.	Since Permanent generation has been completely removed in JDK 8, PermSize and MaxPermSize parameters have also removed from JDK. Instead of Perm Gen space, JDK8 has introduced MetaspaceSize. Code is updated to remove PermSize & MaxPermSize options and add MaxMetaSpaceSize.
IIS-5068 75134876	NCM UI Client was switched from https to http.	This was done for Performance improvement. The change is documented in *NCM 9.4.1 Security Configuration Guide* which can be downloaded from EMC Online Support (*https://support.emc.com*). The steps to re-configure NCM Client to use https are also documented in the guide.
IS-5067 75138150	During discovery and pull all for large number of devices, few devices discovery and pull fails.	This was due to the delay caused during clearing of the receive buffer. Code is changed not to cause the delay while clearing the receive buffer.

Table 3 Fixed problems in NCM 9.4.2.0 (page 4 of 6)

CQ or SR number	Problem summary	Description of fix
75864778	"Device Data Field" doesn't work when applied to Network Level Device Filtering.	“Device Data Field” was not working earlier, now changes are done to make it work as Data Field.
IS-2012	The transformer user shouldn't be created with a fixed uid, as it could already be in use.	Code has been modified to dynamically generate the transformer uid.
IS-5546	System information is exposed when fingerprint.jsp is run.	”fingerprint.jsp” file, examples directory and docs directory are removed from the installation as they expose system information.
IS-5597	Old useless code exists in database-utility.pl.	Removed un-used code from the database-utility.pl.
IS-5549	Setting default datafield value to a long string causes an exception.	Code has been modified not to allow the user to enter more than 255 characters for data field value.
IS-3420 75863724	Contextual launch is not working in NCM.	Added support for the documented URL pattern.
IS-5085	Unable to reset admin password via SysAdmin.	In the SysAdmin console web page, “Active Users” tab is added where reset admin user button is present to reset the sysadmin password to the default value. Note: User needs to logout and re-login to UI, if sysadmin password is reset from SysAdmin console
IS-5736	It’s not possible to cleanup cm_config_diff table.	Modified the database utility to clean up existing stale entries in cm_config_diff using ‘purge ra’ option. Usage: ./database-utility.pl purge ra Archive, prune or delete revisions options of database utility will cleanup cm_config_diff table in addition to cleaning up configuration file revision table.
IS-5749	use strict commented out in database-utility.pl script.	‘use strict’ is enabled and the script now works as intended.
IS-5548	Old rejected jobs cannot be deleted.	Permission for ‘non-sysadmin’ users has been modified to enable deletion of the jobs having tasks associated with deleted/unclassified devices.
IS-5737	Incorrect login error message if server is not reachable.	Error message has been modified to reflect the correct status.
IS-5742	java.util.ConcurrentModificationException is thrown from GUI if multiple jobs are deleted concurrently from Schedule Manager.	Code has been modified to prevent multiple threads from updating Job status in parallel.
IS-5752	Device deletion process of the transformation engine doesn't delete data from the archive tables.	Device deletion code has been modified to delete the data from cm_config_file, cm_dcs_cu_link and cm_device_revisionable_state tables of archive schema and cm_config_diff table of voyence schema for the deleted devices.
IS-5748	getAllUnmanagedOpsDevices API call is broken.	The functionality of the “getAllUnmanagedOpsDevices” is working as expected. The stale device entries in the database were caused due to a missed conditional update in “removeDevicesFromSystem” API that has been fixed.

Table 3 Fixed problems in NCM 9.4.2.0 (page 5 of 6)

CQ or SR number	Problem summary	Description of fix
IS-5745	backup.pl script still contains Solaris support.	Solaris support has been removed from backup.pl, restore.pl, syncPasswords.pl and saveLogs.pl scripts.
IS-5746	backup.pl has a security issue; it assigns world writeable permissions to pg_dump file.	Permissions are corrected in backup.pl, restore.pl and password-change.pl scripts.
IS-5740	NCM GUI client hangs after doing policy enforcement on large number of devices.	This Issue was due to the server accepting synchronized requests from the client. The server code is modified now to accept multiple requests from the client.
IS-5836	Exported tests cannot be imported again.	This happens if the value of “packageidentifier” is sent as string instead of an integer. This is handled in the code by casting string to integer.
IS-5904	database-utility.pl script has incorrect comment.	Comments in the database-utility.pl script are corrected.
IS-6008	Only 10 groups are captured from the regex test when compliance audit is run on the devices.	While evaluating the scope of the test, upper limit of 10 groups is removed.
IS-6124	User with full access rights for a network cannot add/edit autodiscovery jobs.	This was due to loading of RSA token server which requires sysadmin privileges. This is handled by initializing RSA token server at the time of startup.
IS-6145	Need help in changing the number of devices on which policies can be enforced.	New properties file “api_config.properties” is introduced under “$VOYENCE_HOME/ncmcore/webapps/ncm-webapp/WEB-INF/classes” to configure the number of devices for policy enforcement. By default the maximum number of devices for policy enforcement is configured to 1000(recommended). After changing the default value, ncm-as service should be restarted.
IS-6184 75865110	When colon is used in the data field value, data field filter doesn’t work.	Code has been modified to allow colon in the data field value.
IS-5739	The device deletion thread from the transformation engine keeps the transaction running for long time and keeps on holding the lock on the database tables.	Code has been modified to commit the transaction after getting the list of devices which are in removed state.
IS-5503	Catalina.out from $VOYENCE_HOME/ncmcore/logs directory is not collected by saveLogs.pl tool.	saveLogs.pl tool is modified to collect the catalina.out file from $VOYENCE_HOME/ncmcore/logs directory.
IS-6147	backup/restore scripts complete successfully when lock file is present.	Corrected the exit code to 1 in case lock file is present, to indicate the failure.
IS-6148	Integration JMS queue sample code not working.	Added the new sample code under API samples to connect to the “activemq”.

Table 3 Fixed problems in NCM 9.4.2.0 (page 6 of 6)

CQ or SR number	Problem summary	Description of fix
IS-5656 77277450	Inconsistent Behavior with Octet String in Trap Varbind	This issue is because Octet string provided by snmp++ has different display formats (Hex, String, Both(default)). This is a global parameter which will apply for all Octet String. In application code the format is changed to String only format, thus it was changing the display format. With the fix when trap is received the format is reset to "Both", so that it will have same behavior for each trap received.
IS-5780 77335148	Usage of the API returns an exception randomly.	Pessimistic locking is introduced in the user table to avoid multiple threads getting different version of User objects.
IS-6220 78685320	tomcat's log file, catalina.out grows uncontrollably.	Explicit console logging by NCM is disabled as this information is duplicate and also present in powerup.log and server.log. Now catalina.out logs will show only the tomcat server related logs.
IS-6091 78194456	9.4.1: backup/restore scripts complete successfully when lock file is present.	Exit code is changed to 1, if the lockfile is present.
IS-6146 78405262	NCM 9.4.1 Hotfix 5 - migration install fails on remote DS.	Have modified the code to forcefully stop the device server services during patch installation.
IS-6068 77902812	9.4.1: Exception occurs copying an OS push job over to a new job.	Modified the code to update the device details for the task when the job is copied. Note: Java cache needs to be cleared from the client machine as there is a change in the UI jar.

Table 4 lists the problems that have been fixed in EMC Smarts Network Configuration Manager 9.4.1.0.

Table 4 Fixed problems in NCM 9.4.1.0 (page 1 of 5)

CQ or SR number	Problem summary	Description of fix
IS-4788	In Red Hat Linux 7, the /init.d directory was changed to /bin and that caused the restore.pl script to fail.	The script has been updated.
IS-4720	PermSize and MaxPermSize options have been removed in Java 8.	These parameters PermSize and MaxPermSize are removed from java 8. Replaced with MetaspaceSize and MaxMetaspaceSize parameters.
IS-4603	Compliance will always pass when using User Defined Fields and Exact Order.	Device data fields were used in the regex test with exact order. This failed to result the correct compliance state. The required Java class file was modified to accommodate the changes for exact order.
IS-4185	Remediation tests using precondition variables tests insert these statements at the end of the remediation.	The order of the remediation was not proper when precondition variable used. Have modified the required java class file to accommodate the changes.
IS-3802	Device Display Filter does not function correctly when device class filter used. This behaviour observed intermittently.	Delayed the device class filter operation for 20 milli seconds to display the filtered output correctly when Reset/Add/Remove buttons pressed

Table 4 Fixed problems in NCM 9.4.1.0 (page 2 of 5)

CQ or SR number	Problem summary	Description of fix
IS-3751	NCM - 9.4 catalina.out log filling up every day over 40gb	Have removed the cache warning message in catalina.out file which fills up the catalina.out file rapidly.
IS-3701	Performance and Scalability: Performance degraded observed in 9.4 Patch 2 while logging in to NCM UI initial screen.	Code has been modified to improve the performance.
IS-3627 71105464	NCM client has a caching issue, where it sometimes happens that a new policy will show the area selection of the previous open policy.	Made the buffered listener to non-buffered so that it always shows the new policy selection.
IS-3616 71182872	Transformer user not created as UID 514 already in use.	Ensured that the transformer user is allocated a random UID by the Linux rather than a static UID, that is, 514
IS-3599 71106246	The output of cmstatus is partly broken.	Irrelevant data from the the cmstatus output has been removed and only relevant data (Summary and Details) are processed and displayed.
IS-3391 71182872	Report Advisor not allowing filtering by views.	Changes have been made to get all the views under a particular network in the RA settings window, so that user can filter the views in a network.
IS-3076	Save Command Preview pane displayed blank screen when DASL used in Template.	Modified the code to allow the DASL code in the preview pane of Template dialog window during Save Command.
IS-3073 69913748	NCM Smarts adapter is not able to authenticate and throws error "ERROR Public API Connection is DOWN" in the log file.	NCM adapter installed in dark site setup, the spring xsd schema files are now referred from the classpath instead of referring it from the Internet.
IS-2873 69236222	9.4 NCM javadoc had getReadOnly and getReadWrite APIs which were not documented.	The APIs getReadOnly and getReadWrite are documented as internal APIs in javadoc
IS-2867	Performance and Scalability: Performance degrade is observed in 9.4 J2EE APIs when compared to 9.3	Code has been modified to improve the performance
IS-2866	Performance and Scalability: Performance degrade is observed in 9.4 WS APIs when compared to 9.3	Code has been modified to improve the performance
IS-2756 69366566	Email Notifications will not be sent to users when the job Status changes.	Modified the code to make it work.
IS-2740 69394990	NCM 9.4 RA fresh install fails to launch.	Changed the applicationContext.xml to use the existing version of the XSDs which are bundled with the binaries.
IS-2696	NCM to device communication was not working after changing the ciphers and algorithms on the devices.	Algorithm in the putty code is changed to hmac ssh 256 to resolve the issue.
IS-2673 69346376	Scheduled Autodiscovery job failed on NCM 9.4 installation.	When the prompt user option is enabled, there were 2 different hibernate sessions involved to save the job details. Fixed the issue to use the same hibernate session.

Table 4 Fixed problems in NCM 9.4.1.0 (page 3 of 5)

CQ or SR number	Problem summary	Description of fix
IS-2671 68378800	Push Job fails, using Prompt on Manual Execute	When credentials are passed from the UI made sure that e_salt key is added for encrypting the credentials, if it's not there.
IS-2661	Set a filter in regex test and do compliance audit. Remove the filter in the regex test and made it to default while auditing throws an error.	Modified the code to avoid the error when the filter sets to default in regex test.
IS-2654 69230242	Copying the Automation Library Item folder from one network to another does not happen.	Modified the code to copy the folder correctly.
IS-2633 69172508	WS APIs will take more time for giving the results.	Enabled the lazy loading made other code changes
IS-2632 69172140	WS enforcePoliciesOnDevices(String jobName) API call was broken in 9.4.	Included the code in the server side to make WS Api enforcePolicies(String jobName) to work
IS-2623	The following DISA Goals requires changes in the rule definition DISA STIG NET0240 DISA STIG NET0440 DISA STIG NET0470 DISA STIG NET0600 DISA STIG NET0812 DISA STIG NET0820 DISA STIG NET0890 DISA STIG NET1639 DISA STIG NET1665 DISA STIG NET1660 DISA STIG NET-NAC-012	The required changes are made in the rules.
IS-2569 68880558	NCM and RA UI will not launch if NCM and RA servers are installed in the dark site.	Bundled the required dtd file for NCM Core to work. For RA changed the applicationContext.xml to use the same versions of XSD files which are bundled within the binaries.
IS-2538 68902606	When invoked via Browser Axis Happiness Page shows system usernames and passwords.	Removed the happyaxis.jsp page from the NCM deployment as this is not required for NCM.
IS-2534 68806502	Healthcheck functionality broken due to cmstatus binary not having enough permissions on DS instances.	Cmstatus file has been given enough permissions such that the DS would invoke it to send the results to AS so that the healthcheck page shows the results
IS-2523 68803138	NCM UI will not launch if it's installed on the server not having the Internet connectivity.	Bundled the required dtd file for NCM Core to work.
IS-2415 68363202	Two regex tests are looped by one test referring the another test variable. The test variable is resolved to a value. If this resolved value is present in the config file multiple times, while doing compliance audit, then this results in OutOfMemory error because of looping multiple times.	Resolved the code to look for the value correct number of times and avoid the looping. Now the compliance audit will not throw OutOfMemory error when the resolved value present in the config file multiple times.

Table 4 Fixed problems in NCM 9.4.1.0 (page 4 of 5)

CQ or SR number	Problem summary	Description of fix
IS-2321 67858850	A user was not able to generate custom self-signed certificate since NCM ships with its own self-signed certificate.	New tool has been provided to generate a custom self signed certificate Tool: $VOYENCE_HOME/tools/ssl/ssl-utility-self-signed.pl
IS-2105 67340504	Cfwrite.cgi binary can be invoked through an URL which causes infraDb database to be reset thus leading to a severe security issue.	Cfwrite.cgi now ignores the request if invoked through the URL thus ensuring no update to the infraDb database.
IS-2019	POSTUN_SCRIPTS_ERR=Can't open perl script "SysAdmin.pl": No such file or directory	SysAdmin, Core and AppServer.pl are not present in DB install. Modified the uninstaller to invoke these only if present.
IS-2018	DATABASE_POST_ERR=ls: cannot access /opt/smarts-ncm/ui: No such file or directory	Code is changed to take care of error thrown during uninstallation of database service when it doesn't exist.
IS-2017	AS uninstall log (Uninstall-NCM-9.3.0.0-debug.log) contains errors/warnings.	The errors were due to having the same uninstallation scripts called for AS/DS/DB/CS uninstallation. The code is updated to call the relevant scripts only.
IS-2016	AS install log (NCM-9.3.0.0-debug.log) contains errors/warnings.	Code is updated to correct errors.
IS-2008	DS uninstall log (Uninstall-NCM-9.3.0.0-debug.log) contains errors/warnings.	The errors were due to having the same uninstallation scripts called for AS/DS/DB/CS uninstallation. The code is updated to call the relevant scripts only.
IS-2005	DS install log (NCM-9.3.0.0-debug.log) contains errors/warnings.	Code is updated to correct errors.
IS-1999	The AS installation creates errors in the DB log.	Few db sequences were recreated. The code is updated to prevent the recreation of these sequences.
IS-969	Security: No logout option in DDT page after logging into the page.	Logout button and functionality added for DDT tool.
SND-1889	The DSr version HF number is incorrect in 9.4 UI -> Help->About.	Modified the code to make it work. For Linux: Check /etc/voyence.conf (or) [Product Directory]/conf/setup/install.properties DSR_MINOR_VERSION for the correct HF version. In Windows: Check [Product Directory]\conf\setup\install.properties DSR_MINOR_VERSION for the correct HF version.
SND-1887	Vegasteam device classes not part of NCM 9.4.	Drivers are updated now.

Table 4 Fixed problems in NCM 9.4.1.0 (page 5 of 5)

CQ or SR number	Problem summary	Description of fix
SND-1875	On Linux, the NCM installation causes FATAL ERROR messages in the debug logs when in fact there is no error and the installation is successful. The log contains the following: `Status: FATAL ERROR` Additional Notes: FATAL ERROR - class com.zerog.ia.customcode.util.miscutils.ThrowInstallError FatalInstallException: An error occurred while running the post-install script for the Database component. The stderr output is: Exception in thread "main" java.lang.ExceptionInInitializerError at javax.crypto.Cipher.getInstance(Cipher.java:510) at NCM.main(NCM.java:28) Caused by: java.lang.SecurityException: Can not initialize cryptographic mechanism	Code is updated to correct errors.
SND-1856/ CQ 654589	On Windows server, the dbutil schema fails to get created during installation, hence the db-utility tool will not work. Database utility fails to get JAVA_HOME on migrated environment, and displays this error: The system cannot find the path specified. no password supplied at database-utility.pl line 1243.	JAVA_HOME is now set properly.
SND-1532/ SND-1810	• On a Win2k12 R2 Standard edition server, the ncm-as service can not start. • If DNS for www.springframework.org is not resolved, then NCM does not function as expected due to the dependency on the host. The error logs report the following message: "springframework.org unreachable"	The code has been modified to make it work.

Table 5 lists the problems that have been fixed in EMC Smarts Network Configuration Manager 9.4.0.0.

Table 5 Fixed problems in NCM 9.4.0.0 (page 1 of 2)

CQ or SR number	Problem summary	Description of fix
IS-2288/ 67246500	CLONE - Running cmstatus (part of healthcheck) generates a bus error.	Ensured cmstatus binary is removed in AS only installation.
IS-2272/ 65903868	CLONE - ssl-utility.pl is throwing an error.	Fixed the error in ssl-utility script.
IS-2064	Transformation engine not working.	Transformer process heap size is increased from 512 to 1024 MB.
IS-2013	perl modules installed by rpm modules should not be just removed by the installer.	Changes done in uninstaller not to remove the perl modules.
IS-1962/ 66600940	CLONE - Postgres 9.0.7 Security Vulnerability.	NCM 9.4 database upgraded to Postgres 9.0.18.

Table 5 Fixed problems in NCM 9.4.0.0 (page 2 of 2)

CQ or SR number	Problem summary	Description of fix
IS-1822/ 65661118	CLONE - Compliance Audits duplicating on multiple DCS# revisions.	Code changes done to avoid the duplication.
IS-1805/ 65063306	CLONE - incorrect user name used in recurring job.	SCP Job credentials were not decrypted properly. Code fix.
IS-1746/ 66405142	The reporting tables contain a lot of data about devices not in the system anymore.	Fixed in database_utility.pl script.
CQ 654482 CQ 652422	Existing groups/users from NCM 4.1.1 and newly created user/group from NCM 9.2.2, 9.2.2.a, and 9.2.2.a Patch 1, will not have site permissions (create/delete site) if the group/user has default modify network permissions.	Upgrade fixed.
CQ 654358	When you schedule a recurring job, if an invalid date is provided, the job is submitted by converting the invalid date to a future date.	Scheduling feature fixed.
CQ 654115	The browser prompts for Java Runtime Environment every time while connecting to an NCM instance.	Fixed for 9.4
CQ 639884	db and dump directory do not have the correct user under /opt/smarts-ncm	Permissions fixed.
CQ 613854	The password you enter to encrypt the SSL Utility (ssl-utility.pl) keystore is displayed in clear text. In addition, the password is also visible in clear text in this file: /opt/smarts-ncm-93-AS/jboss/server/vc-server/ deploy/jbossweb.sar/server.xml. The server.xml is a Tomcat configuration file, which does not support encryption of the keystore password.	Utility fixed for 9.4

NCM Integration Adapter for Smarts Manager fixed problems

There are no issues fixed in NCM Integration Adapter for Smarts Manager.

Environment and system requirements

The *EMC Smarts Network Configuration Manager Support Matrix* provides information on prerequisites, software and hardware requirements, supported operating systems, required operating system patches, and product and version compatibility. The guide is available at EMC Online Support: https://support.emc.com.

Security recommendations

This section describes EMC security recommendations.

Secure data erasure

For Government customers, or any other customer requiring a heightened level of application and information security, EMC recommends that applications should utilize host-based erasure. Alternatively, if data is held on off-box storage, storage level erasure should be utilized.

Data-at-rest encryption

For Government customers, or any other customer requiring a heightened level of application and information security, EMC recommends that this product be installed onto a host that supports native encryption of DAS, or a storage environment that supports SAN or Array encryption of all storage volumes utilized. Installing and operating this EMC product on encrypted drives or encrypted storage adds a secondary level of security against malicious actions.

End of service dates and extended support

EMC has a standard software support duration policy which specifies that a major version will reach End of Service Life (EOSL) a minimum of 36 months following the General Availability (GA). EOSL may be followed by an Extended Support period during which customers may elect to pay an additional fee to extend their support coverage rather than migrate to a current software version.

Once a software product reaches EOSL, EMC Technical Support is no longer available under base support/maintenance agreements. Customers interested in uninterrupted support must upgrade to a current release or contract for Extended Support (ES).

EMC Online Support contains a list of documents that provide end-of-service and extended support information for EMC software and hardware products.

To access these documents on EMC Online Support, do the following:

1. Go to https://support.emc.com/products
2. Type the product name in the “Find a Product” field and click green right arrow.

   The Service Life information, if available for a given product, is displayed on the left side of the associated product page, and states when the product was Generally Available (GA), when it will be out of Service, and if it has Extended Service coverage.
3. Click the “Release and End of Life Dates” link available on the Service Life information section to view existing Service Life information documents. The “EMC Software Release and End of Service Life Notifications” document provides EOSL dates for EMC software products.

NOTICE

This policy is in effect for select releases and will be phased in as new versions are made available. In cases where a software release is not eligible for Extended Support, the previous policy terms, which specify product support and maintenance under Continuous Coverage Product Maintenance (CCPM), still apply.

For information on how to use EMC Online Support, click the “Online Support FAQ” link available at https://support.emc.com.

Known problems and limitations

The following known problems and limitations are included in this document. When applicable, a resolution for the issue is provided.

- "Known issues in Network Configuration Manager" on page 29
- "Known issues in SolutionPack for EMC Network Configuration Manager" on page 40
- "Known issues in NCM Integration Adapter for Smarts Manager" on page 41

Known issues in Network Configuration Manager

Network Configuration Manager 9.4.2.0 has the known problems and limitations listed in Table 6.

Table 6 Known problems and limitations in NCM 9.4.2.0 (page 1 of 2)

CQ, SR, or JIRA number	Issue	Resolution
SND-3904	Remote Device Server upgrade fails intermittently on Linux platform due to services not getting stopped properly.	Workaround: Before upgrading, 1. Kill all of the Device Server services using these commands: a. ps -aef | grep ‹service name› b. kill -9 ‹service name› DS services are: voyenced, syssyncd, evdispatch, autodiscd, commmgspatchr, cfgmgrd and zebedee. 2. Execute: service vcmaster stop After completing these steps, start the Device Server upgrade.
SND-3900, SND-3894	In a few setups, the change reports in RA do not have links to the running and startup configuration difference data in Chrome and Mozilla browsers. This is an inconsistent issue which happens in a few setups and it happens only in Google Chrome and Mozilla Firefox. Links work fine in Internet Explorer.	Use Internet Explorer. The similar data is also available in the Configuration Change Detail report which works fine in all of the browsers.
SND-3899, SND-3893	In a few Linux setups, while restarting the database service or logging into the database, the Permission Denied error is seen after the NCM upgrade.	This has no functionality impact and applies only to the NCM upgraded setups on the Linux platform. To avoid the warning message, execute the following command to change the permissions of initdb.i18n file: `chown pgdba:voyence <VOYENCE-HOME>/db /controldb/initdb.i18n` Now, log in to voyencdb or restart controldb, the Permission Denied error does not occur.

SND-3711	Windows only, running the installation program in silent mode fails for Report Advisor (RA). The failure generates the following error and does not create the web directory under the /Tomcat8 directory. The error message is:
	`ERROR: The system was unable to find the specified registry key or value.`
	`C:\temp\bundle.p12 : Invalid argument`
	`Error opening input file C:\temp\bundle.p12`
	
	`ERROR:Import_certs_into_RA — Error in importing certificate from pkcs - Password may be wrong at ReportsAdvisor.pl line 2402.`
		No workaround for Windows. Silent mode installation for RA works for Linux.

Table 6 Known problems and limitations in NCM 9.4.2.0 (page 2 of 2)

CQ, SR, or JIRA number	Issue	Resolution
SND-3798, SND-3739	For a Windows distributed setup, the NCM Smarts Adapter is not upgraded with NCM core software.	For a Windows distributed setup, after upgrading the NCM Core software, upgrade the NCM Smarts Adapter separately.

SND-3860	Errors are seen in server and powerup logs related to system account in an upgraded setup. After upgrading from NCM 9.4.1 to 9.4.2 in RHEL 6, logging in to the NCM console with administrator credentials (system/sysadmin) failed. The error message is:
	`2016-09-02 09:15:10,454 ERROR [com.powerup.configmgr.server.security.jmx.SecurityService] (tomcat-http--3) Error authenticating user system with session 7EF0CB3B2C880A291A26D58D6DE1DD60`
	`javax.security.auth.login.LoginException: loginExceptions.loginFailed`
	The Incorrect Password error for the system account occurs during the upgrade, because the password is no longer valid due to the Security Vulnerability fix. Also, since the RA upgrade happens at the end, Tomcat restarts several times.
		After the RA upgrade is completed at the end of an upgrade to 9.4.2, the errors no longer occur.

SND-3836	UI exception is seen when we try to unclassify the device that is not present in Infra database. The error message is: `UI Exception: java.lang.NullPointerException`	There is currently no resolution.

Network Configuration Manager 9.4.1.0 and 9.4 has the known problems and limitations listed in Table 7.

Table 7 Known problems and limitations in NCM 9.4.1.0 and 9.4 (page 1 of 10)

CQ, SR, or JIRA number	Issue	Resolution
SND-2757	The vcmaster service does not come up after machine reboot on Linux 7 platform.	Restart the services manually after the reboot.
SND-2739	Audit trails result status is "not audited" after enforcing second policy on "view.”	Select the static devices instead of Filter.
SND-2728	Report Advisor (RA) is blocked when you try to launch it from a host running the Windows 2012 operating system.	This issue occurs only with Internet Explorer. Use other browsers to avoid this problem. This is due to a security setting that does not recognize the self-signed certificates used when launching RA.
SND-2683	In the Windows version of NCM 9.4.1, Report Advisor (RA) does not come up after upgrading from 9.4 if C:\Tomcat8 folder is not empty before starting the upgrade.	If C:\Tomcat8 directory is not empty after uninstalling the Tomcat8 service, manually delete the contents of C:\Tomcat8 directory. Then restart the upgrade procedure for Report Advisor.
SND-2635 SND-1531	Uninstallation of NCM might leave some ports still in use, which then might interfere with a new installation.	Always run the prereq-check script before attempting an installation. The script detects and clearly provides information about ports still in use, which you can then release manually.

Table 7 Known problems and limitations in NCM 9.4.1.0 and 9.4 (page 2 of 10)

CQ, SR, or JIRA number	Issue	Resolution
SND-2566	The result of listall() operation in jmx-console is shown as html code format on Mozilla Firefox and Chrome.	This problem is related to the choice of browser. There is no functional impact. The workaround is to use Internet Explorer.
SND-2562	Auto Refresh of Device list is not happening after they are deleted from the workspace.	This issue occurs only in -ve use case where the permissions are not correctly assigned. The workaround is to manually refresh the workspace.
SND-2494	User will not be able to revert back to the default password from password-change.pl for jmx-user, smc-user and msa-user..	You cannot revert back to the default password after changing the password with the password-change.pl script. You must follow the security guidelines for creating new complex passwords.
SND-2435 SND-2467	NCM 941 application launch is breaking on Google Chrome.	Chrome has deprecated the NPAPI support which causes Java plugins to be disabled. If you have problems accessing Java applications using Chrome, Oracle recommends using Firefox, Internet Explorer, or Safari instead. https://blogs.oracle.com/java-platform-group/entry/java_web_start_in_or Users that need to run Web Start application may launch that application through a web browser such as Internet Explorer, Mozilla Firefox, Apple Safari, or Pale Moon. The link, https://<ipaddress>:8880/voyence/powerup.jnlp, provides a .jnlp file download you can use to enable the launch of the NCM application.
Issues reported in NCM 9.4		
SND-1011	Bottom scroll bar needs to be added in the reports.	This issue appears only on Chrome browsers.
SND-1180	After an NCM upgrade on a Windows server, the NCM debug log might contain error messages pertaining to registry key values and Class Not Found errors.	These errors do not affect functionality. You can consider the upgrade successful.
SND-1325	The install.sh does not check the RA version and allows re-installing RA if prereq-check is bypassed.	Do not bypass running prereq-check.
SND-1385	When logging into EMC Data Access API (EDAA) for Network Configuration Manager on a Windows server, the login is successful but the stdout file contains a RemoteAccessException error.	These errors do not affect functionality. You can consider the login successful.
SND-1421	When attempting to launch Report Advisor in Internet Explorer 10, the browser goes blank without any error message.	Manually add the host as a trusted site. Then RA launches successfully.
SND-1422	The EMC Data Access API (EDAA) for Network Configuration Manager does not launch in a Safari browser. You can not log in.	Use another browser.

Table 7 Known problems and limitations in NCM 9.4.1.0 and 9.4 (page 3 of 10)

CQ, SR, or JIRA number	Issue	Resolution
SND-1489/ SND-1682/ SND-1708 SND-2477	An upgrade can not retain the JMX password that was set in the previous version of the software. Issues related to the above are: • An upgrade from a previous version to NCM version 9.4.1 does not retain any customizations that were made to values in the system-config.xml file. • For all Create related APIs, the incorrect exception message is generated for an unauthenticated user. AuthenticationException should be thrown instead of TransactionRollBackException.	After the upgrade: • Reset the JMX password • Manually reapply any changes that were made in the system-config.xml file.
SND-1555	If an unsupported special character is used in the lockbox passcode, the lockbox cannot be unlocked.	Use only the following special characters in a lockbox passcode: • Tilde (~) • At (@) • Number (#) • Percent (%) • Exclamation (!)
SND-1556	The decrypt.pl utility omits a ^(caret) from the decrypted lockbox passcode.	Do not use the ^(caret) in a lockbox passcode. The following special characters are supported in a lockbox passcode: • Tilde (~) • At (@) • Number (#) • Percent (%) • Exclamation (!)
SND-1616/ CQ 654704	RSA device discovery fails with "RSA passcode calculation failed" error. Occasionally, RSA credentials PIN reset fails. While resetting a PIN, if wrong credentials are provided, and then if you wish to reset it with correct credentials, it fails.	This happens when wrong credentials are entered in the start - editted later. Do not edit the wrong RSA credentials; instead, delete the credentials and recreate them.
SND-1656	The user interface to the web application hangs when it is accessed too soon after all services are restarted.	Close the current window, and retry the access request. When the Tomcat process restarts, it takes some amount of time for the initialization and loading of the WebApp. The UI response is normal if you wait for the server initialization to complete before accessing the application.
SND-1676	An upgrade from a previous version to NCM 9.4 does not preserve the password for the EMC Data Access API (EDAA) for NCM. The upgrade reverts the password to the default value (`sysadmin`).	After the upgrade, manually change the EDAA password.
SND-1727	NCM SmartsAdapter log is not giving Fatal error when vc_smarts service was not created. A non-fatal error is logged.	Review the logs for ERROR: Failed to install VcSmarts Service
SND-1735	When the controldb service is down, the NCM login screen remains in the loading state without issuing any error messages.	If the login screen is unresponsive for some time, check if the controldb service is down. If the controldb service is down, start it, and restart the ncm-as service as well.

Table 7 Known problems and limitations in NCM 9.4.1.0 and 9.4 (page 4 of 10)

CQ, SR, or JIRA number	Issue	Resolution
SND-1739	In RA reports such as Policy Summary, Standard Summary, Job summary, Policy detail, Standard detail and so on, some drill down links that lead to other reports are not underlined.	No functionality is affected.
SND-1765	In certain configurations, the Console freezes while deleting devices from the network.	Use system commands to delete or kill the console process, and then start a new console.
SND-1785	After upgrading to NCM 9.4, LDAPS must be reconfigured.	After the upgrade to NCM 9.4: 1. Copy the keystore containing LDAPS certificates to the NCM-BASE/java/jre/lib/security directory. 2. Then restart the vcmaster services.
SND-1788	User name in dashboard is shown as 'UNKNOWN'	There is no impact on functionality. The workaround is to log out and log back in to see the user name.
SND-1805	When attempting to perform a cut-through with Telnet, if the Telnet Client feature is not enabled on the client machine, the NCM UI stays in the connecting state indefinitely.	Cancel the operation. Then enable the Telnet Client feature on the client machine (the machine you are using to access the NCM UI), and retry the cut-through operation. To enable the Telnet Client feature, navigate to **Start › Control Panel › Programs and Features ›Turn Windows Features On or Off,** and check T**elnet Client.** **Notice:** The enable step might be slightly different depending on the Windows version you are using.
SND-1807	On Windows servers, two different jre versions are installed with the Smarts Adapter.	No functionality is affected.
SND-1808	The msa instances listing fails on both Linux and Windows. The Type is listed but not the instances.	Try using a Chrome browser. The issue does not occur in that browser.
SND-1813	Network level operations, including Pull Config, Scheduling Config Pull, Pull Hardware Spec, Pull All, might cause the following exception messages: "No Row Identifier”	Ignore these exceptions. No functionality is affected.
SND-1831	On a Windows server, the installer allows installation of Smarts Adapter after an NCM complete installation.	No functionality is affected.
SND-1845	Fields in the .csv files exported through RA will be merged into one field if the contents in the field end with a double quote("). For example, if a report contains the following two field values: ncm "cisco-account" and the report is exported, in the .csv file the two fields will be concatenated to one field, leaving the other blank.	There is no workaround.
IS-4823	The readable_running-config file has been removed for Cisco Wireless LAN Controllers.	Workaround: The command, "show running-config," is no longer valid in the device. Instead, it is now an alias for "show run-config" Type "show run-config commands" to display the configuration commands. Press Enter to continue or ‹Ctrl-Z› to abort.

Table 7 Known problems and limitations in NCM 9.4.1.0 and 9.4 (page 5 of 10)

CQ, SR, or JIRA number	Issue	Resolution
IS-4733	Some index entries in the NCM Online Help system do not resolve properly, resulting in an HTTP 404 - File not found error.	Workaround: Use the Online Help system's built-in search to find the requested information. Alternatively, you can navigate to the requested information using the left pane table of contents navigation structure.
IS-3747 71111378	Discovery of a large number of devices causes device server restart.	There is no work-around available at this time.
CQ 654451	The ssl utility of NCM, while installing certificates prompts for a password. Although a space character is documented as being supported, the utility does not support a space characters in passwords.	Do not use spaces in your password.

CQ 654343	Performing a restore operation on a multi-platform backup results in a blank device configuration.	To workaround the problem:
		1. If a lockbox error appears, unlock the lockbox with the passphrase of the source system (where backup is taken).
		2. From [Product directory]/cgi-bin, run the following command
		`run cflist.cgi > cflist`
		3. Edit the cflist to point the POP entries to the correct DS (that is, edit the hostname).
		4. From [Product directory]/cgi-bin, run the following command
		`run cfwrite.cgi < cflist`
		5. Restart the vcmaster services.

CQ 654210	If the credentials that you try to import using the Bulk-import Utility ([Product directory]\tools\bulk-import\runCmd.pl) already exists, the following error message is displayed: `Could not create Credentials.`	The message is a misleading, and should have display: Could not import Credentials.
CQ 652908	Although NCM ships with the 64-bit JRE, if the 32-bit version of JRE is already installed on the machine where you are installing NCM, the installer continues to use the 32-bit version. The 32-bit JRE might negatively impact performance.	If you have installed a 32-bit version of JAVA, uninstall before installing NCM.
CQ 652396	Configuration Difference does not load in the EMC M&R frame.	This problem is caused because of an untrusted certificate. To workaround the problem: 1. Right click on the browser frame, and then view the frame source. 2. The frame source is displayed in a new tab. 3. A certificate error appears. 4. Choose to proceed anyway, or accept the certificate. 5. Return to the EMC M&R frame. 6. Right-click, and refresh or reload the frame. 7. The MSA login page appears.
CQ 652395	The reports in W4n which include external URL content like Configuration Difference or Audit Trail shows a blank page when no data is available instead of displaying a message similar to "This report does not select any data".	There is currently no resolution. This does not impact the functionality of NCM.

Table 7 Known problems and limitations in NCM 9.4.1.0 and 9.4 (page 6 of 10)

CQ, SR, or JIRA number	Issue	Resolution

CQ 651086	An incorrect NCM Server URL is displayed if you do not provide an EMC M&R configuration during install.
	An URL of this format is displayed:
	`http://<NCM_Server_IP_Address>:58080/APG/`
		To workaround the problem, manually update the file:
		1. [Product directory]/ncmcore/webapps/voyence/powerup.jnlp
		2. In the following, replace the ‹ › with the EMC M&R IP address:
		`<property name="jnlp.reports_advisor_url" value="_http://<   >:58080/APG/"/>`
		and
		1. [Product directory]/ui/html/index.html
		2. In the following, replace the ‹NCM_Server_IP_Address› with the EMC M&R IP address:
		`<a href="_http://<NCM_Server_IP_Address>:58080/APG/">Launch EMC Watch4Net</a><br />`

CQ 651072 CQ 650560 CQ 610513	The UpdateCredential utility fails to create the .csv file for a network if the following special characters are used in the network name: Windows: / \ : * ? " ‹ › | Linux: / The .csv file uses the same name as the network. These special characters are not supported in the file names of both Linux and Windows operating systems.	Do not use these special characters in the network name.
CQ 650862	If you have set active sync to ON, and if one of the Smarts domain managers goes down and comes back up, Smarts Adapter fails to sync properly and no notifications are propagated to Service Assurance Manager.	To workaround the problem, restart the NCMsmartsAdapter service.
CQ 649512	You will not be able to login to the user interface, if you perform an installation on a Linux machine using X Windows mode.	Restart the ncm-as service.
CQ 650738	If the Smarts Adapter web page is kept idle, a prompt is displayed: `Are you still there? Confirm to continue status monitor.` After you accept the confirmation, details in the Operation section are no longer displayed.	To workaround the problem, refresh the browser window.
CQ 644340	When the API updateView is used to change the name of the view, occasionally the network name gets appended to the view. This is observed only in the user interface, but the name in the database remains the same.	Refresh the view.
CQ 643867	During installation, if you copy and paste the database password, the password continues to be displayed in clear text, and is not converted to asterisks.	This problem occurs because of a limitation of the third-party software InstallAnywhere used for creating the NCM installers software packages.

Table 7 Known problems and limitations in NCM 9.4.1.0 and 9.4 (page 7 of 10)

CQ, SR, or JIRA number	Issue	Resolution
CQ 643594	The environment variables in the bash_profile are not configured when Tomcat starts and the web.properties file does not load. This results in Report advisor failure.	Manually set the environment variables using the command: `source $TOMCAT_HOME/.bash_profile` Restart Tomcat service.
CQ 643573	Operating system upgrade mechanism uses the Blowfish algorithm instead of AES encryption method for encrypting the SNMPv3 credentials.	There is currently no resolution.
CQ 641518	SNMPv3 credentials are not synchronized from NCM to IP and also from IP to NCM.	If devices are discovered in NCM or IP using SNMPv3 credential, they are not updated in IP or NCM, that is, SNMPv3 credential sync does not happen from NCM to IP and from IP to NCM. There is currently no resolution.
CQ 641421	NCM installation failed in a Cluster environment.	When installing Tomcat in a non-default user specified location, the Tomcat service does not start with "permission denied" error for the .bash_profile. To resolve this issue, ensure that the Apache Tomcat install location has the root:voyence permission. For example, if $TOMCAT_HOME is /home/xyz/tomcat/apache-tomcat-6.0.35, then the complete tree home, xyz, and tomcat should have root:voyence permission.
CQ 640148	Deleted devices when added back to the network were not shown in the Devices list for the same network.	This issue appears to be intermittent. There is currently no resolution.
CQ 640028	Unwanted voyence registry entries in Windows.	The registry entry HKEY_LOCAL_MACHINE\SOFTWARE\Voyence\Control\Configuration should be deleted manually before installing NCM again on the same server. The ideal step to do would be to delete all occurrences of NCM/VOYENCE from the registry (Keys, Values, and Data).
CQ 639916	In the Config Pull feature, the "Pull Selected" option fails to pull only the selected items after "SelectAll" is clicked and then if a few options are manually deselected. When the job starts running, all the deselected items are seen in running state in place of only selected.	Select the required items manually by checking the options individually instead of clicking "SelectAll" and then deselecting the items not needed.
CQ 639868	In NCM UI, the events in the Results tab of the Schedule Manager should be time stamped to measure the time taken for each event.	Each job scheduled should be measured for time taken and it should be logged in the Results tab. There is currently no resolution.
CQ 639672	Pull of interfaces through SSH failed for an Alcatel device. This was because the output of the command used to get the interface information was very long and the device session got timed out.	The openSSH version in the problematic device is OpenSSH_2.9p2 which needs to be upgraded to a higher version.
CQ 638618	Able to see the asterisk (*) when sorting is done by ipaddress in the device view.	The asterisk (*) can be seen even when the ordering is changed in other columns. The sorting is still done for the device_name column. This has no impact on the functionality. There is currently no resolution.

Table 7 Known problems and limitations in NCM 9.4.1.0 and 9.4 (page 8 of 10)

CQ, SR, or JIRA number	Issue	Resolution
CQ 638410	The "save to disk" option saves the reports in default path- [Product directory]/web/published-reports and that path is saved in DB. Post migration, the VOYENCE_HOME is changed from /opt/ionix-ncm to /opt/smarts-ncm. Hence the old path is no longer existent and the "savetodisk" to the default location fails.	Re-schedule such jobs.
CQ 636276 CQ 585435 SR 46471962	Voyence API Web Service responses do not adhere to the schema and specification requirements. Elements from extended complexTypes are not sequenced prior to elements in the complexType doing the extending.	There is currently no resolution.
CQ 615347	For devices where the configuration file size is more than 500MB, a pull operation of the file times out.	To workaround the problem, edit the corresponding device driver code, and increase the pull command TIMEOUT value to 1200sec, or higher.
CQ 609543 SR58136858	All new features and changes in a particular release are documented in the Release Notes document. The "what_is_new_in_this_release.htm" help file was removed to avoid duplicating the same content from the Release Notes. The spurious links will be removed from the HTML files in a later release of NCM.	This problem does not impact any functionality and can be ignored. There is currently no resolution.
CQ 608607 CQ 57799	The browser prompts for Java Runtime Environment every time while connecting to an NCM instance. This issue occurs if you install JRE 6 on top of JRE 7.	Uninstall JRE, and reinstall version 7.
CQ 588965 CQ 587005 SR 47232258	Apache 2.x was discovered to have multiple STIG findings.	There is currently no resolution.
CQ 588961 CQ 587481 SR 47053734	Cannot retrieve AttributeQueryInfo and AttributeTestInfo objects and subclasses of ALItemInfo, for example, ApiService.getAutomationLibraryItemsInAFolder(networkFolder,null) does not return any AttributeQueryInfo/AttributeTestInfo objects even though they are there.	The API does not support returning Attribute query information. There is currently no resolution.
CQ 567340 CQ 567211 SR 47354224	The communication mechanism is not being set correctly if once set incorrectly. In the autodisc logs, the mechanism was set as "Telnet" but later it gets ignored because as per the "Cisco IOS Router" Device class, "SSH" has higher priority as compared to "Telnet", for example, Jun 06 10:45:35 :-1297093728/10.6.226.2@1/telnet#2: DeviceObj::newDevice === Mechanism Set as Telnet	This issue appears only if you make SSH as the highest priority mechanism for a device where SSH is not enabled and discover the device with only SNMP credentials configured. There is currently no resolution.
CQ 561138 CQ 560850 SR 45263130	Attribute queries to gather hardware data cannot be run without System Administration rights.	The user needs sysadmin permission to get the results. There is currently no resolution.
CQ 554978	Following the recovery procedure for a device server results in duplicated POP and DEV lines for the related DS in the infra db. This results in duplicate DS in system administration and have an issue running jobs.	There is currently no resolution.

Table 7 Known problems and limitations in NCM 9.4.1.0 and 9.4 (page 9 of 10)

CQ, SR, or JIRA number	Issue	Resolution
CQ 552647 CQ 548079 SR 40042556	The SNMP Integration module did not send all DevicePolicyCheckFailedEvent traps if some policies were of the status error, not audited, or did not qualify.	There is currently no resolution.
CQ 548159	While viewing the configurations of devices from different networks, and selecting horizontal or vertical groups the window constantly flashed wrong primary tabs.	There is currently no resolution.
CQ 545901	When trying to install the NCM RSA Token Server, the NCMRSATokenService.exe encountered a problem.	The RSA password should be incorporated with alphanumeric characters.
CQ 532917	Incorrect error message when using Schedule Manager Auto-refresh When the Schedule Manager auto-refresh feature is enabled and properly working, and a network container pull job is scheduled and submitted without approval and then approved using the Schedule Manager, a Failed to retrieve all Actions associated with Task... error message displays.	Click OK on the message dialog to safely bypass and ignore this error message.
CQ 531135 CQ 528677	When pushing configurations to devices, the # character at the beginning of a line can cause Velocity to fail to parse the configuration since Velocity uses the # as syntax for many commands, such as #set, #if, #else, and #include.	To avoid Velocity parse failures when pushing configurations, # characters that are not part of a velocity statement can be escaped using one of the following. "/# "For example, /#‹config text› "## "For example, ##‹config text› "# followed by a space, and then the next character "For example, # ‹config text›
CQ 522479	A list of valid filter attributes was incorrect and valid filter attributes displayed errors, invalid filter attributes were accepted, and filter attributes returned no results.	There is currently no resolution.
CQ 521705	Unable to save a configuration unit to a file if the configuration unit name contains the : character.	The resolution for this issue is to confine the cuid attribute to path specifiers such as / and \ and providing identifying tag for associating content. Also, consider adding a display-name attribute for incorporating the colon.
CQ 481472	Connection to SSH Proxy Fails.	For an SSH Client to successfully connect with SSH Proxy on NCM, X11 forwarding should be disabled on the SSH Client.
CQ 481032	When using the Automation Library and left clicking on the Import button, the applications deadlocks intermittently. This is a Java bug. The following are the Java defect IDs you may want to use for tracking purposes. http://bugs.sun.com/view_bug.do?bug_id=6741890 http://bugs.sun.com/view_bug.do?bug_id=6789084 http://bugs.sun.com/view_bug.do?bug_id=6744953	This deadlock condition may occur in the application anytime a user opens a file dialog window.

Table 7 Known problems and limitations in NCM 9.4.1.0 and 9.4 (page 10 of 10)

CQ, SR, or JIRA number	Issue	Resolution
CQ 473887	Error: “Version Already Installed” message is displayed after a failed install or upgrade	The issue occurs when there is a lack of sufficient disk space, or when there is a loss of terminal session during installation or upgrade. When the “Version Already Installed” error message is displayed during installing, after a failed installation or upgrade, the following resolution can be used: **Installation resolution** When the "Version Already Installed" error is displayed uninstall and then re-install Network Configuration Manager. The steps for uninstall are provided in the *Network Configuration Manager Installation Guide.* If the uninstall fails to run, perform the following steps: 1. Stop all Network Configuration Manager services. 2. Remove the Network Configuration Manager installation directory. **Note:** Step 2 will delete all Network Configuration Manager data. 3. Remove the /etc/voyence.conf file. (Linux) 4. Ensure that the failure condition is fixed. (enough disk space, run session through screen or VNC) 5. Run the installation again. **Upgrade resolution** When the “Version Already Installed” error message is displayed during installation, after a failed upgrade, you can modify the current version number to allow the upgrade to continue. The following steps should only be used if Version Already Installed error message is displayed when the data migration has completed successfully, and the upgrade failed: • Change the current Network Configuration Manager build number. For example, if the build number is the last number in the version. Change it to one less than its initial value. For example, if the line reads "4.1.0.850", change it to "4.1.0.849". In Linux platforms: Edit the /etc/voyence.conf file and modify the VERSION line. In Windows platforms: Edit the registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Voyence\Control\Configuration\VERSION • Ensure that the failure condition is fixed (with enough disk space, run session through screen or VNC) • Run the installation again

Known issues in SolutionPack for EMC Network Configuration Manager

The SolutionPack for EMC Network Configuration Manager has the known problems and limitations listed in Table 8 on page 40.

Table 8 Known problems and limitations in SolutionPack for EMC Network Configuration Manager (page 1 of 2)

CQ or SR number	Issue	Resolution

CQ 654892
CQ 616656
	A few rows of data may be missing in the NCM SolutionPack Jobs Report, as the rows in the APG database are over-written.
	This problem occurs because the unique identifier for the individual rows for the Jobs query is over-written. For the queries *Jobs_Active and Jobs_History*, the unique identifier is:
	`properties="${property=source},${collecting-configuration-id},${property=device},${property=parttype},${property=part}"`
	As the data for these two queries is collected in an incremental manner, and the unique identifier is not unique, the previously collected incremental data gets over-written by the data collected later. Because the data is overwritten in the APG database, the records for Jobs Report are missing.
		Edit sql-collector-ncm.xml file as follows:
		Under
		`<main-collecting-configuration id="main_JobsActive">`
		tag , replace the
		`<raw-value-variable >` contents with the following :
		`<raw-value-variable separator="_" properties="${property=source},${collecting-configuration-id},${property=device},${property=parttype},${property=part},${property=acjobnum},${property=ajtsknum},${property=ajactid}" />`
		Under
		‹main-collecting-configuration id="main_JobsHistory"›
		tag , replace the
		`<raw-value-variable >` contents with the following:
		`<raw-value-variable separator="_" properties="${property=source},${collecting-configuration-id},${property=device},${property=parttype},${property=part},${property=hijobnum},${property=hjtsknum},${property=hjactid}" />`

CQ 652719 CQ 577913	A certificate error appears when connecting to Report Advisor from EMC M&R in the EMC M&R NCM SolutionPack.	For Firefox: 1. Open the Report Advisor in a separate tab. 2. Add the Report Advisor exception to the Firefox browser. 3. Launch Report Advisor in the EMC M&R SolutionPack. For Chrome: 1. Open the Report Advisor in a separate tab. 2. The SSL Error appears. Click Proceed anyway. 3. Launch Report Advisor in the EMC M&R SolutionPack. For Internet Explorer: Enable the browser to display blocked content. **Notice:** It is recommended to use Firefox as your browser for EMC M&R SolutionPack.

Table 8 Known problems and limitations in SolutionPack for EMC Network Configuration Manager (page 2 of 2)

CQ or SR number	Issue	Resolution
CQ 603841	The EMC M&R RemoteShellCollector that is used to collect system information for Application server, Device server, and Report server is not supported on Windows platform for this release. If Application server or Device server or Report server is running on Windows platform, the system information reports appear blank.	The support for Windows platform will be addressed in a future release.

Known issues in NCM Integration Adapter for Smarts Manager

Table 9 on page 41 lists the known problems and limitations in Network Configuration Manager Integration Adapter for Smarts Manager.

Table 9 Known problems and limitations in NCM Integration Adapter

CQ or SR number	Issue	Resolution
JIRA SND-1815	“NCM System Name” will become blank after clicking “Get Available Domain Managers” button.	Actually NCM System Name is automatically picked up in the backend and user need not provide it manually.

587796
585888
	When the NCM Integration Adapter gets devices from the IP Manager, the IP Manager provides the following device type for each device:
	`Device       Device Type`
	`Firewall---->Router`
	`FileServer---->Host`
	`Host---->Host`
	`LoadBalancer---->Router`
	`MediaGateway---->MediaGateway`
	`Node---->Other`
	`Router---->Router`
	`Switch---->Switch`
	As a result, filters configured based on device type do not work as expected.
		Use both exclusion filter and inclusion filter. Exclusion filter can be configured based on the IP range filter. Inclusion filter can be configured based on the device type filter. Exclusion filter takes more precedence than the inclusion filter.

Technical Notes for Network Configuration Manager

This release contains the following technical notes:

- “Policy Enforcement” on page 42
- “DB Maintenance plan” on page 43
- “Enabling default telnet client for cut-through” on page 44
- “UpdateCredential utility fails if certain special characters are used in network names” on page 44
- “Disabling “Configuration tab” in NCM UI under Global Search if you encounter system performance problems” on page 44
- “Java exception " java.net.UnknownHostException” on page 45

Policy Enforcement

CQ 654573

When you explicitly enforce a policy using the **Enforce Policy** option, it is not enforced on the live configuration of a device monitored by NCM. It acts on the latest configuration available in the NCM database.

Once a policy is enforced and you run the report, any subsequent enforcement of the same policy on the current device configuration results in the same output as the last unless changes are made to Policy/Standard/Test.

Recommendation

We recommend using explicit **Enforce Policy** on devices or network only if any changes are made to the associated Policy, Standard, Tests, or if you want to run it on relatively small set of devices.

If a policy is enabled on any device, network or site, the same policy will be enforced during a configuration pull job execution. This is the recommended method of policy enforcement.

With this you can check that the latest configuration coming in to NCM is compliant or non-compliant. In addition, the corresponding RA report will contain the latest compliance data.

As the policy enforcement is an computing expensive task, we recommend that you follow these guidelines:

1. Ensure that you have only required standards or tests associated with a policy.
2. Avoid having multiple polices enabled for the same network or site. If required, combine those standards and tests into a single policy.
3. If you have the same device in multiple sites, and the policy is enforced in all locations, then it would be an overhead for the system to run those policies. Ensure that you do not too many devices that fall into this category.
4. Allow policies to be enforced during scheduled config pulls rather than explicitly enforcing them through the GUI, unless it is required due to any change in the policy.
5. If you have many contracts trying to enforce a policy explicitly around the same time on a number of devices, then it might slow the system, and also increase the load on NCM. Consequently, policy enforcement will take a long time to complete.

You can control policy enforcement if you perform the activity using scheduled configuration pull jobs. This is because configuration pulls are usually set for different contracts at planned intervals. As soon as a configuration is pulled, NCM stores the new configuration and the enforces the defined policy. This is repeated device by device until all the devices in a job are completed.

DB Maintenance plan

CQ 654573

Use these notes as general guidelines for maintaining NCM database tables.

Archiving, Purging, and Pruning of events, jobs and revisions

A built-in utility script is available in the [Product directory]/tools/db-utility folder (database-utility.pl) using which you can Archive, Purge, and Prune database events, jobs, and revision data.

When jobs and revisions data grow, and you do not archive or prune them, UI operations and push or pull operations become intensive and the system performance is impacted.

Large events data negatively impacts UI performance in addition to making the ncm-as service slow to startup.

Recommendation

- For revisions—archive them; this ensures that the data still in the system
- For jobs and events—keep 30 days data in Voyence schema, 60 days data in archive schema, and prune the rest.

Periodic Maintenance using VACUUM FULL, REINDEX, ANALYZE

Once a week

- To assess the database growth, run the following SQL queries once a week and track the growth in size with respect to the whole DB and also with individual tables:
  - `SELECT * FROM CM_TOTAL_DB_SIZE;`
  - `SELECT * FROM CM_CALCULATE_TABLE_SIZES limit 20;`

    Query returns the top 20 tables in size.

    If the size of the database grows at rapid rate, run the above queries once a week, for period of 3-4 weeks, and compare the results to determine the tables with the fastest growth.

Once a month

- Run the following commands on the top 10 tables in size:
  - VACUUM FULL ‹Table Name›
  - REINDEX TABLE ‹Table Name›
  - ANALYZE (This commands runs on entire DB)

Once every two months

- Run the RA_Purge_Script.pl to clean up unwanted data in report tables, and run the VACUUM FULL, REINDEX, ANALYZE commands.

NOTICE

The effective alternative to VACUUM FULL on each individual table is to *take the backup image using backup.pl, and restore the backup using restore.pl*, which would clean up the VACUUM. After clean up, run the ANALYZE command on the entire database.

Enabling default telnet client for cut-through

CQ 616118

By default the property jnlp.use.client.default.telnet is set to true. Therefore, the client configured application is used to launch the telnet (cut-through window).

If you have not setup any application (like putty) for launching telnet (using the registry settings), the cut-through will not work. To set putty as the default telnet application, refer to the *EMC Smarts Network Configuration Manager Version 9.4 Installation Guide*.

If you do not have a preference, to launch the default java console for telnet, do the following:

1. Under [Product Directory]/ui/html

   Edit powerup.jnlp and modify the property: jnlp.use.client.default.telnet to false.

   ```
   <property name="jnlp.use.client.default.telnet" value="false"/>
   ```

2. Save the file.
3. From your client machine download the powerup.jnlp by entering the following to launch the client:

   https://‹server_IP›

UpdateCredential utility fails if certain special characters are used in network names

CQ 650560

The **UpdateCredential** utility fails to create the .csv file for a network if the following special characters are used in the network name – / \ : * ? " ‹ › |.

The .csv file uses the same name as the network. Since these special characters are not supported in file names of Linux and Windows operating systems, it is recommended to not use them in the name of a network.

Disabling “Configuration tab” in NCM UI under Global Search if you encounter system performance problems

CQ 653836, CQ 653799, CQ 653474

Follow these steps to disable the Configuration tab in NCM UI under Global Search:

1. Source the voyence.conf file

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

2. Edit system-config.xml

   ```
   vi [Product Directory]/
        ncmcore/webapps/ncm-webapp/WEB-INF/classes/system-config.xml
   ```

3. Modify the configitem

```
com.powerup.configmgr.server.services.network.impl.global_device_co
nfig_search_enable_tab
```

default Value to false.

NOTICE

By default this config item value is true.

```
<configItem>
<configType>config.server</configType>
<name>com.powerup.configmgr.server.services.network.impl.global_dev
ice
_config_search_enable_tab</name>
<editable>true</editable>
<defaultValue>false</defaultValue>
</configItem>
```

4. Restart the service

```
service ncm-as restart
```

Java exception " java.net.UnknownHostException

When the client is unable to resolve FQDN to IP address of the NCM server, the client logs an exception java.net.UnknownHostException to the uiClient.txt log file, resulting in login failure from NCM GUI. Verify this using the command ping ‹FQDN› from the client machine.

As a solution, use the correct DNS Server name for the client.

Documentation

Product documentation is available as a download from EMC Online Support at:

https://support.emc.com

An alternate way to access the product documentation is from the EMC Smarts Documentation Index available on the EMC Community Network (ECN).

https://community.emc.com/community/connect/smarts

NOTICE

User guides are not installed with the application except the *EMC Smarts Network Configuration Manager Online User Guide* and the *EMC Smarts Network Configuration Manager Application Program Interface (API) Javadoc Reference Guide*.

Starting from Network Configuration Manager Version 9.2.2, the prerequisites information has been moved from the *EMC Smarts Network Configuration Manager Installation Guide* to a new document named *EMC Smarts Network Configuration Manager Support Matrix*. This document contains the system and software requirements for NCM on Windows and Linux platforms.

The *EMC Smarts Network Configuration Manager Documentation Portfolio* is a single, downloadable, and searchable PDF document that contains the entire Network Configuration Manager documentation set and is available as a download from EMC Online Support.

- *EMC Smarts Network Configuration Manager Version 9.4.2 Documentation Portfolio*
- *EMC Smarts Network Configuration Manager Version 9.4 Application Program Interface (API) Javadoc Reference Guide*
- *EMC Smarts Network Configuration Manager Version 9.4.2 Release Notes*
- *EMC Smarts Network Configuration Manager Version 9.4.2 Installation Guide*
- *EMC Smarts Network Configuration Manager Version 9.4.2 Support Matrix*
- *EMC Smarts Network Configuration Manager DSr Support Matrix*
- *SolutionPack for EMC Network Configuration Manager Summary Sheet Article*
- *EMC Smarts Network Configuration Manager Version 9.4.2 Security Configuration Guide*
- *EMC Smarts Network Configuration Manager Device Driver Toolkit Version 9.2 Technical Notes*
- *EMC Smarts Network Configuration Manager Version 9.4.1 Advisors User Guide*
- *EMC Smarts Network Configuration Manager Version 9.2 Attributed Model User Guide*
- *EMC Smarts Network Configuration Manager Version 9.2 Device Access Scripting Language (DASL) Specifications Guide*
- *Smarts Network Configuration Manager EMC Data Access API (EDAA) Programmer Guide*
- *EMC Smarts Network Configuration Manager Application Program Interface (API) Programmer Guide*
- *EMC Smarts Network Configuration Manager Version 9.2 System Management Console Guide*
- *EMC Smarts Network Configuration Manager Version 9.2 Troubleshooting Guide*
- *EMC Smarts Network Configuration Manager Version 9.4 Online User Guide*

Electronic versions of the updated manuals are available on EMC Online Support at: https://support.emc.com.

Installation and Migration

The *EMC Smarts Network Configuration Manager Installation Guide* provides detailed information on installing NCM and all its components, upgrading from NCM 9.3.x, 9.4.0.x, or 9.4.1, post installation and configuration procedures, and backup and recovery procedures.

The *EMC Smarts Network Configuration Manager Migration Guide* describes procedures for migrating data from an existing NCM installation into a new installation on a new server. It includes procedures for migrating from NCM 4.1.x (excluding 4.1.0) to NCM 9.4.

Troubleshooting and getting help

EMC support, product, and licensing information can be obtained as follows.

Product information — For documentation, release notes, software updates, or for information about EMC products, go to EMC Online Support at:

https://support.emc.com

An alternate way to access the product documentation is from the EMC Smarts Documentation Index available on the EMC Community Network (ECN).

https://community.emc.com/community/connect/smarts

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

Published September, 2016

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided as is. EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date regulatory document for your product line, go to EMC Online Support (https://support.emc.com).