

NetIQ Secure Configuration Manager 6.2 Windows Agent Release Notes

October 2016



Secure Configuration Manager 6.1 Windows Agent (Windows Agent 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 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, see the [Secure Configuration Manager Documentation](#) website. To download this product, see the [NetIQ Secure Configuration Manager](#) website.

- ♦ [Section 1, "Software Fixes," on page 1](#)
- ♦ [Section 2, "System Requirements," on page 1](#)
- ♦ [Section 3, "Installing or Upgrading to Secure Configuration Manager 6.1 Windows Agent," on page 2](#)
- ♦ [Section 4, "Known Issues," on page 3](#)
- ♦ [Section 5, "Contact Information," on page 3](#)
- ♦ [Section 6, "Legal Notice," on page 3](#)

1 Software Fixes

Secure Configuration Manager 6.1 Windows Agent includes the following software fix.

1.1 Secure Configuration Manager Does Not Report Some Service Startup Types in Windows 2012 R2

Issue: Secure Configuration Manager fails to report the following service startup types:

- ♦ Manual (Triggered start)
- ♦ Automatic (Delayed start)
- ♦ Automatic (Triggered start)

This issue occurs because these are the new service startup types introduced in Windows 2012 R2, and therefore were not previously covered. (BUG 898055)

Fix: Windows Agent now monitors these new service startup types, and hence Secure Configuration Manager reports them correctly.

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 Windows Agent

To install Secure Configuration Manager 6.1 Windows Agent, see the [NetIQ Secure Configuration Manager Windows Agent Installation and Configuration Guide](#).

You can upgrade to Secure Configuration Manager 6.1 Windows Agent from Secure Configuration Manager Windows Agent 5.9 or later. To upgrade to Secure Configuration Manager Windows Agent 6.1, see [NetIQ Secure Configuration Manager Windows Agent Installation and Configuration Guide](#).

IMPORTANT: You can upgrade Secure Configuration Manager 6.0 Windows Agent to version 6.1 only by using the command line. For more information, see “Using the Command Line to Install” in the [NetIQ Secure Configuration Manager Windows Agent Installation and Configuration Guide](#).

Before installing or upgrading to this version, consider the following:

- ♦ If you want to install or upgrade an agent on a local computer, use the `NetIQSecurityAgentForWindows.msi` setup program included in the installation kit.
- ♦ If you want 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 [NetIQ Secure Configuration Manager Windows Agent Installation and Configuration Guide](#) and the [NetIQ Secure Configuration Manager User Guide](#).
- ♦ The Secure Configuration Manager 6.1 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. Secure Configuration Manager also makes this agent the default Deployment Agent for the computer's domain.
- ♦ 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 version 6.1 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.
- ♦ If you want 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 Secure Configuration Manager Module for SCAP (SCAP module) installed on the agent computer.
- ♦ 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 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.

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 6.1**.

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/>.

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.