NetIQ® Aegis™ Adapter for NetIQ Security Manager®

Configuration Guide

June 9, 2009

Contents

Overview 1

Product Requirements 1

Implementation Overview 1

Configuring the Security Manager Central Computer 2

Installing the Security Manager Adapter 3

Configuring Additional Security Manager Configuration Groups 5

Verifying a Successful Installation 5

Workflow Activities Overview 6

Updating Your License 6

Upgrading the Security Manager Adapter 7

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

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

© 2009 NetIQ Corporation. All Rights Reserved.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government’s rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Check Point, FireWall-1, VPN-1, Provider-1, and SiteManager-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

ActiveAgent, ActiveAnalytics, ActiveAudit, ActiveReporting, ADcheck, Aegis, AppAnalyzer, AppManager, the cube logo design, Change Administrator, Change Guardian, Compliance Suite, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Group Policy Administrator, Group Policy Guardian, Group Policy Suite, IntelliPolicy, Knowing is Everything, Knowledge Scripts, Mission Critical Software for E-Business, MP3check, NetConnect, NetIQ, the NetIQ logo, the NetIQ Partner Network design, Patch Manager, PSAudit, PSDetect, PSPasswordManager, PSSecure, Risk and Compliance Center, Secure Configuration Manager, Security Administration Suite, Security Analyzer, Security Manager, Server Consolidator, VigilEnt, Vivinet, Vulnerability Manager, Work Smarter, and XMP are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the United States and other jurisdictions. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

EXCEPT AS MAY BE EXPLICITLY SET FORTH IN THE APPLICABLE END USER LICENSE AGREEMENT, NOTHING HEREIN SHALL CONSTITUTE A WARRANTY AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW AND ARE EXPRESSLY DISCLAIMED BY NETIQ, ITS SUPPLIERS AND LICENSORS.

Overview

The NetIQ Aegis Adapter for NetIQ Security Manager (Security Manager adapter) allows NetIQ Aegis to communicate with a Security Manager central computer.

The Security Manager adapter includes a library of workflow activities specific to Security Manager that Process Authors can use in the Workflow Designer.

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

Product Requirements

The Security Manager adapter requires the following software versions:

- Security Manager 6.5
- Aegis 2.0

Implementation Overview

The following table provides an overview of tasks to configure the Security Manager adapter.

☑	**Steps**	**For more information, see…**
☐	**1.** Configure the Security Manager central computer.	“Configuring the Security Manager Central Computer” on page 2
☐	**2.** Install the Security Manager adapter.	“Installing the Security Manager Adapter” on page 3
☐	**3.** Configure additional Security Manager configuration groups.	“Configuring Additional Security Manager Configuration Groups” on page 5
☐	**4.** Verify the installation was successful.	“Verifying a Successful Installation” on page 5

Configuring the Security Manager Central Computer

Before installing the Security Manager adapter on the Aegis server computer, you must first configure the Security Manager central computer you want to use to communicate with Aegis. The `ResourceManagementClientSetup.exe` program installs the NetIQ Namespace Server on the central computer, which allows the Aegis server computer to communicate with the entire configuration group.

Notes

- If you want to evaluate a trial or "proof of concept" installation of Aegis and install all Security Manager and Aegis components on the same computer, you do not need to run the `ResourceManagementClientSetup.exe` program.
- For performance reasons, NetIQ does not recommend installing Aegis and Security Manager components on the same computer in a production environment.
- If you have multiple central computers in your configuration group, ensure you configure the central computer you want Aegis to use to connect to the configuration group. You can configure other central computers using the Aegis Adapter Configuration Utility after installing the Security Manager adapter.

You must install Aegis on the Aegis server computer before configuring the central computer. For more information about installing Aegis, see the *Administrator Guide for Aegis*.

To configure the Security Manager central computer you want to communicate with Aegis:

1. Log on to the central computer using an account that is a member of either the OnePointOp ConfgAdms or System group.
2. Open the *`installation folder`*`\NetIQ\IQConnectRuntime\`*`version number`* folder, where *`installation folder`* is the location where you installed NetIQ Security Manager version 6.5 and *`version number`* is the version number of the NetIQ Namespace Server framework.
3. Run the `ResourceManagementClientSetup.exe` program.
4. Click **Next**.
5. Verify the destination folder and click **Next**.
6. Specify the Aegis server computer host name and port number.
7. Specify the user name and password you want to use to access Aegis, using the format *`domain`*`\`*`user`*, and click **Next**.

8. Click **Next**.

9. Click **Finish**.

Notes

- You may need to restart your Security Manager central computer after configuring the NetIQ Namespace Server.
- The `ResourceManagementClientSetup.exe` program does not validate the permissions of the account used to access Aegis. Ensure the specified Aegis account has the necessary permissions. For more information about Aegis account permissions, see the *Administrator Guide for Aegis*.
- The Security Manager central computer, Security Manager database server, and Aegis server computer must all be in domains that trust each other.

Installing the Security Manager Adapter

After configuring your Security Manager central computer, install the Security Manager adapter on the Aegis server computer you specified in the central computer configuration. The Security Manager adapter allows Aegis to communicate with Security Manager and allows Process Authors to add Security Manager activities to the Aegis workflow.

You must install the Security Manager adapter on an Aegis server computer. You cannot install the software remotely. In addition, the Security Manager central computer, Security Manager database server, and Aegis server computer must all be in domains that trust each other.

For more information about installing Aegis, see the *Administrator Guide for Aegis*.

To install the Security Manager adapter and activity library:

1. Log on to the Aegis server computer using an account that has permission to access the OnePoint database on the Security Manager database server.

   If possible, the account should be a member of the OnePointOp System group on the Security Manager central computer.

2. Run the `SMAegisAdapter` program from the folder where you downloaded the NetIQ Aegis Adapter for NetIQ Security Manager.

3. Click **Next**.

4. Accept the license agreement, and then click **Next**.

5. Verify the Aegis host name and host port.

6. Specify the Aegis user name and password you want to use to install the Security Manager activity library and click **Next**.

   Note
   The setup program does not validate the permissions of the account used to access Aegis. Ensure that the specified Aegis account has the necessary permissions. For more information about Aegis account permissions, see the *Administrator Guide for Aegis*.

7. Specify the OnePoint database server name or IP address in *servername**instancename* format, where *instancename* is the name of the specific SQL instance, if applicable.

8. Specify the Security Manager central computer service account you want Aegis to use for Security Manager communication, and then click **Next**.

Note

Ensure you specify an account that is a member of either the OnePointOp ConfgAdms or System group on the Security Manager central computer.

---

9. Click **Finish**.

Configuring Additional Security Manager Configuration Groups

When the installation is complete, the Aegis Adapter Configuration Utility allows you to configure additional Security Manager configuration groups at any time.

To configure an additional Security Manager configuration group:

1. Log on to the Aegis Server computer using a local administrator account.
2. In the NetIQ program group, click **Aegis > NetIQ Aegis Adapter Configuration**.
3. In the left pane, click **Security Manager**.
4. On the Edit menu, click **New Entry**.
5. Specify the configuration group database server name or IP address.
6. Specify the name of the database server SQL Server 2005 instance, if applicable.
7. Click **OK**.
8. In the left pane, click the name of the central computer for the new configuration group.
9. Click **OK**.
10. Specify the port number you want the Security Manager adapter to use to connect to the central computer.
11. Specify the Security Manager service account you want Aegis to use to communicate with the central computer in the format *domain**user*.

    Note
    Ensure you specify an account that is a member of either the OnePointOp ConfgAdms or System group on the Security Manager central computer.

12. Specify and then confirm the service account password.
13. Click **Save All**.
14. Click **Close**.
15. Restart the NetIQ Aegis Namespace Provider service.

Verifying a Successful Installation

You can verify a successful installation of the Security Manager adapter. After the Aegis installation is complete, Aegis imports the Security Manager adapter 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 Aegis Configuration Console, see the *Administrator Guide for Aegis*.

2. In the Navigation pane, click **Resources**.
3. In the left pane, click **Adapter Resource Hierarchies**.
4. Expand the Security Manager adapter.
5. Ensure Aegis displays the Security Manager adapter you specified during installation as a data source.
6. Ensure the computers associated with the adapter display as resources.

After verifying the Security Manager adapter and its computers display as a data source and its resources, build a simple workflow with one of the activities in the Security Manager activity library. For more information about building workflows, see the *Administrator Guide for Aegis*.

Workflow Activities Overview

The activities in the Security Manager activities library allow Aegis to perform the following types of tasks:

- Find and update Security Manager real-time alerts
- Send a new event to Security Manager
- Retrieve and update knowledge for processing rules
- Get data from a recent Forensic Analysis report
- Perform Security Manager functions, such as forcing configuration changes and enabling or disabling processing rules

For detailed information about each activity, see its related Help.

Updating Your License

The Security Manager adapter installation kit includes a 30-day trial license for the adapter by default. You can update your existing license at any time. For example, if the adapter license has expired or is about to expire, you can update it with a valid updated license key from the appropriate vendor. For more information about Aegis licenses, see the *Administrator Guide for Aegis*.

Upgrading the Security Manager Adapter

If you upgrade your Aegis server computer, ensure you install the latest version of the Security Manager adapter and activity library, as well. For more information about upgrading Aegis, see the *Administrator Guide for Aegis*.

Note
Before upgrading to the latest version of the Security Manager adapter, you must upgrade your Security Manager installation to version 6.5 or later and reconfigure the central computer you use to communicate with Aegis.

To reconfigure Security Manager and upgrade the Security Manager adapter:

1. Log on to the central computer using an account that is a member of either the OnePointOp ConfgAdms or System group.
2. Open the *`installation folder`*`\NetIQ\IQConnectRuntime\`*`version number`* folder, where *`installation folder`* is the location where you installed NetIQ Security Manager version 6.5 and *`version number`* is the version number of the NetIQ Namespace Server framework.
3. Run the `ResourceManagementClientSetup.exe` program.
4. Click **Next**.
5. Verify the destination folder and click **Next**.
6. Specify the Aegis server computer host name and port number.
7. Specify the user name and password you use to access Aegis, using the format *`domain`*`\`*`user`*, and click **Next**.
8. Click **Next**.
9. Click **Finish**.

   Notes
   - You may need to restart your Security Manager central computer after configuring the NetIQ Namespace Server.
   - The `ResourceManagementClientSetup.exe` program does not validate the permissions of the account used to access Aegis. Ensure you specify the correct Aegis account. For more information about Aegis account permissions, see the *Administrator Guide for Aegis*.
10. Log on to the Aegis server computer using an account that has permission to access the OnePoint database on the Security Manager database server.

    If possible, the account should be a member of the OnePointOp System group on the Security Manager central computer.
11. Run the `SMAegisAdapter` program from the folder where you downloaded the new version of the NetIQ Aegis Adapter for NetIQ Security Manager.
12. Click **Next**.
13. Accept the license agreement, and then click **Next**.

14. Verify the Aegis host name and host port.

15. Specify the Aegis user name and password you use to access the Security Manager activity library and click **Next**.

    Note
    The setup program does not validate the permissions of the account used to access Aegis. Ensure that you specify the correct Aegis account. For more information about Aegis account permissions, see the *Administrator Guide for Aegis*.

16. Specify the OnePoint database server name or IP address in *servername**instancename* format, where *instancename* is the name of the specific SQL instance, if applicable.

17. Specify the Security Manager central computer service account Aegis uses for Security Manager communication, and then click **Next**.

    Note
    Ensure you specify an account that is a member of either the OnePointOp ConfgAdms or System group on the Security Manager central computer.

18. Click **Finish**.