NetIQ Secure Configuration Manager 6.2 Release Notes

October 2016

Secure Configuration Manager 6.1 includes new features, improves usability, and resolves several previous issues.

Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure our products meet all your needs. You can post feedback in the Secure Configuration Manager forum, our community website that also includes product notifications, blogs, and product user groups.

For more information about Secure Configuration Manager, see the Secure Configuration Manager website.

For the latest version of this release notes, see the NetIQ Secure Configuration Manager 6.1 documentation website.

1 What’s New?

The following sections outline the key features and functions provided by this version, and issues resolved in this release.

1.1 Secure Configuration Manager Dashboard

The Dashboard is available with Secure Configuration Manager 6.1, which presents the security and compliance status of your IT environment in graphs and charts. The Dashboard is designed to allow users to view through this information on a web browser on a local computer. For more information about the Dashboard, see the *NetIQ Secure Configuration Manager Dashboard Release Notes*.

1.2 Java Upgrade

Secure Configuration Manager 6.1 includes Java 8 update 65, which includes fixes for several security vulnerabilities and also improves Secure Configuration Manager performance.

1.3 OpenSSL Upgrade

Secure Configuration Manager 6.1 includes OpenSSL 1.0.1p, which includes fixes for several security vulnerabilities. For more information, see the OpenSSL 1.0.1 Series Release Notes.

1.4 Security Checks and Policy Templates

Secure Configuration Manager 6.1 supports a number of new security checks and policy templates, and also enhances some existing security checks.

1.4.1 New Security Checks

Secure Configuration Manager 6.1 supports the following new security checks:

Shares with any Control by Specific User

This security check identifies the network shared assets that the user can access. (BUG 881013)

Fixed Role Members of a Database

This security check lists the fixed database role members for the specified database. (BUG 906474)

Top-Level Directories in all Drives

This security check lists the top-level directories and files present in all disk volumes of a computer. (BUG 928979)

Display the Amount of RAM on a Windows Server

This security check determines the amount of RAM available in the Windows server computer. (BUG 935459)

Installed Software by Parameter (Windows)

This security check lists the software currently installed on the Windows computer that are unauthorized and are not supposed to be installed.This prohibited list is obtained from the parameter of the check. (BUG 834044)

Entitlement for Files and Directories by OU Filter

This security check lists specified user or user group permissions for the specified files and directories. (BUG 880422)

Verify File Size

This security check verifies the size of the file. (BUG 919564)

1.4.2 Enhancements to Security Checks

Secure Configuration Manager 6.1 provides enhancements to the following security checks:

AD Accounts Not Logged in for X Days

This check now considers the `last Logon Time Stamp` date field, and hence does not report incorrectly when users who use editors such as the Active Directory Explorer run it. This check is now is renamed as the **AD Accounts Not Logged in by Timestamp for X Days** check. It looks for the last logon timestamp for the assessment. `(BUG 890917)`

User Rights with Exception Accounts

Result for this check now contains a new column, **Expected Values**, that displays the expected result value for the check. `(BUG 937681)`

1.4.3 New Policy Templates

Secure Configuration Manager 6.1 supports the following new policy templates:

- CIS Red Hat Enterprise Linux 5 Benchmark version 2.1.0
- CIS Red Hat Enterprise Linux 6 Benchmark versions 1.2.0 and 1.3.0
- CIS Red Hat Enterprise Linux 7 Benchmark version 1.0.0
- CIS Windows Server 2012 R2 Benchmark version 1.1.0
- CIS Windows Server 2008 R2 Benchmark version 2.1.0
- CIS SUSE Linux Enterprise Server 11 Benchmark 1.0.0

1.5 Time Zone Enhancements

Secure Configuration Manager 6.1 updates the way time zones are handled.

Previously, whenever you run a policy template, a security check, schedule a job, or perform any activity in the Secure Configuration Manager console, the time zone of the Secure Configuration Manager Core Service/Database was considered. This caused discrepancy if the Console and the Secure Configuration Manager Core Service/Database are not in the same time zone.

Secure Configuration Manager Console now uses the local time of the Console computer for any activity. All the time fields are populated with local time instead of Secure Configuration Manager Core Service/Database time.

To enable this, the following are implemented:

- Secure Configuration Manager Core Service / Database use Coordinated Universal Time (UTC) as the time zone by default.
- Secure Configuration Manager Console uses the local time zone of the Console computer. It converts all the time fields from the local time zone to UTC when performing an operation and also converts the fields from UTC to local time zone while displaying any data on the Console.

`(BUG 866343)`

1.6 Software Fixes

Secure Configuration Manager 6.1 includes software fixes that resolve several issues.

- Section 1.6.1, “Some Security Checks Fail in Windows 2008 and Later Versions,” on page 4
- Section 1.6.2, “Issues with Microsoft Excel Reports Distribution,” on page 4
- Section 1.6.3, “Secure Configuration Manager does not Forward Assessment Reports to SIEM Servers when Asset is in Compliance with Exception,” on page 5
- Section 1.6.4, “Cannot Install Secure Configuration Manager,” on page 5

1.6.1 Some Security Checks Fail in Windows 2008 and Later Versions

Issue: The following security checks fail in computers where Secure Configuration Manager is running on Windows 2008 or a later version:

- Application event log failure auditing
- Application event log success auditing
- Security event log failure auditing
- Security event log success auditing
- System event log failure auditing
- System event log success auditing

Secure Configuration Manager displays the following error when you try to run any of these security checks:

```
Object does not exist. System could not find file specified.
```

```
(BUG 883062)
```

Fix: You can now run these security checks successfully.

1.6.2 Issues with Microsoft Excel Reports Distribution

Issue: Microsoft Excel report distribution has the following issues:

- If multiple Microsoft Excel report distributions are running concurrently, only the first report is distributed correctly, and the rest of the report distributions are stopped.
- Sometimes, Secure Configuration Manager does not save Microsoft Excel reports because of network connectivity issues.

```
(BUG 965161)
```

Fix: Secure Configuration Manager 6.1 provides the following resolutions:

- Multiple Microsoft Excel report distributions are now handled correctly.
- You can now enable Secure Configuration Manager to save Microsoft Excel reports in a local directory in the interim while also saving them in a network location. If there is a network connectivity outage and reports are not saved in the network location, you can manually copy the

reports from the local directory to the network location. For more information, see "Enabling Interim Local Storage of Microsoft Excel Reports" in the *NetIQ Secure Configuration Manager User Guide*.

1.6.3 Secure Configuration Manager does not Forward Assessment Reports to SIEM Servers when Asset is in Compliance with Exception

Issue: When an asset is in compliance with an exception, Secure Configuration Manager does not forward the assessment reports to the Security Information and Event Management (SIEM) solution servers such as NetIQ Sentinel and Splunk. (BUG 967270)

Fix: Secure Configuration Manager now forwards the assessment reports to the SIEM servers correctly.

1.6.4 Cannot Install Secure Configuration Manager

Issue: Secure Configuration Manager installation fails in the following scenarios:

- When the drive chosen for remote database installation does not exist in the local server where you are installing the Secure Configuration Manager Core Services.
- In Microsoft SQL Server cluster environments.

The installation wizard displays the following error:

`Invalid Drive: <drive name>:\`

(BUG 924521, BUG 912780, and BUG 924367)

Fix: Now you can install Secure Configuration Manager in successfully in all the preceding scenarios.

1.6.5 Report Distribution Fails

Issue: Secure Configuration Manager does not create reports in XML and PDF formats for distribution. (BUG 923468)

Fix: Secure Configuration Manager now creates reports for distribution correctly.

1.6.6 Reporting Experience is not the Same for Different Users with the Same Role

Issue: Report generation and distribution options vary for different users with the same role. (BUG 944580)

Fix: Report generation and distribution options are the same for users with the same role.

1.6.7 Web Service API for Managed Systems does not Populate Core Services IP Address

Issue: The web service API for managed systems does not populate the IP address field with the IP address of the Core Services computer. (BUG 896774)

Fix: The web service API for managed systems populates the IP address field correctly.

1.6.8 Cannot Export Domain Keys Using the ExportDomainKeysx64.bat File

Issue: Secure Configuration Manager displays an error when you try to export domain keys using the `ExportDomainKeysx64.bat` file. This issue occurs because the file points to an older version of the jTDS JDBC driver. `(BUG 938466)`

Fix: The `ExportDomainKeysx64.bat` file now points to correct jTDS JDBC driver, and exports domain keys correctly.

1.6.9 Exported Data Views do not Have Headers

Issue: When you export the data in Microsoft Excel format, the exported data view does not contain a header. `(BUG 913134)`

Fix: Exported data views in now contain correct headers.

1.6.10 Secure Configuration Manager does not Display Version Information for Endpoints and Managed Groups

Issue: Secure Configuration Manager does not populate and display any data for the version information attributes such as `Major Version`, `Minor Version`, and `Version` for some endpoints and managed groups. `(BUG 890252 and BUG 906884)`

Fix: Secure Configuration Manager now displays correct data for version information attributes for all endpoints and managed groups.

1.6.11 Exceptions not Applied On Re-Run Of Jobs for Failed Endpoints

Issue: Secure Configuration Manager does not apply exceptions when you re-run a job for failed endpoint groups. `(BUG 891536)`

Fix: Secure Configuration Manager now applies correct exceptions when you re-run a job for failed endpoints.

1.6.12 Issues with the Major Version Attribute in Endpoint Properties

Issue: The `Major Version` attribute has the following issues:

- Cannot add Windows 2003 R2 as a major version. So, `Major Version` attribute displays NULL value when you try to manage a Windows Server 2003 R2 endpoint.
- Windows 2008 version is displayed as Windows Server 2008. This is not consistent with other major version attribute values, and hence causes problems in the sorting order.
- The `Major Version` attribute is populated with NULL value if the operating system of the endpoint is Windows Server 2012 R2.

`(BUG 926272, BUG 939119, and BUG 926269)`

Fix: The `Major Version` attribute is updated to display correct value for the preceding scenarios.

2 System Requirements

For information about hardware requirements, supported operating systems, and browsers, see the NetIQ Secure Configuration Manager Technical Information web page.

3 Installing or Upgrading to Secure Configuration Manager 6.1

To install Secure Configuration Manager 6.1, see the *NetIQ Secure Configuration Manager Installation Guide*.

You can upgrade to Secure Configuration Manager 6.1 from 5.9 or later versions. To upgrade to Secure Configuration Manager 6.1, see "Upgrading Secure Configuration Manager"in the *NetIQ Secure Configuration Manager Installation Guide*.

NetIQ recommends that you review the following considerations before upgrading to this version:

- If you want to deploy NetIQ Secure Configuration Manager Windows Agent version 6.1 to Windows agents already registered with Secure Configuration Manager, you must locally upgrade at least one agent in each domain. Secure Configuration Manager uses the first upgraded agent as a Deployment Agent for the domain. Once an agent is upgraded, Secure Configuration Manager can automatically assign it as a Deployment Agent. For more information about deployment and Deployment Agents, see the *NetIQ Secure Configuration Manager Windows Agent Installation and Configuration Guide* and the *NetIQ Secure Configuration Manager User Guide*.
- The setup program automatically adds a Windows agent to the Core Services computer, if no agent previously existed on the computer. If a Windows agent exists on the computer, the setup program upgrades the agent to NetIQ Security Agent for Windows 6.1. Secure Configuration Manager assigns this agent as the default Deployment Agent. During installation, you should ensure that the run-as account specified for the NetIQ Security Agent for Windows service has the credentials to deploy to remote computers. For example, specify a domain administrator account.
- If you want to immediately upgrade your Windows agents to version 6.1, you might need to re-register the agents before using the Deployment feature in the console. Secure Configuration Manager requires that the Properties window for each agent specifies a fully qualified host name (FQHN) for the agent computer. Secure Configuration Manager needs to know in which domain each agent resides so that Core Services can assign a Deployment Agent to use for deploying version 6.1 to the agents.

  However, if you upgrade your Windows agents more than 30 days after upgrading the Secure Configuration Manager infrastructure to version 6.1, you might not need to re-register your Windows agents. The Asset Details and Discovery job might collect the FQHN during a regularly scheduled run since this job enables Core Services to update agent and endpoint properties. You can also run this job manually from the Scheduled Jobs queue.
- When the upgraded agent registers with Core Services, the default communication port changes from 1626 to 1627. If you upgrade an agent that communicates with Core Services on a port other than the default ports, you must manually re-register the upgraded agent.
- The upgrade process removes all existing records from the Discovered Host table in the database. This means that the upgrade also removes all systems from the Discovered Systems content pane. After you successfully upgrade or install Secure Configuration Manager and register your agents, the Asset Details and Discovery job automatically adds application endpoints discovered on currently registered Windows and UNIX systems.

  To manually repopulate Discovered Systems with unmanaged systems, update the Discovery settings in the Core Services Configuration Utility, and then initiate the discovery process. For more information about discovery, see the Help and the *NetIQ Secure Configuration Manager User Guide*.

- If you want to discover systems in Active Directory, you must update the settings on the Discovery tab of the Core Services Configuration Utility.
- If you want to re-deploy an agent that has already been successfully deployed to a remote computer, you must uninstall the agent first. For example, you might want to change the credentials of the NetIQ Security Agent for Windows service or resolve issues with the agent. The Deployment wizard does not change the settings for a previously installed agent, even though you modify the settings as part of the deployment process. The Windows agent setup program prevents you from installing an agent when the same version already exists on the computer, but the Deployment wizard does not.

4 Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact Technical Support.

4.1 Cannot Upgrade Standalone AutoSync Client from Version 6.0 to 6.1

Issue: Upgrading the standalone AutoSync client 6.0 to version 6.1 fails. Though the installation completes when you run the installation setup program, the standalone AutoSync client does not upgrade to version 6.1. (BUG 971092)

Workaround: Uninstall standalone AutoSync client 6.0 and perform a fresh installation of standalone AutoSync client 6.1. If you have configured any specific settings for your standalone AutoSync client 6.0, you must reconfigure those settings manually, using the AutoSync Configuration Utility.

4.2 Cannot Create, Install, or View Security Certificates Using the sslkey.bat File

Issue: You cannot create, install, or view security certificates in your Core Services computer by running the sslkey tool. Secure Configuration Manager displays an error when you run the `sslkey.bat` file. (BUG 971532)

Workaround: You can use any third-party tool to create, install, or view security certificates.

4.3 Weekly and Daily Scheduled Jobs Do Not Save and Apply the Updated Recurrence Time Schedule

Issue: When you edit an existing weekly or daily scheduled job for recurrence time schedule and save it, Secure Configuration Manager does not save and apply the updated recurrence schedule. The next run date is not updated as per the updated recurrence schedule. (BUG 971902)

Workaround: Delete the scheduled job you intend to update and create a new schedule job with the same parameters but with the new, intended recurrence time schedule.

4.4 Endpoint Registration Fails After Regenerating Crypto Keys

Issue: While registering or reregistering an endpoint, if you regenerate the crypto key for SSH, the registration fails. This occurs because the key is not replaced in the `.ssh/known_hosts` file. (BUG 860552)

Workaround: Delete the `.ssh/known_hosts` file and register the endpoint again.

4.5 The Retry Option in SCM Installer Does Not Work on Windows 7 and Windows Server 2008 R2

Issue: When you try to uninstall an SCM application using the SCM installer on a computer that has Windows 7 or Windows Server 2008 R2, and if some files that belong to the application are in use, a **File in Use** dialog box is displayed. If you click **Retry** in that dialog box, ideally uninstallation should not continue and the error message should persist, but uninstallation resumes. (BUG 893069)

Workaround: Install the Microsoft KB 2649868.

4.6 Issues with Command Execute Check Output View

Issue: The Command Execute check output view in Secure Configuration Manager reports has the following issues:

- The output view is incomplete.
- The scroll bar function is not supported.

(BUG 852044)

Workaround: There is no workaround at this time.

5 Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

For detailed contact information, see the Support Contact Information Web site.

For general corporate and product information, see the NetIQ Corporate Web site.

For interactive conversations with your peers and NetIQ experts, become an active member of the Secure Configuration Manager forum, our community Web site that offers product forums, product notifications, blogs, and product user groups.

6 Legal Notice

For information about NetIQ legal notices, disclaimers, warranties, export and other use restrictions, U.S. Government restricted rights, patent policy, and FIPS compliance, see http://www.netiq.com/company/legal/.

For information about NetIQ trademarks, see http://www.netiq.com/company/legal/. All third-party trademarks are the property of their respective owners.