

Code Promotion

December 2013



IMPORTANT: Code Promotion is an early access feature in the NetIQ Access Manager 4.0 release.

Code Promotion is an easy to use secure functionality to move the configuration data of Access Manager from one environment to another. It allows you to export the configuration data as a password-protected encrypted file. You can then import this file into another Access Manager system and seamlessly replicate the configuration into the target system.

The exported configuration data includes generic Identity Server cluster configuration and policy configuration. It is independent of the device specific data and network specific data. Hence, you can use the Code Promotion feature to promote configuration between two Access Manager systems that are in different networks, with different number of devices, and with different user stores. The Access Manager systems must be on the same platform.

- ♦ [Section 1, "How Code Promotion Helps?," on page 1](#)
- ♦ [Section 2, "Use Cases," on page 2](#)
- ♦ [Section 3, "Sequence of Promoting the Configuration Data," on page 2](#)
- ♦ [Section 4, "Prerequisites," on page 4](#)
- ♦ [Section 5, "Limitations," on page 4](#)
- ♦ [Section 6, "Applying the Code Promotion EAR Patch," on page 4](#)
- ♦ [Section 7, "Enabling Code Promotion," on page 5](#)
- ♦ [Section 8, "Exporting the Configuration Data by Using Code Promotion," on page 5](#)
- ♦ [Section 9, "Importing the Configuration Data by Using Code Promotion," on page 7](#)
- ♦ [Section 10, "Post-Import Configuration Tasks," on page 9](#)
- ♦ [Section 11, "Exporting the Access Gateway Configuration Data," on page 10](#)
- ♦ [Section 12, "Importing the Access Gateway Configuration Data," on page 11](#)
- ♦ [Section 13, "A Case Study: Moving Access Manager to Another Environment," on page 13](#)
- ♦ [Section 14, "Troubleshooting," on page 13](#)
- ♦ [Section 15, "Legal Notice," on page 14](#)

1 How Code Promotion Helps?

Code Promotion addresses the pain points associated with the following activities:

- ♦ **Managing Multiple Access Manager Setups:** Typically, multiple Access Manager setups are maintained to test configuration changes before applying them on production systems. For example, you can use the staging environment to deploy Access Manager, test various configurations and customizations, and apply these changes to the production environment. Earlier, there was no easy way to promote the tested and approved configuration data to the production environment. The configuration data had to be manually replicated in to another system. This was a time-consuming and error prone process. Code Promotion provides a

mechanism to move the configuration data across environments. This increases efficiency, improves productivity, and in turn reduces costs of managing configurations across environments.

- ♦ **Managing Different Administrators for Different Setups:** Different administrators can manage different Access Manager environments. Hence, manually replicating the configuration to the different stages requires the maintenance of the precise list of all changes done on one system and this knowledge must be transferred among administrators.
- ♦ **Replacing or Moving Physical Devices:** You may need to replace physical devices or you may need to move devices to a different network due to a business decision, such as, changing a network infrastructure vendor. Hence, a mechanism that is independent of these network changes is needed to transfer the configuration data.

2 Use Cases

Code Promotion simplifies promotion of the configuration data in the following scenarios:

- ♦ You want to test your configuration in a dedicated testing environment and then deploy the configuration data to a new production environment.
- ♦ You maintain multiple test environments and you want the configuration changes to pass through these stages before deploying the configuration data to an existing production environment.
- ♦ You want to move your application to another physical server.
- ♦ You want to move the application hardware to a different network infrastructure.

3 Sequence of Promoting the Configuration Data

You must promote the configuration data in the following sequence:

1. Identity Server configurations, policies configurations, and Certificates and Keystores configurations
2. Access Gateway configurations

[Table 1](#) lists the configurations that you can promote to another environment and the corresponding promotion mechanism.

Table 1 Configuration Promotion Mechanism

Data	Promotion Supported?	Mechanism
Identity Server configuration	Yes	Use the Code Promotion feature. For more information, see Section 8, “Exporting the Configuration Data by Using Code Promotion,” on page 5 and Section 9, “Importing the Configuration Data by Using Code Promotion,” on page 7 .
Policies configurations	Yes	Use the Code Promotion feature. For more information, see Section 8, “Exporting the Configuration Data by Using Code Promotion,” on page 5 and Section 9, “Importing the Configuration Data by Using Code Promotion,” on page 7 .

Data	Promotion Supported?	Mechanism
Certificates and Keystores configurations	Yes	Use the Code Promotion feature. For more information, see Section 8, “Exporting the Configuration Data by Using Code Promotion,” on page 5 and Section 9, “Importing the Configuration Data by Using Code Promotion,” on page 7 .
Access Gateway configurations	Yes	Use the existing Access Gateway Export and Import Configuration feature. For more information, see Section 11, “Exporting the Access Gateway Configuration Data,” on page 10 and Section 12, “Importing the Access Gateway Configuration Data,” on page 11 .
Device customizations	No	Manually export and import the data. For more information, see Section 10, “Post-Import Configuration Tasks,” on page 9 .
Device information	No	Not applicable as devices are specific to a setup.

Promoting the configuration data consists of the following steps:

1. Install Access Manager 4.0 or upgrade the prior version of Access Manager on your source and target systems.

For more information about how to install Access Manager, see [NetIQ Access Manager 4.0 Installation Guide](#).

For more information about how to upgrade and migrate Access Manager, see [NetIQ Access Manager 4.0 Migration and Upgrade Guide](#).
2. Apply the Code Promotion EAR patch on both the systems.
For more information, see [Section 6, “Applying the Code Promotion EAR Patch,” on page 4](#).
3. Enable Code Promotion on both source and target systems.
For more information, see [Section 7, “Enabling Code Promotion,” on page 5](#).
4. Export the Identity Server configuration and Policy configuration by using the Code Promotion feature from the source system.
For more information, see [Section 8, “Exporting the Configuration Data by Using Code Promotion,” on page 5](#).
5. Export the Access Gateway configuration the source system.
For more information, see [Section 11, “Exporting the Access Gateway Configuration Data,” on page 10](#).
6. Import the Identity Server configuration and Policy configuration by using the Code Promotion feature on the target system.
For more information, see [Section 9, “Importing the Configuration Data by Using Code Promotion,” on page 7](#).
7. Add Identity Server devices to the newly imported clusters if any. Update the devices if they are already part of the cluster.
8. If your Access Gateway devices are in a cluster, remove the Access Gateway device you want to update from of the cluster.
9. Import the Access Gateway configuration into that device.

10. Create a new Access Gateway cluster with that device.
11. Move Access Gateway devices from the old cluster into the new cluster. When all devices are moved, the old cluster is automatically deleted.
12. Assign the Identity Server to the Access Gateway cluster.
13. Update the Access Gateway cluster.

4 Prerequisites

- Code Promotion is an early access feature in the 4.0 release. Hence, you must enable this feature to use it. See [Section 7, “Enabling Code Promotion,” on page 5](#).
- The source server and the target server must have Access Manager 4.0. If you want to export the configuration data from an earlier version of Access Manager into Access Manager 4.0, you must upgrade or migrate the existing setup to Access Manager 4.0. For more information about how to upgrade or migrate Access Manager, see the [NetIQ Access Manager 4.0 Migration and Upgrade Guide](#).
- The source server and the target server must run on the same operating system.
- The source server and the target server must have the same model; that is, both must be either Access Manager or Access Manager Appliance.
- Importing configuration data replaces the existing configuration data. Hence, use the backup option in the Import wizard to preserve a copy of the existing configuration before an import.

5 Limitations

- Code Promotion supports export and import of only the Identity Server configuration and policy configuration data.
- Code Promotion supports export and import of only the generic configuration data. It does not support exporting and importing the configuration data that vary from one system to another. For example, you can export and import network specific configuration, device specific configuration, configuration store, and its replica ring configuration.
- You can enable this feature only on the primary Administration Console.

6 Applying the Code Promotion EAR Patch

Prerequisites

- Before upgrading Access Manager, back up your current configuration. If the upgrade fails for any reason, you can use the backup file to recover your configuration.

To back up your Access Manager configuration, go to the `/opt/novell/devman/bin` directory on the primary Administration Console. Run the `ambkup.sh` script.

- Verify that you have installed the latest version of Access Manager 4.0.

In the Administration Console, click **Access Manager > Auditing > Troubleshooting > Version**.

Procedure

- 1 Download the `AM_400_HF_CP_EA_PatchTool.zip` file from [Novell Downloads \(download.Novell.com/patch/finder\)](http://download.Novell.com/patch/finder).
- 2 Run the following command to unzip the file:


```
unzip AM_400_HF_CP_EA_PatchTool.zip
```

- 3 Go to `/opt/Novell/patching/bin`.
- 4 Run the following command to install the patch:

```
./patch -i /home/AM_400_HF_CP_EA-<buildnumber>.patch
```

For more information about options to administer the Access Manager patch file, see section *Upgrading Access Manager Using the Patch Process > Administering Patches* in the [NetIQ Access Manager 3.2 SP2 Installation Guide](#).

7 Enabling Code Promotion

You must enable Code Promotion manually on the primary Administration Console. After enabling, the Administration Console displays a new option Code Promotion (**Access Manager > Code Promotion**), which allows you to export and import of configuration data across environments.

Linux:

- 1 Log in to the primary Administration Console as a root user.
- 2 Stop the Administration Console by using the `/etc/init.d/novell-ac stop` command.
- 3 Add the following line to the end of the `/opt/novell/nam/adminconsole/conf/tomcat7.conf` file:

```
JAVA_OPTS="${JAVA_OPTS} -Dcom.netiq.nam.enableStaging=true"
```
- 4 Start the Administration Console by using the `/etc/init.d/novell-ac start` command.

Windows:

- 1 Log in to the Windows primary Administration Console system.
- 2 Stop the Tomcat7 service.
- 3 Go to `C:\Program Files(x86)\Novell\Tomcat\bin`.
- 4 Double-click `tomcat7w.exe`.
- 5 Go to the **Java** tab and add `-Dcom.netiq.nam.enableStaging=true` to the Java options.
- 6 Click **Ok**.
- 7 Go to the **General** tab and start Tomcat.

8 Exporting the Configuration Data by Using Code Promotion

The Code Promotion page displays a list of all configuration files exported from that system. It displays the metadata of each exported configuration: date of export, configuration exported, name of user who exported, a link to download the exported file, and the comments.

You can download the previously exported configuration files from this page. These exported files are also saved on the primary Administration Console system at the following location:

Linux: `/var/opt/novell/novlwww/namconfig`

Windows: `C:\Program Files(x86)\Novell\Tomcat\bin`

You as an administrator can delete or back up these files if needed. If these files are deleted from the disk, they will no longer be listed on the Code Promotion page.

Access Manager ▾ Devices ▾ Policies ▾ Auditing ▾ Security

Code Promotion

Code Promotion

Export Configuration | Import Configuration

Date of Export	Configuration Exported	Exported By	Action	Comments
Configuration Exports				
Oct 21, 2013 10:41 AM	2 Identity Provider Clusters	cn=admin,o=novell	Download	Auto backup created during configuration import
Oct 18, 2013 09:52 AM	1 Identity Provider Cluster	cn=admin,o=novell	Download	Auto backup created during configuration import

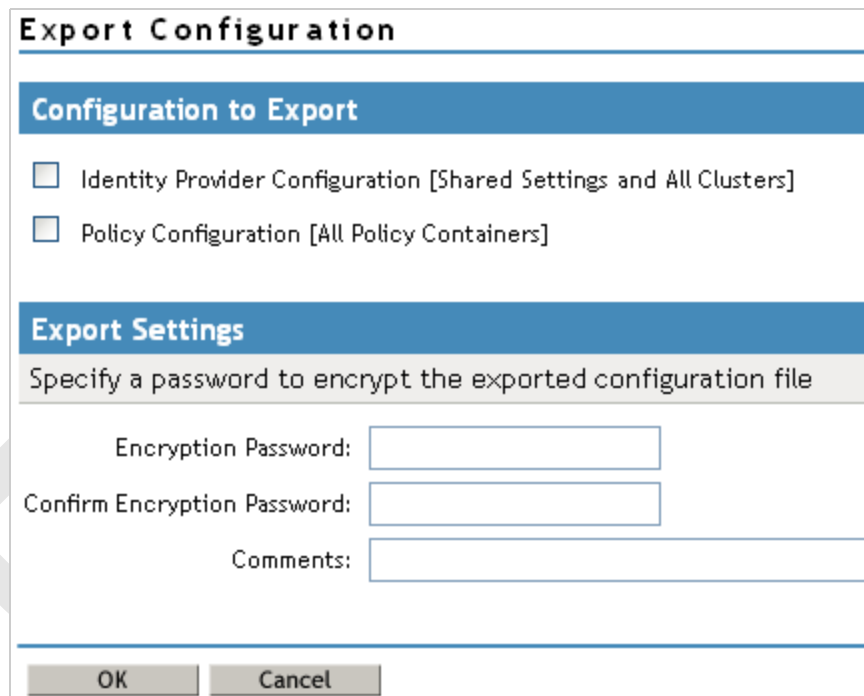
Close

The exported configuration data includes:

- ◆ Identity Server configuration
 - ◆ Cluster configuration
 - ◆ Shared Settings
 - ◆ Keystores
 - ◆ Trusted roots
- ◆ Policy configuration
 - ◆ All policy containers
 - ◆ All policy definitions
 - ◆ Policy extensions

Perform the following steps to export the configuration data:

- 1 Log in to the Administration Console from where you want to export the configuration data.
- 2 In the Administration Console, click **Access Manager > Code Promotion**.
You must enable Code Promotion to see this option. See [Section 7, “Enabling Code Promotion,” on page 5](#).
- 3 In the Code Promotion page, click **Export Configuration**.



Export Configuration

Configuration to Export

☐ Identity Provider Configuration [Shared Settings and All Clusters]

☐ Policy Configuration [All Policy Containers]

Export Settings

Specify a password to encrypt the exported configuration file

Encryption Password:

Confirm Encryption Password:

Comments:

OK Cancel

- 4 Based on your requirements, select the configuration to export:

Identity Provider Configuration: This will export all clusters, shared settings, keystores, and trust stores.

Policy Configuration: This will export all the policy containers, policy definitions, and policy extensions.

- 5 Specify a password to encrypt the archived configuration data file.

You require this password to decrypt the ZIP file while importing configuration data into another environment.

- 6 Add an appropriate comment for this export in **Comments**. This can be helpful to identify the exported configuration.

For example, Configuration export after UAT completion.

- 7 Click **OK** and save the file at your preferred location on your local system.

9 Importing the Configuration Data by Using Code Promotion

Import the configuration data only on the primary Administration Console.

Perform the following steps to import configuration data:

- 1 Ensure that the ZIP file containing the configuration data that you want to import is accessible.
- 2 Log in to the Administration Console in which you want to import configuration data.
- 3 In the Administration Console, click **Access Manager > Code Promotion**.
- 4 In the Code Promotion page, click **Import Configuration**.


Import Configuration

Step 1 of 3: Upload configuration file to import

Configuration File To Import: No file selected.

Decryption Password:


Backup Settings

 : Always enable the configuration backup option. This will help you to roll back your changes if needed.

☒ Backup current configuration before import

(Note: Backed up configuration will be encrypted using the password specified above.)

Import Settings

 : Import all configuration as a whole. If importing individual pieces, ensure that the dependencies are met.

☒ Import Identity Provider Clusters

☒ Import Identity Provider Shared Settings

☒ Import Policies

<< Back

Next >>

Cancel

- 5 Click **Browse** to import the configuration file.
- 6 In **Decryption Password**, specify the password that you used to encrypt the configuration data file. You need this password to extract the contents of the configuration file.
- 7 (Optional) Select **Backup current configuration before import**. This backup helps to roll back your changes if needed. The backup file is encrypted with the same password that is used for decryption in [Step 6](#). You can download this backup file from the Code Promotion page.
- 8 Under **Import Settings**, select the desired options based on your requirements.

Select all configurations and import them as a whole. Identity Server clusters have dependencies on Shared Settings. Hence, if you want to select only to import the Identity Server clusters configuration data, ensure that all Shared Settings that are referenced are configured in this system.

Importing Shared Settings overwrites the existing Shared Settings on the system with new Shared Settings. However, these will not be deleted.

The following table lists examples with Attribute Sets illustrating the import action:

Imported Attribute Sets	Existing Attribute Sets	Import Action
OIOSAML with five mappings	OIOSAML with two mappings	OIOSAML set is replaced with the imported one. Hence, it has five mappings.
AttrSet1	Not available	AttrSet1 is added.
No import	AttrSet2 is defined only in the target system	AttrSet2 remains unchanged.

- 9 Click **Next**.

If you selected **Import Identity Provider Clusters** in [Step 8](#), the Import Identity Provider Clusters page allows you to specify the import action for each cluster found in the imported configuration.

- 10 Select a cluster to configure import settings in **Clusters To Import**.
- 11 Select an action for the selected cluster from **Import Action**. The following options are available:

Do Not Import: The default setting for all clusters. To import the cluster configuration data, you need to apply any of the other two options available for a particular cluster.

Import As New Cluster: Select this option if you want to import the cluster as a new cluster. Specify **New Cluster Name** and **New Cluster URL**. Ensure that the new cluster name is different from the existing cluster names defined on that system.

Overwrite Existing Cluster: Select this option if you want to overwrite the existing cluster with the selected cluster. Specify which **Cluster To Overwrite**.

NOTE: You need to configure import action for each cluster separately. If the cluster you want to import has only one user store, it will be mapped to the default user store of the existing cluster. If the cluster you are importing has multiple user stores, then you must specify how to map them to the user stores of the existing cluster.

- 12 Click **Next**.

When import is done, the final page displays the status of the import operation. It also lists the manual steps you must perform to get the Identity Server clusters to a working state.

- 13 Make a note of manual configuration steps and then click **Finish**. Continue with [Section 10, "Post-Import Configuration Tasks,"](#) on page 9.

10 Post-Import Configuration Tasks

After importing the Identity Server configuration data, you must perform configurations that are specific to the target system and that are not part of the exported data.

- ♦ After the import process is complete, the system displays a list of certificates that you need to create manually. Identity Server key stores are imported, but you must create the certificates referenced in them on the server where you have imported the configuration data. The new certificate name must exactly match with the names listed. For more information about how to create certificates, see ["Creating Certificates"](#) in the *NetIQ Access Manager 4.0 Administration Console Guide*.
- ♦ Configure user stores for the newly added clusters. After the import process is complete, the system displays a list of Identity Server clusters for which you need to configure user stores. A placeholder user store entry will be created. You must enter the IP address, search context, and the password for the target system user stores. For more information, see ["Configuring Identity User Stores"](#) in the *NetIQ Access Manager 4.0 Identity Server Guide*.
- ♦ Distribute the policy extension JARs to devices in the Administration Console under **Policy > Extensions**. For more information, see ["Distributing a Policy Extension"](#) in the *NetIQ Access Manager 4.0 Policy Guide*.
- ♦ Update service providers with the new metadata. (Conditional)

The identity provider certificate is different in the exported and imported systems. Hence, you must re-import the identity provider metadata to all service providers in that cluster for federation to work. For more information, see ["Viewing and Reimporting a Trusted Provider's Metadata"](#) in the *NetIQ Access Manager 4.0 Identity Server Guide*.

- ♦ Copy customization files from the exported setup into the devices in this setup. This includes the Identity Server custom Authorization classes, custom JSP files, and so forth.
- ♦ Persistent federation identities and shared secrets are not imported. These are to be shared between the Identity Servers in your exported setup and service providers only. They do not apply to the Identity Servers in the imported system. You must configure these on the server after you import the configuration data.

11 Exporting the Access Gateway Configuration Data

- 1 In the Administration Console, click **Devices > Access Gateway > [Name of Access Gateway]**.
- 2 Click **Configuration > Export**.
- 3 (Conditional) If you want to encrypt the file, specify the following details:

Password protect: Select this option to encrypt the file.

Password: Specify a password to encrypt the file. You require the same password during decrypting the file on the target system.

- 4 Click **OK**, then select to save the configuration to a file.

The filename is the name of the Access Gateway with an `.xml` extension.

- 5 (Conditional) If you want to change the names of the proxy services and their DNS names from a staging name to a production name, complete the following:

5a Open the configuration file in a text editor.

5b Search and remove the staging suffix.

If you have specified DNS names with a staging suffix (for example, `innerwebstaging.provo.novell.com`), you can search for `staging.provo.novell.com` and remove `staging` from the name.

In particular, you need to change the following:

- ♦ Any fully qualified DNS names from the staging name to the production name (DNSName elements in the file)
- ♦ The cookie domains associated with each proxy service (AuthenticationCookieDomain elements in the file)
- ♦ The URL masks in pin lists that contain fully qualified names (URLMask elements in the file)

Depending upon your naming standards, you might want to change the names of the following:

- ♦ UserInterfaceID elements (proxy service, pin list, and protected resource user interface ID's)
- ♦ Description elements (proxy service, pin list, and protected resource descriptions)
- ♦ Name (proxy service, pin list, and protected resource names)
- ♦ SubServiceID elements
- ♦ MultiHomeMasterSubserviceIDRef elements
- ♦ LogDirectoryName elements
- ♦ ProfileIDRef elements

- ♦ ProtectedResourceID elements
 - ♦ ProfileID elements (TCP Listen options name)
- 5c** (Conditional) If your Web servers in the staging area have different IP addresses and hostnames than the Web Servers in the production area, you can search and replace them in the configuration file or wait until after the import and modify them in the Administration Console.
- 6** Click **Export** and modify the proposed filename if needed.
- 7** Copy the Access Gateway configuration file to a place accessible by the target system.
- 8** Continue with [Importing the Access Gateway Configuration Data](#).

12 Importing the Access Gateway Configuration Data

- 1** Verify that the Access Gateway meets the conditions for an import:
 - ♦ The Access Gateway should not be a member of a cluster. If it is a member of a cluster, remove it from the cluster before continuing.
In the Administration Console, click **Devices > Access Gateways**, select the Access Gateway, then click **Actions > Remove from Cluster**.
You can create a cluster and add this machine to the cluster as the primary server after you have completed the import.
 - ♦ Delete reverse proxies if any configured.
In the Administration Console, click **Devices > Access Gateways > Edit > Reverse Proxies / Authentication**. In the **Reverse Proxy List**, select **Name**, then click **Delete**. Update the Access Gateway and the Identity Server.
- 2** Click **Access Gateways > [Name of Access Gateway] > Configuration > Import**.
- 3** Browse to the location of the configuration file, select the file, enter the password if you specified while exporting the configuration, then click **OK**.
- 4** When the configuration import has finished, verify the configuration for your reverse proxies.
 - 4a** Click **Access Gateways > Edit > [Name of Reverse Proxy]**.
 - 4b** Verify the listening address.
This is important if your Access Gateway has multiple network adapters. By default, the IP address of eth0 is always selected as the listening address.
 - 4c** Verify the certificates assigned to the reverse proxy.
The Subject Name of the certificate should match the published DNS name of the primary proxy service in the **Proxy Service List**.
 - 4d** Verify the Web Server configuration. In the **Proxy Service List**, click the **Web Server Addresses** link. Check the following values:
 - ♦ **Web Server Host Name:** If this name has a staging prefix or suffix, remove it.
 - ♦ **IP addresses in the Web Server List:** If the IP addresses in the production area are different from the IP addresses in the staging area, modify the IP addresses to match the production area.
 - ♦ **Certificates:** If you have configured SSL or mutual SSL between the proxy service and the Web servers, configure the **Web Server Trusted Root** and **SSL Mutual Certificate** options. The export and import configuration option does not export and import certificates.
 - 4e** Click **OK > OK**.
- 5** (Conditional) If you have multiple reverse proxies, repeat [Step 4](#) for each proxy service.

- 6 On the Configuration page, click **Reverse Proxy / Authentication**, then select the **Identity Server Cluster** configuration.
- 7 If you have multiple reverse proxies, verify that the Reverse Proxy value in the **Embedded Service Provider** section is the reverse proxy you want to use for authentication, then click **OK** twice.
- 8 Click **Access Gateways > Update**.
- 9 Click **Identity Servers > Update**.
If your Identity Server does not prompt you for an update, complete the following steps to trigger the update:
 - 9a In the Administration Console, click **Devices > Access Gateways > Edit > Reverse Proxy / Authentication**.
 - 9b Set the **Identity Server Cluster** field to **None**, then click **OK**.
 - 9c Click **Reverse Proxy / Authentication**.
 - 9d Set the **Identity Server Cluster** field to the correct value, then click **OK**.
 - 9e Update the Access Gateway.
 - 9f Update the Identity Server.
- 10 Configure the keystores for the Access Gateway.
If you have configured the Access Gateway for SSL between the Identity Server and the Access Gateway and between the Access Gateway and the browsers, verify that the trust stores and the keystores contain the correct certificates.
 - 10a In the Administration Console, click **Security > Certificates**.
 - 10b Find the certificate for the Access Gateway.
The subject name of this certificate should match the DNS name of the Access Gateway. If this certificate is not in the list, you need to create it or import it.
This certificate should be in use by the ESP Mutual SSL and Proxy Key Store of the Access Gateway.
 - 10c If the certificate is not in use by the required keystores, select the certificate, then click **Actions > Add Certificate to Keystores**.
 - 10d Click the **Select Keystore** icon, select **ESP Mutual SSL** and **Proxy Key Store of the Access Gateway**, then click **OK** twice.
- 11 Configure the trust stores for the Access Gateway.
 - 11a In the Administration Console, click **Security > Certificates > Trusted Roots**.
The trusted root certificate of the CA that signed the Access Gateway certificate needs to be in the NIDP-truststore.
The trusted root certificate of the CA that signed the Identity Server certificate, needs to be in the ESP Trust Store of the Access Gateway.
 - 11b If you need to add a trusted root to a trust store, select the trusted root, click **Add Trusted Roots to Trust Stores**.
 - 11c Click the **Trust Store** icon, select the required trust store, then click **OK** twice.
- 12 If you made any keystore or trust store modifications, update the Access Gateway and the Identity Server.
- 13 (Optional) Create a cluster configuration and add this server as the primary server.

13 A Case Study: Moving Access Manager to Another Environment

This section explains how to use the Code Promotion feature when you want to promote the configuration data from a staging environment to a production environment.

Let us assume that you have a configured Access Manager 4.0 setup in a staging environment. Administration Console and other devices are installed. You have set up a new Access Manager 4.0 production environment with the Administration Console installed. Other devices may not be installed on the production environment at this point.

Perform the following steps to promote configurations:

- 1 Enable the Code promotion feature in staging Access Manager and production Access Manager environments.

For more information about how to enable Code Promotion, see [Section 7, “Enabling Code Promotion,” on page 5](#).

- 2 On the staging environment, log in to the Administration Console and go to **Access Manager > Code Promotion**.

- 3 Click **Export Configuration** and export the configuration data.

For more information about how to export the configuration data, see [Section 8, “Exporting the Configuration Data by Using Code Promotion,” on page 5](#).

- 4 On the production environment, log in to the Administration Console and go to **Access Manager > Code Promotion**.

- 5 Click **Import Configuration** and import the configuration data you have exported from the staging environment.

For more information about how to import the configuration data, see [Section 9, “Importing the Configuration Data by Using Code Promotion,” on page 7](#).

- 6 Perform tasks required to get the Identity Server clusters in the working state.

For more information, see [Section 10, “Post-Import Configuration Tasks,” on page 9](#).

- 7 Install Identity Servers and add them to the Identity Server cluster.

For more information about how to install the Identity Server, see [“Installing the Identity Servers”](#) in the *NetIQ Access Manager 4.0 Installation Guide*

For more information about how to assign an Identity Server to a cluster configuration, see [“Assigning an Identity Server to a Cluster Configuration”](#) in the *NetIQ Access Manager 4.0 Identity Server Guide*.

- 8 Install the Access Gateway. You can export and import the Access Gateway configuration if the Access Gateway is not in a cluster.

For more information about how to export and import the Access Gateway configuration data, see [Section 11, “Exporting the Access Gateway Configuration Data,” on page 10](#) and [Section 12, “Importing the Access Gateway Configuration Data,” on page 11](#).

14 Troubleshooting

Importing Configuration Fails

Explanation: While importing the configuration data, the Import Configuration wizard displays the Configuration Import Failed message.

Action: See the details of the failure the Administration Console tomcat logs at the following location:

Linux: /opt/novell/nam/adminconsole/logs/catalina.out

Windows: C:\Program Files(x86)\Novell\Tomcat\log\stderr.log

Collect the error details and contact the Technical Support team.

To restore your system, go to **Access Manager > Code Promotion**. You will find the backup file that was created as part of import. Download the file and then click **Import Configuration** on the same page. Re-import this backup configuration to restore to the previous configuration.

15 Legal Notice

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.

© 2013 NetIQ Corporation and its affiliates. 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.

Access Manager, ActiveAudit, ActiveView, Aegis, AppManager, Change Administrator, Change Guardian, Cloud Manager, 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, PlateSpin,

PlateSpin Recon, Privileged User Manager, 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 affiliates 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.

DRAFT