Aegis Adapter for Sentinel

Configuration Guide

April 2016

This document describes how to install and configure the Aegis Adapter for Sentinel.

Contents

Legal Notice

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

Overview

The Aegis Adapter for Sentinel (Sentinel adapter) allows Aegis to communicate with Sentinel to:

- Receive alerts and initiate work items. If an alert received from Sentinel matches a trigger associated with a workflow, Aegis initiates a work item.
- Call and initiate Sentinel actions through the Sentinel REST Application Programming Interface (API). For more information about the Sentinel REST API, see http://www.novell.com/developer/plugin-sdk/ref/restapi/7.0/#DataObject_REST_API.

The Sentinel adapter also includes Aegis workflow activities specific to Sentinel that Process Authors can use in the Workflow Designer.

For more information about activities or activity libraries, see the *Process Authoring Guide for Aegis*.

Sentinel Adapter Requirements

The Sentinel adapter requires the following software versions.

Component	Version
Sentinel	Version 7.4.0.0 or later. Install on a computer with network access to the computer where you want to install the Sentinel adapter. Ensure you install the latest hotfixes and patches for the version you are using in your environment.
Aegis	One of the following versions installed on a computer with network access to the Sentinel adapter and the NetIQ Resource Management Namespace Provider: • 3.0, with the following hotfixes installed: • 7015363 • 7015389 • 3.1, with the following hotfixes installed: • 7015364 • 7015709 • 3.2, with the following hotfixes installed: • 7015365 • 7015648

Ports

The Sentinel adapter uses port 8443 on the Sentinel server computer to communicate with Aegis.

Installation Overview

The following table provides an overview of tasks to install and configure the Sentinel adapter.

	Steps	For more information, see…
☐	1. Configure the minimum rights and privileges for the Run As account.	"Ensuring Minimum Rights and Privileges" on page 4
☐	2. Install the Sentinel adapter.	"Installing the Sentinel Adapter" on page 4
☐	3. Configure the adapter to connect to additional Sentinel servers.	"Configuring a Sentinel Server" on page 4
☐	4. Verify the installation was successful.	"Verifying a Successful Installation with Aegis" on page 5

Ensuring Minimum Rights and Privileges

When you install the Sentinel adapter, you must specify an account that has the following minimum privileges in Sentinel:

- Manage All Alerts
- Any of the following:
  - Create Incident
  - Modify Incident
  - Manage Incident (All)

The logon account allows the Sentinel adapter to communicate with the specified Sentinel server.

Installing the Sentinel Adapter

You must install the Sentinel adapter on a non-clustered Aegis Server computer. You cannot install the adapter remotely.

1 Log on to the Aegis Server computer with a local administrator account.

2 Run the Aegis Adapter for Sentinel setup program (`AegisAdapterforSentinel.exe`) located in the Sentinel installation kit in the `Installer` folder under the subfolder appropriate for your locale.

3 Follow the instructions in the wizard, and then click *Finish*.

Configuring a Sentinel Server

When the installation is complete, you can configure additional Sentinel servers with the Aegis Adapter Configuration Utility.

1 Log on to the Aegis Server computer with a local administrator account.

2 In the NetIQ program group, click **NetIQ > Aegis > Aegis Adapter Configuration Utility**.

3 In the left pane, expand *Sentinel Servers*.

4 On the Edit menu, click **New Entry**.

5 Provide the appropriate information, and then click **Validate Credentials**.

6 Save the Sentinel server information.

7 Repeat Step 3 through Step 6 for each server you need to add.

8 Close the Aegis Adapter Configuration Utility.

Verifying a Successful Installation with Aegis

The setup program for the Sentinel adapter installs a new event type that you can use to create triggers and triggering event definitions. To verify a successful installation, check the new event type in the Aegis Configuration Console.

1 Start the Aegis Configuration Console.

For more information about starting the Configuration Console, see the *Administrator Guide for 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 Ensure `Sentinel.Alert` is in the list of available event types.

After verifying a successful installation, build a simple workflow with one of the activities in the Sentinel Activities library. For more information about building workflows, see the *Process Authoring Guide for Aegis*.

Aegis Workflow Activities Overview

The activities in the Sentinel Activities library allow Aegis to perform the following types of tasks, among others:

 ◆ Retrieve the attributes for specific alerts

 ◆ Retrieve the events related to a specific alert

 ◆ Query the knowledge base and retrieve comments

 ◆ Create, update, or close an alert

 ◆ Add comments to an alert

 ◆ Promote an alert to an incident

You can see all available activities by looking at the Sentinel Activities library in the Aegis Workflow Designer. For more information about each activity, see the Help.

Uninstalling the Sentinel Adapter

To uninstall the Sentinel adapter, use the Windows Add/Remove Programs tool.