Secure Configuration Manager Windows Agent 7.0 Release Notes

February 2018

Secure Configuration Manager Windows Agent 7.0 (Windows Agent 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 inputs. 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 Web site that also includes product notifications, blogs, and product user groups.

For more information about this release and for the latest release notes document, see the Secure Configuration Manager 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 Updates to Managed Endpoints

Windows Agent 7.0 can manage several new endpoints, but some endpoint platforms have been deprecated.

For more information, see the *Secure Configuration Manager Windows Agent Installation and Configuration Guide*.

1.1.1 New Endpoints

Windows Agent 7.0 adds support for managing the following Microsoft platforms:

- Active Directory on Windows Server 2016
- IIS 10.0
- SQL Server 2016
- Windows 10
- Windows 8.1
- Windows Server 2016

1.1.2 Endpoints No Longer Supported

Windows Agent 7.0 cannot manage the following endpoints:

- Active Directory on Windows Server 2008
- Active Directory on Windows Server 2012
- Oracle 9i
- Windows 7
- Windows Server 2012
- Windows Server 2008
- Windows Vista

To continue managing these endpoints in your environment, ensure that you keep at least one older version of the Windows agent. Secure Configuration Manager 7.0 supports the following Windows agent versions:

- 7.0
- 6.2
- 6.1

2 System Requirements

Windows Agent 7.0 requires Secure Configuration Manager 7.0.

For information about hardware requirements, supported operating systems, and browsers, see the *Secure Configuration Manager Windows Agent Installation and Configuration Guide* and the Secure Configuration Manager Technical Information web page.

3 Installing or Upgrading to This Release

You can upgrade to this version from Secure Configuration Manager Windows Agent 5.9.1 or later.

Before installing or upgrading, consider the following issues:

- To install or upgrade the agent on remote computers, use the deployment wizard in the Secure Configuration Manager console. Before using the remote deployment feature, you must locally install or upgrade at least one agent in each domain. Secure Configuration Manager uses this first upgraded agent as a Deployment Agent for the domain. After you upgrade an agent, Secure Configuration Manager can automatically assign it as a Deployment Agent. For more information about deployment and Deployment Agents, see the *Secure Configuration Manager Windows Agent Installation and Configuration Guide* and the *User's Guide to Secure Configuration Manager*.
- When you install Secure Configuration Manager, the setup program automatically adds a Windows agent to the Core Services computer. If a Windows agent already exists on the computer, the setup program upgrades the agent in it. Secure Configuration Manager also makes this agent the default Deployment Agent for the computer's domain.
- To install or upgrade an agent on a local computer, use the `NetIQSecurityAgentForWindows.msi` setup program included in the installation kit.

NOTE: You can upgrade an agent to version 6.2 on a local computer only by using the command line. For more information, see "Using the Command Line to Install" in the *Secure Configuration Manager Windows Agent Installation and Configuration Guide*.

- Before using the Deployment feature in the console to upgrade older agents, you might need to specify 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 this version to the agents.
- During installation and deployment, the installation program makes the following changes on the target computer:
  - Automatically grants the “Log on as a service” right to the specified account for the Windows agent service.
  - Enables the Services utility in the Windows Control Panel to automatically restart the Windows agent service after a failure.
- To use an upgraded agent as a Deployment Agent, you might need to modify the run-as account for the NetIQ Security Agent for Windows service on that agent's computer. The service account for Deployment Agents must have the credentials to deploy to remote computers. For example, specify a domain administrator account. When you upgrade a Windows agent, the setup program persists the agent settings, including baselines and registry key settings.
- If you upgrade an agent that communicates with Core Services on a port other than the default port, you must manually re-register the upgraded agent. When the upgraded agent registers with Secure Configuration Manager Core Services, the default communication port changes from 1626 to 1627.
- You can upgrade a Windows agent that has the NetIQ SCAP Module For Windows Agent (SCAP agent) installed on the agent computer.
- 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 Windows agent 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.

For more information about installing or upgrading, see the *Secure Configuration Manager Windows Agent Installation and Configuration Guide*.

3.1 Verifying the Windows Agent Installation

To verify that the Windows agent installation was successful, on the computer where you installed the Windows agent, open the Control Panel utility for adding and removing programs. The currently installed programs should include **NetIQ Security Agent for Windows 7**.

4 Known Issues

There are no known issues in this release.

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 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.