NetIQ Secure Configuration Manager 7.0 Release Notes

May 2017

Secure Configuration Manager 7.0 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 document, see the NetIQ Secure Configuration Manager 7.0 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 Java Upgrade

Secure Configuration Manager 7.0 includes Java 8 update 112, which includes fixes for several security vulnerabilities and also improves the performance.

1.2 Security Checks

Secure Configuration Manager 7.0 includes new security checks, and also enhances some existing security checks.

1.2.1 New Security Checks

Secure Configuration Manager 7.0 includes the following new security checks:

<placeholder>

1.2.2 Enhancements to Security Checks

Secure Configuration Manager 7.0 provides enhancements to the following security checks:

<placeholder>

1.3 Enhancements

Secure Configuration Manager 7.0 includes the following enhancements.

1.3.1 Enhanced Auditing Capabilities

Secure Configuration Manager now provides detailed auditing information for the following:

- When changes made in permissions of user roles
- When members are added and removed in user roles
- When email option is selected for report distribution, and email addresses are specified

Console users with the View Audit History permission can view these updates, such as what changes were made and which user has made the changes.

For more information about viewing the audit history log, see “Understanding Console User and Administrator Auditing” in the *NetIQ Secure Configuration Manager User Guide*.

`(Bug 888231, Bug 888230, and Bug 891479)`

1.3.2 Ability to Distribute Reports Only if the Score is Greater Than Zero

You can now configure Secure Configuration Manager to distribute reports only if the score is greater than zero. For more information, see “Enabling the Ability to Distribute Reports Only if the Score Is Greater Than Zero” in the *NetIQ Secure Configuration Manager User Guide*. `(Bug 883100)`

1.3.3 Managed Groups can Inherit Parent Group’s Exceptions

You can now enable managed groups to inherit its immediate parent group’s exceptions. For more information, see “Enabling Managed Groups to Inherit Parent Group’s Exceptions” in the *NetIQ Secure Configuration Manager User Guide*. `(Bug 969956)`

1.3.4 Users with NetIQ Exceptions Approval Manager Role Receive Notification Emails Whenever Exceptions are Created

If exception approval is enabled, Secure Configuration Manager now sends notification emails to the users with the NetIQ Exception Approval Manager role whenever exceptions are created. The user who has created the exception also get a notification email whenever there is a change in the approval status of the exception. For more information, see "Approving Exceptions" in the *NetIQ Secure Configuration Manager User Guide*. (Bug 887814)

1.3.5 Enhancement to Configure Scheduled Jobs Behavior when Core Services Restarts after a Downtime

You can configure scheduled jobs to not run immediately when the Core Services restarts after a downtime. This helps you to avoid too many jobs simultaneously running after Core Services starts.

For example, if the Core Services computer has stopped at 9 a.m. because of an outage and restarts at 10.30 a.m., and you have scheduled 25 jobs to run at 10 a.m., those jobs might run immediately after Core Services restarts.

To configure scheduled jobs to not run immediately after Core Services restarts following a downtime, see "Configuring Scheduled Jobs Behavior when Core Services Restarts after a Downtime" in the *NetIQ Secure Configuration Manager User Guide*.

1.4 Software Fixes

Secure Configuration Manager 7.0 includes software fixes that resolve several issues.

1.4.1 Incorrect Time Displayed in Reports

Issue: Delta reports and security check reports display incorrect time. (Bug 1005719)

Fix: Reports now display correct time.

1.4.2 Invalid XML Character No Longer Causes a Failed Policy Template Run

Issue: This release resolves an issue where a policy template run against Windows 2008R2 fails with following type of error:

```
An invalid XML character (Unicode: 0x8) was found in the element content of the document.
```

This issue occurred because the name of a group included a character that must be escaped in xml. For example, the group is `Texas/balanced`. Secure Configuration Manager could not parse the '`/b`' part of the name because the characters represent the backspace action in code. (Bug 1003189)

Fix: Secure Configuration Manager adds an escape character before '`/b`' to allow parsing of the xml file.

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 Secure Configuration Manager 7.0

To install Secure Configuration Manager 7.0, see the *NetIQ Secure Configuration Manager Installation Guide*.

4 Upgrading to Secure Configuration Manager 7.0

You can upgrade to Secure Configuration Manager 7.0 from <TBD> or later versions.

For more information, 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:

- To deploy NetIQ Secure Configuration Manager Windows Agent (Windows agent) version 7.0 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 version 7.0. 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.
- To immediately upgrade your Windows agents to version 7.0, 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 7.0 to the agents.

  However, if you upgrade your Windows agents more than 30 days after upgrading the Secure Configuration Manager infrastructure to version 7.0, 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*.

- 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.

5 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.

5.1 Exporting Full Delta Reports to Microsoft Excel Format Fails

Issue: Secure Configuration Manager does not export full delta reports to Microsoft Excel format. `(Bug 1001599)`

Workaround: You can export delta reports in any other file formats such as `.pdf`, `.tsv`, `.rtf`, or `.xml`.

5.2 Problem with Clicking the Back Button While Upgrading in Distributed Setup

Issue: While upgrading Secure Configuration Manager to version 7.0 in the distributed setup in a computer where Core Services and the console are installed, the installation wizard displays incorrect screens if you click **Back** after the License Agreement screen. `(Bug 994646)`

Workaround: Cancel the upgrade process by closing the wizard, and start upgrading again.

5.3 Installation Fails on Computers that have Microsoft .Net Framework Version 4.5 Installed and Microsoft .Net Framework Version 3.5 is Not Enabled

Issue: If the computer on which you are installing contains Microsoft .NET framework version 4.5 and Microsoft .NET framework version 3.5 is not enabled, Secure Configuration Manager installation fails. (Bug 921158)

Workaround: Perform the steps specified in NetIQ Knowledgebase Article 7017878 before installing Secure Configuration Manager.

5.4 Cannot Upgrade Standalone AutoSync Client from Version 6.0

Issue: Upgrading the standalone AutoSync client 6.0 to this version fails. Although the installation completes when you run the installation setup program, the standalone AutoSync client does not upgrade to version 7.0. (Bug 971092)

Workaround: Uninstall standalone AutoSync client 6.0 and perform a fresh installation of standalone AutoSync client 7.0. 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.

5.5 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.

5.6 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.

5.7 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.

5.8 Retry Option in the Installation Program Does Not Work on Windows 7 and Windows Server 2008 R2

Issue: When you try to uninstall a Secure Configuration Manager component using the installation program on a computer that has Windows 7 or Windows Server 2008 R2, and if some files that belong to the component are in use, the installation program displays a **File in Use** dialog box. 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.

5.9 Issues with Check Output View when the Data is High

Issue: The check output view in Secure Configuration Manager reports has the following issues when the amount of the data is high:

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

(Bug 852044)

Workaround: There is no workaround at this time.

6 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.

7 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/.

Copyright © 2016 NetIQ Corporation. All Rights Reserved.

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