



# NetIQ® Aegis™ Adapter for NetIQ® Directory and Resource Administrator™ Configuration Guide

May 2012

---

## Contents

|   |   |
|---|---|
| Overview .....  | 3 |
| Product Requirements .....  | 3 |
| Understanding How the<br>DRA Adapter Uses<br>Multi-Master Sets..... | 3 |
| Supported Configurations .....                                      | 3 |
| Implementation Overview .....                                       | 4 |
| Ensuring Minimum Rights<br>and Privileges .....                     | 5 |
| Default Ports.....  | 5 |
| Installing the DRA Adapter....                                      | 6 |
| Validating Administration<br>Server Connections .....               | 7 |
| Configuring Administration<br>Server Connections .....              | 8 |
| Verifying a Successful<br>Installation.....                         | 9 |

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

NetIQ Aegis is protected by United States Patent No(s): 5829001, 5999178, 6708224, 6792462.

NetIQ Directory and Resource Administrator is protected by United States Patent No. 6792462.

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.

© 2012 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.

ActiveAudit, ActiveView, Aegis, AppManager, Change Administrator, Change Guardian, Compliance Suite, the cube logo design, 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, Knowledge Scripts, NetConnect, NetIQ, the NetIQ logo, PSAudit, PSDetect, PSPasswordManager, PSSecure, Secure Configuration Manager, Security Administration Suite, Security Manager, Server Consolidator, VigilEnt, and Vivinet are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the USA. 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.

---

## Overview

The NetIQ Aegis Adapter for NetIQ Directory and Resource Administrator (DRA adapter) allows Aegis to communicate with NetIQ Directory and Resource Administrator (DRA) and automate manual processes associated with the administration and security of Microsoft Active Directory.

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

---

## Product Requirements

The DRA adapter requires the following minimum software versions:

- DRA 8.6 Service Pack 1
- Aegis 2.2
- Microsoft .NET Framework 3.0

The DRA adapter requires one of the following operating system versions:

- Windows Server 2008 R2 (32-bit and 64-bit)
- Windows Server 2008 (32-bit and 64-bit)
- Windows Server 2003 Standard Service Pack 2 (32-bit and 64-bit)
- Windows Server 2003 Enterprise Service Pack 2 (32-bit and 64-bit)

---

## Understanding How the DRA Adapter Uses Multi-Master Sets

In DRA, a Multi-Master Set (MMS) is a set of multiple Administration servers. Each MMS consists of a primary Administration server and one or more secondary Administration servers. The primary server provides security and domain management as well as account and Microsoft Exchange management. Each secondary server acts as a supplemental server, providing additional access to enterprise data while allowing you to balance loads and traffic across local or remote locations. Secondary servers also ensure availability if the primary server is offline.

The DRA adapter requires at least one MMS in the Aegis namespace for Aegis to model the DRA environment. If your DRA environment does not have an existing MMS, you do not have to create one in DRA. The installation program creates one for you in the Aegis namespace. The default name is `Mul ti MasterSet`, but you can specify any name.

Each MMS has an associated Run As account the DRA adapter uses to communicate with DRA and run the activities in a workflow. For more information about the Run As account, see [“Ensuring Minimum Rights and Privileges”](#) on page 5.

---

## Supported Configurations

The DRA adapter supports the following DRA configurations.

### Single Administration Server

The DRA adapter communicates with one Administration server that manages a single domain. The Aegis Server computer must be a member of the managed domain. The Aegis service account must have “run as” privileges.

### Multiple Administration Servers

The DRA adapter communicates with multiple Administration servers, each of which manages a different domain. There must be a trust relationship between the domains, and the Aegis Server computer must be a member of the trusted domain. The Aegis service account must have “run as” privileges.

### Single MMS

The DRA adapter communicates with an MMS that manages a forest. There must be a trust relationship between the domains in the forest, and the Aegis Server computer must be a member of the trusted domain. The Aegis service account must have “run as” privileges.

### Multiple MMSs

The DRA adapter communicates with multiple MMSs, each of which manages a different forest. There must be a trust relationship between the forests, and the Aegis Server computer must be a member of the trusted domain. The Aegis service account must have “run as” privileges.

For more information about assigning “run as” privileges to the Aegis service account, see [“Ensuring Minimum Rights and Privileges”](#) on page 5.

---

## Implementation Overview

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

| <input checked="" type="checkbox"/> | Steps  | For more information, see...  |
|-------------------------------------|--|---|
| <input type="checkbox"/>            | 1. Configure the minimum rights and privileges for the Run As account and Aegis service account. | <a href="#">“Ensuring Minimum Rights and Privileges”</a> on page 5        |
| <input type="checkbox"/>            | 2. Install a DRA console on the Aegis Server computer.   | <a href="#">“Installing the DRA Adapter”</a> on page 6                    |
| <input type="checkbox"/>            | 3. Install the DRA adapter on the Aegis Server computer.   | <a href="#">“Installing the DRA Adapter”</a> on page 6                    |
| <input type="checkbox"/>            | 4. Validate the configuration information you supplied during the installation process.          | <a href="#">“Validating Administration Server Connections”</a> on page 7  |
| <input type="checkbox"/>            | 5. Configure the adapter to connect to additional Administration servers.                        | <a href="#">“Configuring Administration Server Connections”</a> on page 8 |
| <input type="checkbox"/>            | 6. Verify the installation was successful.   | <a href="#">“Verifying a Successful Installation”</a> on page 9           |

---

## Ensuring Minimum Rights and Privileges

Before you install the DRA adapter, configure the following *minimum* rights and privileges for the Run As account and the Aegis service account.

### Run As Account

When you install the DRA adapter, you must specify the credentials for the Run As account. The Run As account allows the DRA adapter to communicate with DRA and run the activities in a workflow. The Run As account must be:

- A member of the Domain Users Global Security Group in the target domain or a Local Account on a managed server
- A valid Assistant Admin (AA) in DRA with the `Audit All Objects` role

### ActiveView for the Run As Account

In DRA, create an ActiveView for the Run As account. Ensure the ActiveView has the powers to add, modify, and delete the following objects:

- Groups
- Users
- Contacts
- ActiveViews
- AA groups
- Organizational Units (OUs)

### Aegis Service Account

The Aegis service account is the account Aegis uses to execute the Namespace Provider service on the Aegis Server. The Aegis service account on the Aegis Server computer must have “run as” privileges in your environment.

To ensure the Aegis service account has “run as” privileges, in Local Security Settings on the Aegis Server computer, assign the `Impersonate a client after authentication` policy to the Aegis service account.

For more information about supported configurations, see [“Supported Configurations”](#) on page 4.

---

## Default Ports

To enable proper communication between the DRA adapter and the DRA Administration service in your DRA environment, ensure the following ports are open on the DCOM server computer.

| Port Number            | Component Computer       | Port Use   |
|------------------------|--------------------------|--|
| DCOM 135               | Aegis Server computer    | Allows the DRA adapter to locate the Administration service.   |
| RPC <i>xxxxx-xxxxx</i> | Database Server computer | Allows the DRA adapter to communicate with the DCOM Service communication. Enter the port range you specified in your DCOM configuration, typically ports 60000-60100. |

---

## Installing the DRA Adapter

You must install the DRA adapter on an Aegis Server computer. You cannot install the adapter remotely.

Before you install the DRA adapter, you must install one of the following DRA consoles on the Aegis Server computer:

- Delegation and Configuration Console
- Account and Resource Management Console
- Command Line Interface

For more information about installing these components, see the *Installation Guide for Directory and Resource Administrator*.

If your Aegis Server computer is part of a cluster, you must install the adapter on the active node first, and then on each each passive node.

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

These steps guide you through the process of installing the DRA adapter on one of the following:

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

**To install the DRA adapter on the Aegis Server computer:**

1. Log on to the Aegis Server computer with an administrator account.
2. Run the setup program from the folder where you downloaded the NetIQ Aegis Adapter for NetIQ Directory and Resource Administrator.
3. Click **Next**.
4. Accept the license agreement, and then click **Next**.
5. On the Logon Information page of the installation wizard, provide the logon credentials for the Aegis service account. If you do not know the logon credentials for the Aegis service account, contact your Aegis administrator.
6. Click **Next**.
7. On the NetIQ Directory and Resource Administrator Connection page of the setup program, provide the following information:
  - **Name of an MMS to configure.** If your environment does not have an MMS, the installation program creates one for you. You can specify the name or accept the default. For more information about how the DRA adapter uses MMSs, see [“Understanding How the DRA Adapter Uses Multi-Master Sets”](#) on page 3.
  - **Name of an Administration server to configure.** Specify the primary Administration server for the MMS. You can configure secondary Administration servers using the Aegis Adapter Configuration Utility. For information about configuring Administration server connections, see [“Adding an Administration Server to an Existing MMS”](#) on page 8. If you do not specify an MMS, the installation program creates one for you and adds the Administration server to it.

- **Logon credentials for the Run As account on the specified Administration server.** If you do not know the logon credentials for the Run As account, contact your DRA administrator.

---

**Note**

The installation program uses the Administration server and Run As account information to populate the registry. It does not validate the information at this time. For more information about validating the information, see [“Validating Administration Server Connections”](#) on page 7.

---

8. Click **Next**.
9. Follow the remaining instructions in the setup program.
10. When you finish installing the DRA adapter, click **Finish**.

## Installing on a Passive Node in a Cluster

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

### To install the DRA adapter on a passive node in a cluster:

1. Log on to the passive Aegis Server node with an administrator account.
2. Open a command prompt for the folder where you downloaded the NetIQ Aegis Adapter for NetIQ Directory and Resource Administrator.
3. Type the following command:  

```
msiexec /i IQDRAInstaller.msi /I *V IQDRAInstaller.log SKIPCONFIG="TRUE"
```
4. Follow the instructions in the setup program until you finish installing the DRA adapter, and then click **Finish**.

---

## Validating Administration Server Connections

When the installation is complete, the Aegis Adapter Configuration Utility allows you to validate the information you supplied during the installation process.

### To validate a connection to an Administration server:

1. Log on to the Aegis Server computer with an administrator account.
2. In the NetIQ program group, click **Aegis > NetIQ Aegis Adapter Configuration**.

---

**Note**

If your user account does not have administrator privileges on the Aegis Server computer, right-click the **NetIQ Aegis Adapter Configuration** shortcut, and then click **Run As Administrator**.

---

3. In the left pane, expand **DRA Adapter**, and then expand the appropriate MMS.
4. In the left pane, click the Administration server for which you want to validate the connection.
5. Click **Validate**.
6. *If the connection is invalid*, make the appropriate changes, and then click **Save All**.
7. Click **Close**.
8. *If you made any changes*, restart the NetIQ Aegis Namespace Provider service.

---

## Configuring Administration Server Connections

When the installation is complete, the Aegis Adapter Configuration Utility allows you to configure Administration server connections at any time. Using the Aegis Adapter Configuration Utility, you can:

- Add Administration servers to any existing MMS.
- Configure the DRA adapter to communicate with additional MMSs.
- Modify the Run As account credentials for existing servers.

### Adding an Administration Server to an Existing MMS

Using the Aegis Adapter Configuration Utility, you can add one or more Administration servers to an existing MMS. The DRA adapter automatically detects the primary Administration server in the MMS.

#### To add an Administration server to an existing MMS:

1. Log on to the Aegis Server computer with an administrator account.
2. In the NetIQ program group, click **Aegis > NetIQ Aegis Adapter Configuration**.

---

**Note**

If your user account does not have administrator privileges on the Aegis Server computer, right-click the **NetIQ Aegis Adapter Configuration** shortcut, and then click **Run As Administrator**.

---

3. In the left pane, expand **DRA Adapter**, and then click the MMS to which you want to add a new Administration server.
4. On the Edit menu, click **New Entry**.
5. Provide the appropriate information, and then click **Save All**.
6. Click **Close**.
7. Restart the NetIQ Aegis Namespace Provider service.

### Configuring a New MMS in the DRA Adapter

Using the Aegis Adapter Configuration Utility, you can create a new MMS.

#### To configure the DRA adapter to communicate with an additional MMS:

1. Log on to the Aegis Server computer with an administrator account.
2. In the NetIQ program group, click **Aegis > NetIQ Aegis Adapter Configuration**.

---

**Note**

If your user account does not have administrator privileges on the Aegis Server computer, right-click the **NetIQ Aegis Adapter Configuration** shortcut, and then click **Run As Administrator**.

---

3. In the left pane, click **DRA Adapter**.
4. On the Edit menu, click **New Entry**.
5. Provide the name for the new MMS, and then click **Save All**.

6. *To add an Administration server to the MMS*, complete the following steps:
  - a. In the left pane, click the new MMS.
  - b. On the Edit menu, click **New Entry**.
  - c. Provide the appropriate information, and then click **Save All**.
7. Click **Close**.
8. Restart the NetIQ Aegis Namespace Provider service.

---

## Verifying a Successful Installation

After you configure at least one Administration server connection, Aegis imports all computers in the managed domains as resources.

**To verify successful registration with the Resource Management database:**

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 **Resources**.
3. In the left pane, expand **Adapter Resource Hierarchies**.
4. Ensure **DRA Adapter** is in the list of installed adapters.
5. *If you configured one or more Administration server connections*, complete the following steps:
  - a. Expand **DRA Adapter**.
  - b. Expand **DRA Data Source for MMS**, where MMS is the name of the MMS to which an Administration server belongs.
  - c. Ensure the domains and OUs associated with the MMS display in the list.
  - d. Ensure the Administration servers associated with the MMS display as resources.

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

