NetIQ® Aegis™ Adapter for NetIQ Secure Configuration Manager®

Configuration Guide

September 2011

Contents

This document provides information about installing and configuring the NetIQ Aegis Adapter for NetIQ Secure Configuration Manager. This document also covers how to verify a successful installation.

Legal Notice

Overview

The NetIQ Aegis Adapter for NetIQ Secure Configuration Manager (Secure Configuration Manager adapter) allows Aegis to communicate with a Secure Configuration Manager Core Services computer to:

- Determine which policy templates to run
- Run policy templates, or re-run for failed endpoints
- Review summarized and detailed endpoint compliance results based on security check and policy template runs
- Create, modify, approve, and deny endpoint exceptions

The Secure Configuration Manager adapter includes a library of workflow activities specific to Secure Configuration Manager that Process Authors can use in the Workflow Designer. For more information about activities or activity libraries, see the *Process Authoring Guide for NetIQ Aegis*.

Product Requirements

The Secure Configuration Manager adapter requires the following software versions:

- Secure Configuration Manager 5.8 Service Pack 2
- Aegis 2.2

The Secure Configuration Manager adapter can be installed on a computer running one of the following operating systems:

- Windows Server 2003 (32-bit)
- Windows Server 2008 (32- and 64-bit)
- Windows Server 2008 R2 (64-bit)

For more information about supported operating systems in clustered and non-clustered environments, see the *Administrator Guide for NetIQ Aegis*.

Implementation Overview

The following table provides an overview of tasks to install and configure the Secure Configuration Manager adapter.

	Steps	For more information, see…
☐	1. Enable Secure Configuration Manager to communicate with Aegis.	"Preparing Secure Configuration Manager" on page 2
☐	2. Install the Secure Configuration Manager adapter.	"Installing the Secure Configuration Manager Adapter" on page 2
☐	3. Configure the adapter to connect to additional Core Services computers.	"Adding Core Services Computers" on page 4
☐	4. Verify the installation was successful.	"Verifying a Successful Installation" on page 4

Preparing Secure Configuration Manager

Before you install the Secure Configuration Manager adapter, you must set up a user account and enable Web Services in Secure Configuration Manager.

Setting up an Aegis Account in Secure Configuration Manager

You must create a user account for Aegis in the Secure Configuration Manager console with the following rights and privileges:

- Administrator privileges
- Administrator role

This user account allows the adapter to communicate with Secure Configuration Manager Core Services and run the activities in a workflow. When you install the Secure Configuration Manager adapter, you must specify the credentials for this user account.

Enabling Web Services

Secure Configuration Manager Web Services allow communication between the Core Services computer and client computers. On the Web Services tab of the Secure Configuration Manager Core Services Configuration Utility, set Enable Web Service to **true**.

Installing the Secure Configuration Manager Adapter

You must install the Secure Configuration Manager adapter on the Aegis Server computer. For more information about installing Aegis, see the *Administrator Guide for NetIQ Aegis*.

If your Aegis Server computer is part of a cluster, you must install the adapter on the active node first, and then on each passive node. The NetIQ Aegis Adapter for Secure Configuration Manager setup program detects whether you are installing in a cluster and installs the adapter according to your environment.

Installing on an Active Node in a Cluster or on a Non-clustered Computer

These steps guide you through the process of installing the Secure Configuration Manager adapter on one of the following:

- The active node of a cluster
- A single non-clustered computer

To install the Secure Configuration Manager adapter on the Aegis Server computer:

1. Log on to the Aegis Server computer with a local administrator account.
2. Run the setup program from the folder where you downloaded the NetIQ Aegis Adapter for Secure Configuration Manager.
3. Click **Next**.
4. Accept the license agreement, and then click **Next**.
5. Specify the logon credentials for the Aegis service account, and then click **Next**. If you do not know the logon credentials for the Aegis service account, contact your Aegis administrator.

6. On the NetIQ Secure Configuration Manager Connection Information page of the installation wizard, provide the following information:

   - **Server Name/IP Address.** Specify the full server name or IP address of the Secure Configuration Manager Core Services computer to connect to the adapter, such as `houvc01.netiq.com`. If you do not know the name or address, contact your Secure Configuration Manager administrator. You can configure additional Core Services computers using the Aegis Adapter Configuration Utility. For more information about adding Core Services, see "Verifying a Successful Installation" on page 4.
   - **Port.** Specify the TCP port to communicate with Core Services computers. By default, the Secure Configuration Manager adapter uses port 8044, which is also the default port for Secure Configuration Manager Web Services. For more information, see "Enabling Web Services" on page 2.
   - **Connection Protocol.** Specify whether the Secure Configuration Manager Core Services computer uses http or https protocol to communicate with Aegis.

     Note
     This setting must match the protocol specified in the Secure Configuration Manager Core Services Configuration Utility.

   - **User Name.** Specify the user name for a valid Secure Configuration Manager account with Administrative privilege and Administrator role, which grant access to Core Services. If you do not know the logon credentials for the account, contact your Secure Configuration Manager administrator. For more information, "Setting up an Aegis Account in Secure Configuration Manager" on page 2.
   - **Password.** Specify the password associated with the specified User Name.

7. Click **Next**.
8. Follow the remaining instructions in the NetIQ Aegis Adapter for Secure Configuration Manager Setup wizard, and then click **Finish**.
9. Restart the Aegis Configuration Console after the installation process completes.

Installing on a Passive Node in a Cluster

These steps guide you through the process of installing the Secure Configuration Manager adapter on a passive node in a cluster. You must install the adapter on the active node of the cluster first.

To install the Secure Configuration Manager adapter on a passive node in a cluster:

1. Log on to the passive Aegis Server node with a local administrator account.
2. Open a command prompt for the folder where you downloaded the NetIQ Aegis Adapter for Secure Configuration Manager.
3. Type the following command:

   ```
   msiexec /i SCMAegisAdapter.msi /l*V SCMAegisAdapter.log SKIPCONFIG="TRUE"
   ```

4. Follow the instructions in the setup program until you finish installing the Secure Configuration Manager adapter, and then click **Finish**.

Adding Core Services Computers

When the installation is complete, the Aegis Adapter Configuration Utility allows you to configure Aegis to communicate with additional Core Services computers at any time.

To configure an additional Core Services computer:

1. Log on to the Aegis Server computer with a local administrator account.
2. In the NetIQ program group, click **Aegis > NetIQ Aegis Adapter Configuration Utility**.
3. In the left pane, click **Secure Configuration Manager**.
4. On the Edit menu, click **New Entry**.
5. Provide the appropriate information, and then click **Test Connection**.
6. ***If the Authentication account does not have connection privileges***, in the Secure Configuration Manager console, create a valid account for the adapter to access the specified Core Services.
7. Click **Exit**.
8. Restart the NetIQ Aegis Namespace Provider service.

Verifying a Successful Installation

You can verify a successful installation of the Secure Configuration Manager adapter in the following ways:

- Verifying the data source
- Verifying the pre-defined triggering event definitions

After verifying a successful installation, NetIQ recommends you build a simple workflow with one of the activities in the Secure Configuration Manager Adapter Library. For more information about building workflows, see the *Process Authoring Guide for NetIQ Aegis*.

Verify the Data Source

Aegis connects to the Secure Configuration Manager Core Services computer you specified during installation as a data source and all related computers as resources.

To verify a successful adapter installation:

1. Start the Aegis Configuration Console.

   For more information about starting the Configuration Console, see the *Administrator Guide for NetIQ Aegis*.
2. In the Navigation pane, click **Resources**.
3. In the left pane, expand **Adapter Resource Hierarchies > Secure Configuration Manager Adapter**.
4. Expand the Core Services computer you specified during installation and ensure its associated data resources, such as the assets in the My Groups folder, display in the left pane.
5. Click a resource folder and ensure its associated resources display in the Adapter Resources pane.

Verify the Pre-Defined Triggering Event Definitions

The adapter setup program installs Secure Configuration Manager event types you can use to create triggers and triggering event definitions. The adapter includes the following pre-defined triggering event definitions:

- Secure Configuration Manager.Compliance Change Event
- Secure Configuration Manager.Compliance Event
- Secure Configuration Manager.Job Status Event

To verify successful addition of the triggering event definitions:

1. Start the Aegis Configuration Console.

   For more information about starting the Configuration Console, see the *Administrator Guide for NetIQ Aegis*.

2. In the Navigation pane, click **Administration**.
3. In the left pane, click **Triggering Event Definitions**.
4. In the Event Definitions View Tasks list, click **Create New Event Definition**.
5. On the Create Triggering Event Definition window, click **<event type>**.
6. Verify the Triggering Event Definitions pane displays the pre-defined Secure Configuration Manager triggering event definitions.

After verifying a successful adapter installation, build a simple workflow with one of the activities in the NetIQ Secure Configuration Manager activity library. For more information about building workflows, see the *Process Authoring Guide for NetIQ Aegis*.

Understanding Activities

The activities in the Secure Configuration Manager Adapter Library allow you to manage Secure Configuration Manager agents and endpoints and to gather data through Aegis workflows. For detailed information about each activity, see its related Help.

The following table provides a general description of activities you can use to interact with Secure Configuration Manager. For a complete list of activities, see the Secure Configuration Manager Adapter Library.

Activity	Allow you to...
Approve/Deny Exception	Approve or deny an exception request for a security check or policy template report.
Copy Policy Template	Create a new policy template by duplicating an existing one.
Create Data Exception	Create exceptions for a policy template, security check, or endpoint.
Create Endpoint Exception	Create exceptions for endpoints applying to all or specific security checks and policy templates.
Export Report to File	Save a security check or policy template report to a file in a variety of formats.
Extend Exception	Change the date when Secure Configuration Manager stops applying an exception to a security check or endpoint.
Find Violations	Determine which endpoints failed which security checks in a policy template.

Activity	Allow you to...
Get Endpoint Compliance Status	Determine the compliance status of endpoints based on a security check or policy template.
Get Policy Template Knowledge	Determine whether a policy template is useful by reviewing its detailed description, including a list of the security check instances in the template.
Get Report Summary	Review summarized results of a security check or policy template run.
Get Security Check Knowledge	Determine whether a security check is useful by reviewing its description, explanation, risks, and remedies.
Get Security Check Results Detail	Review and filter the detailed report for a security check run.
Run Job Again	Re-run a security check or policy template, particularly for failed endpoints.
Run Policy Template	Run a policy template, either from the Secure Configuration Manager database or by gathering current data from endpoints.

Uninstalling the Secure Configuration Manager Adapter

You can uninstall the Secure Configuration Manager adapter using one of the following methods:

- Run the setup program from the folder where you downloaded the current version of the Secure Configuration Manager adapter.
- In Add/Remove Programs, select NetIQ Aegis Adapter for Secure Configuration Manager.

Do not attempt to use the Aegis setup program to uninstall the Secure Configuration Manager adapter.