Quick Start

Access Manager 3.2 SP2

June 2013

Legal Notice

Contents

About This Guide

This guide is designed to help you get a basic Access Manager system installed and configured. It contains the following:

Audience

This guide is intended for Access Manager administrators who are new to the product.

It is assumed that you have the knowledge of evolving Internet protocols, such as:

- Extensible Markup Language (XML)
- Simple Object Access Protocol (SOAP)
- Security Assertion Markup Language (SAML)
- Public Key Infrastructure (PKI) digital signature concepts and Internet security
- Secure Socket Layer/Transport Layer Security (SSL/TLS)
- Hypertext Transfer Protocol (HTTP and HTTPS)
- Uniform Resource Identifiers (URIs)
- Domain Name System (DNS)
- Web Services Description Language (WSDL)

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the *Access Manager Quick Start Guide*, visit the Novell Access Manager Documentation Web site (http://www.novell.com/documentation/novellaccessmanager31).

Additional Documentation

- *NetIQ Access Manager 3.2 SP2 Installation Guide*

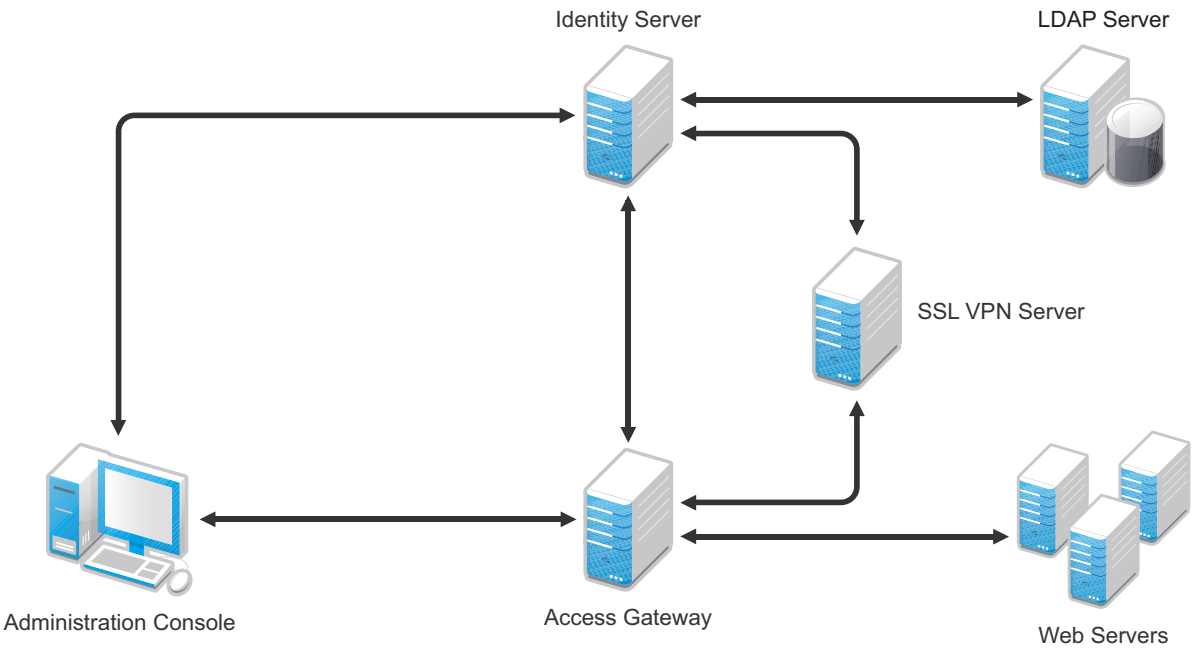
- *NetIQ Access Manager 3.2 SP2 Setup Guide*
- *NetIQ Access Manager 3.2 SP2 Administration Console Guide*
- *NetIQ Access Manager 3.2 SP2 Policy Guide*
- *NetIQ Access Manager 3.2 SP2 Identity Server Guide*
- *NetIQ Access Manager 3.2 SP2 Access Gateway Guide*
- *NetIQ Access Manager 3.2 SP2 SSL VPN Server Guide*
- *NetIQ Access Manager 3.2 SP2 J2EE Agent Guide*

NOTE: Contact namsdk@netiq.com for any query related to Access Manager SDK.

1 Installing Access Manager Components

A basic Access Manager installation has three Access Manager components (an Administration Console, an Identity Server, and an Access Gateway), an LDAP server, and Web servers with applications and data. Figure 1-1 illustrates a setup where these components are installed on separate machines.

Figure 1-1 *Basic Installation*



The Administration Console must be installed first. The other components can then be installed in any order.The SSL VPN server can be installed so that it communicates with the Identity Server or with the Access Gateway for authentication credentials.

1.1 System Requirements

Review the following sections to ensure that your machines or virtual images meet the installation prerequisites:

- "Administration Console Requirements" in the *NetIQ Access Manager 3.2 SP2 Installation Guide*
- "Identity Server Requirements" in the *NetIQ Access Manager 3.2 SP2 Installation Guide*
- "Access Gateway Requirements" in the *NetIQ Access Manager 3.2 SP2 Installation Guide*
- "SSL VPN Requirements" in the *NetIQ Access Manager 3.2 SP2 Installation Guide*

1.2 Administration Console

What you need to know	• The username and password you want to use for the Access Manager administrator. • This is your first installation of an Administration Console, so answer Yes for a primary installation, when prompted. • You can create a failover environment by installing more than one Administration Console. For more information, see "Clustering and Fault Tolerance" in the *NetIQ Access Manager 3.2 SP2 Setup Guide*.
For more information	See "Installing the Access Manager Administration Console" in the *NetIQ Access Manager 3.2 SP2 Installation Guide*.

1.2.1 Linux Administration Console

1. Download the `tar.gz` file, extract it, and use `install.sh` to start the installation.

   For software download instructions, see the "Novell Access Manager Readme" (http://www.novell.com/documentation/novellaccessmanager31/accessmanager_readme/data/accessmanager_readme.html).
2. At the Installation menu, select 1, then follow the prompts.
3. Answer Yes to the primary installation prompt.

1.2.2 Windows Administration Console

1. Download the Windows file and execute it.

   For software download instructions, see the "Novell Access Manager Readme" (http://www.novell.com/documentation/novellaccessmanager31/accessmanager_readme/data/accessmanager_readme.html).
2. Select to install the *Novell Access Manager Administration* component.
3. Answer Yes to the primary installation prompt.

1.3 Identity Server

The Identity Server can be installed on its own machine or with the Administration Console.

What you need to know	◆ Username and password of the Access Manager administrator. ◆ (Conditional) IP address of the Administration Console if it is installed on a separate machine
For more information	See "Installing the NetIQ Identity Server" in the *NetIQ Access Manager 3.2 SP2 Installation Guide*.

1.3.1 Linux Identity Server

1. Download the `tar.gz` file, extract it, and use `install.sh` to start the installation.

   For software download instructions, see the "Novell Access Manager Readme" (http://www.novell.com/documentation/novellaccessmanager31/accessmanager_readme/data/accessmanager_readme.html).
2. At the Installation menu, select 2, then follow the prompts.

1.3.2 Windows Identity Server

1. Download the Windows file and execute it.

   For software download instructions, see the "Novell Access Manager Readme" (http://www.novell.com/documentation/novellaccessmanager31/accessmanager_readme/data/accessmanager_readme.html).
2. Select to install the *Novell Identity Server* component.

1.4 Access Gateway Appliance

What you need to know	◆ Username and password of the Access Manager administrator. ◆ IP address of the Administration Console. ◆ Static IP address, hostname, and domain name to use for the Linux Access Gateway. ◆ Network settings: IP address of default gateway and the subnet mask for your network. ◆ DNS settings: the IP address of one or two DNS servers.
For more information	See "Installing the Access Gateway Appliance" in the *NetIQ Access Manager 3.2 SP2 Installation Guide*.

1. Insert the CD.
2. At the installation options page, select *Standard Installation*.
3. Accept the license agreement.
4. Select an appropriate keyboard and time zone.
5. Change the date and time to match the Identity Server.
6. Specify the following information:
   - The Network Configuration information. Specify the IP address you have selected for the Access Gateway.

- A password for the `root` user.
- The hostname and domain name for the Access Gateway and the IP address of at least one DNS server.
- The IP address, username, and password of the Administration Console.
- (Optional) If you want to install SSL VPN along with Linux Access Gateway, select *Install and enable SSL VPN Service*.

7 Click *Next* and review the installation settings page.

8 Click *Install* to continue with installation.

During installation, the machine reboots. During the reboot, some error messages are displayed. Let them scroll by and wait for the login prompt.

1.5 Access Gateway Service

What you need to know	◆ Username and password of the Access Manager administrator. ◆ IP address of the Administration Console.
For more information	See "Installing the Access Gateway Service" in the *NetIQ Access Manager 3.2 SP2 Installation Guide*.

1 Download the file to the Linux or Windows machine.

For software download instructions, see the "Novell Access Manager Readme" (http://www.novell.com/documentation/novellaccessmanager31/accessmanager_readme/data/accessmanager_readme.html).

2 (Linux) Grant execute rights to the installation program.

3 Start the installation program:

Linux: Enter the following command:

```
./<filename>
```

Windows: Double-click the executable file.

4 Accept the license agreement.

5 Specify the Administration Console information.

6 Configure the disk cache.

7 Review the installation summary.

8 If everything looks correct, select to install.

1.6 SSL VPN Server

What you need to know	◆ Username and password of the Access Manager administrator. ◆ IP address of the Administration Console.
For more information	See "Installing the SSL VPN Server" in the *NetIQ Access Manager 3.2 SP2 Installation Guide*.

You can install the SSL VPN server either as a traditional SSL VPN server (which communicates with the Access Gateway for authentication credentials) or as an ESP enabled server (which communicates with the Identity Server for authentication credentials). You can install the SSL VPN server on a separate machine, with the Identity Server, with the Administration Console, or with the Access Gateway Appliance.

- To install the SSL VPN on a separate machine, continue with this section.
- To install the SSL VPN with the Identity server, see Section 1.3, "Identity Server," on page 8.
- To install the SSL VPN with the Administration Console, see Section 1.2, "Administration Console," on page 8.
- To install the SSL VPN with the Access Gateway Appliance, see Section 1.4, "Access Gateway Appliance," on page 9

To install SSL VPN on a separate machine:

1. Download the `tar.gz` file, extract it, and use `install.sh` to start the installation.

   For software download instructions, see the "Novell Access Manager Readme" (http://www.novell.com/documentation/novellaccessmanager31/accessmanager_readme/data/accessmanager_readme.html).
2. Do one of the following:
   - Type 4 to install the traditional SSL VPN.
   - Type 3 to install the ESP-Enabled SSL VPN.
3. Press Enter, then follow the prompts.

1.7 Verifying the Installation

To verify the installation of the components:

1. Open a browser and enable browser pop-ups.
2. Log in to the Administration Console. The URL is the IP address of the Administration Console followed by `:8080/nps` for the port and the application. For example:

   ```
   http://10.10.15.10:8080/nps
   ```

   If you get an error message, restart Tomcat on the Administration Console:

   Linux: Enter the following command:

   ```
   /etc/init.d/novell-tomcat5 restart
   ```

   Windows: Enter the following commands:

   ```
   net stop Tomcat5
   ```

   ```
   net start Tomcat5
   ```

   If you still receive an error, see "Unable to Log In to the Administration Console" in the *NetIQ Access Manager 3.2 SP2 Administration Console Guide*.
3. Click *Access Manager* > *Overview*.

   Each icon should contain the number one, if your component successfully imported into the Administration Console.

   If a component has not imported, click the link to the device. If a repair import option is available, click this link. If it is not available, see "Troubleshooting Installation and Upgrade" in the *NetIQ Access Manager 3.2 SP2 Installation Guide*.

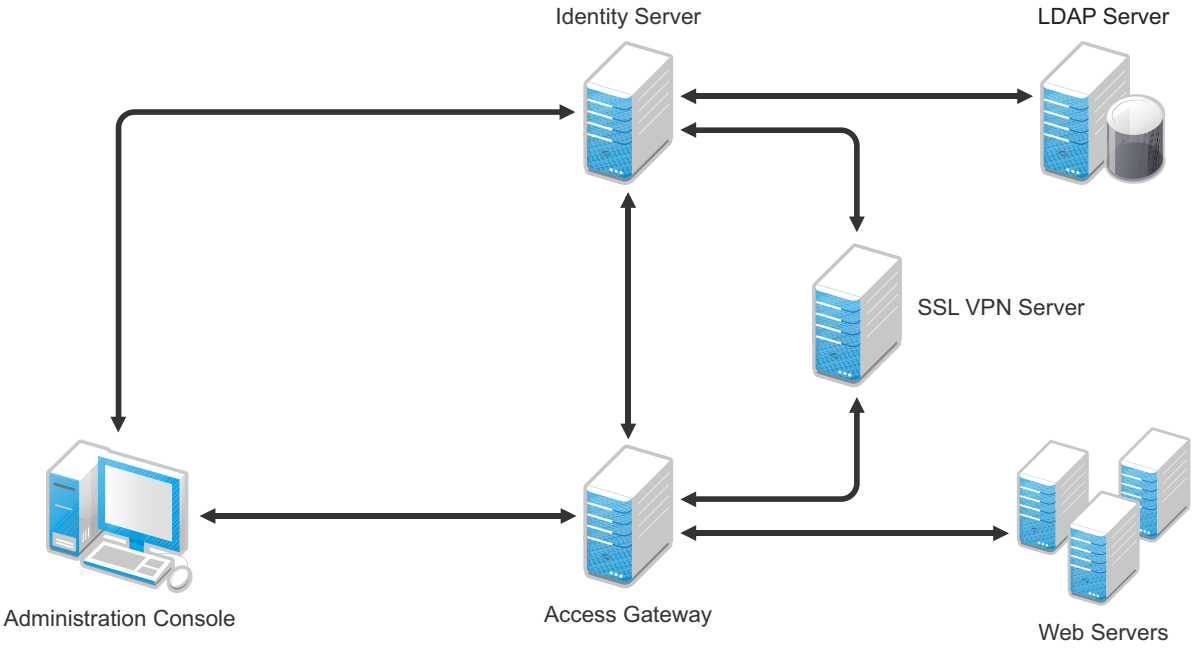
4 Before continuing with configuration, verify the following:

- Use the `ping` command to verify that the DNS names for the Identity Server and the Access Gateway are resolvable.
- Make sure time is synchronized among your components.

2 Configuring Access Manager Components

A basic configuration has three Access Manager components (an Administration Console, an Identity Server, and an Access Gateway), an LDAP server, and Web servers with applications and data. Figure 2-1 illustrates a configuration where these components are installed on separate machines.

Figure 2-1 *Modules Required for a Basic Configuration*



This section explains how to configure your system so that users in your LDAP server can log in and access a protected resource on a Web server and also access an SSL VPN application.

- Section 2.1, "New Identity Server Cluster Configuration," on page 13
- Section 2.2, "First Reverse Proxy Configuration," on page 15
- Section 2.3, "Configuring the Protected Resource for Authentication," on page 17
- Section 2.4, "Basic Configuration for SSL VPN," on page 18

2.1 New Identity Server Cluster Configuration

This section explains how to add your Identity Server to a cluster and how to configure the cluster to communicate with the LDAP server and use its authentication credentials.

Table 2-1 *Identity Server Configuration Information*

What you need to know	Example	Your Value
LDAP server information:		
DN of the administrator	`cn=admin,o=novell`	_____
Password of the administrator	`novell`	_____
IP address of the LDAP server	`10.10.10.16`	_____
DN of the user container	`ou=users,o=novell`	_____
DNS name of the Identity Server	`idpa.test.novell.com`	_____
Names you need to create:		
Identity Server cluster name	`idpa`	_____
User store name	`User Store`	_____
Replica name	`User Store Replica`	_____
Alias certificate name	`UserStoreRoot`	_____
Organization information for the Identity Server cluster:		
Name	`Access Manager`	_____
Display name	`Access Manager 3`	_____
URL	`idpa.am.novell.com`	_____

For more information, see "Creating a Basic Identity Server Configuration" in the *NetIQ Access Manager 3.2 SP2 Setup Guide*.

1. In the Administration Console, click *Devices* > *Identity Servers*.
2. Click *New Cluster*.
3. Specify a name such as `idpa`, select your Identity Server, then click *OK*.

   In Table 2-1, `idpa` is the Identity Server cluster name you created.
4. Configure the Base URL of the Identity Server, using the DNS name of the Identity Server:

   `http://idpa.test.novell.com:8080/nidp`

   In Table 2-1, this is the DNS name of the Identity Server with a port and `/nipd`.
5. Click *Next*, then configure the organization information.

   Name: `Access Manager`

   Display name: `Access Manager 3`

   URL: `idpa.am.novell.com`

   In Table 2-1, these three fields are the organization information you created for the Identity Server cluster.
6. Click *Next*, then configure the user store:

   Name: `User Store`

In Table 2-1, `User Store` is the sample name for the user store.

Admin name: `cn=admin,o=novell`

In Table 2-1, this is the sample DN of the administrator for the LDAP server.

Admin password: `novell`

Confirm password: `novell`

In Table 2-1, these fields are the sample password for the administrator of the LDAP server.

Directory Type: Select a type from the drop-down menu.

7 In the *Server replicas* section, click *New*, then fill in the following fields:

Name: `User Store Replica`

In Table 2-1, `User Store Replica` is the sample name for the replica

IP Address: `10.10.10.16`

In Table 2-1, this is the sample IP address of the LDAP server.

Use secure LDAP connections: Select this option.

Auto import trusted root: Click this link, follow the prompts, and specify `UserStoreRoot` for the alias.

In Table 2-1, `UserStoreRoot` is the sample alias certificate name.

8 Click *OK*, then make sure the Validation Status of the replica displays a green check mark. If the check mark is red, you have a configuration error:

- Check the distinguished name of the admin user, the password, and the IP address of the replica.
- Check for network communication problems between the Identity Server and the LDAP server.

9 In the *Search Contexts* section, click *New*, then specify the following:

Search context: `ou=users,o=novell`

In Table 2-1, this is the sample DN of the user container.

Scope: `Subtree`

10 Click *OK* > *Finish*, then restart Tomcat as prompted.

11 Wait for the health status of the Identity Server to turn green, then verify the configuration:

11a Enter the Base URL of the Identity Server in a browser.

```
http://idpa.test.novell.com:8080/nidp
```

11b Log in using the credentials of a user in the LDAP server.

The user portal appears.

If the URL returns an error rather than displaying a login page, verify the following:

- The browser machine can resolve the DNS name of the Identity Server.
- The browser machine can access to the port.

2.2 First Reverse Proxy Configuration

This section explains how to create a reverse proxy to protect the name and IP address of your Web server from being exposed to users. Section 2.3, “Configuring the Protected Resource for Authentication,” on page 17 builds on this configuration and explains how to require authentication to gain access to the Web server.

Table 2-2 *Access Gateway Configuration Information*

What You Need To Know	Example	Your Value
Name of the Identity Server cluster	`idpa`	_____
DNS name of the Access Gateway	`lag.test.novell.com`	_____
Web server information		
IP address	`10.10.16.16`	_____
DNS name	`digital.test.novell.com`	_____
Names you need to create		
Reverse proxy name	`DigitalAirlines`	_____
Proxy service name	`DA`	_____
Protected resource name	`everything`	_____

For more information, see "Configuring the Access Gateway" in the *NetIQ Access Manager 3.2 SP2 Setup Guide*.

1. In the Administration Console, click *Devices* > *Access Gateways*.
2. Click *Edit*, then click *Reverse Proxy/Authentication*.
3. Configure a reverse proxy:
   - In the *Authentication Settings* section, select `idpa` from the drop-down list.

     In Table 2-2, this is the sample name of the Identity Server cluster.
   - In the *Reverse Proxy* section, click *New*, specify `DigitalAirlines`, then click *OK*.

     In Table 2-2, `DigitalAirlines` is the sample reverse proxy name.
4. To configure a proxy service, click *New* in the Proxy Service section, then fill in the following fields:

   Proxy Service Name: `DA`

   In Table 2-2, `DA` is the sample proxy service name.

   Published DNS Name: `lag.test.novell.com`

   In Table 2-2, this is the sample DNS name of the Access Gateway.

   Web Server IP Address: `10.10.16.16`

   In Table 2-2, this is the sample IP address of the Web server.

   Host Header: Select the *Web Server Host Name* from the drop-down list.

   Web Server Host Name: `digital.test.novell.com`

   In Table 2-2, this is the sample DNS name of the Web server.
5. Click *OK*, then configure a protected resource.
   - Click the *Protected Resource* tab.
   - In the *Protected Resource* section, click *New*, then specify `everything`.

     In Table 2-2, `everything` is the sample protected resource name.
   - In the *URL Path* section, examine the path. It should be set to /* to match everything on the Web server.
6. Click *OK* to save the configuration.

7 Click the *Access Gateways* task, then click *Update*.

Wait for the health status to turn green. If it doesn't turn green, click the *Health* icon to discover the cause.

- If the Access Gateway cannot connect to the Web server, verify the IP address of the Web server.
- Use the `ping` command to verify that the Access Gateway can communicate with the Web server and the Identity Server.
- Verify that the Access Gateway can resolve the DNS name of the Identity Server.
- For other problems, see "Monitoring the Health of an Access Gateway" in the *NetIQ Access Manager 3.2 SP2 Access Gateway Guide*.

8 Click the *Identity Servers* task, then click *Update*.

9 To test that the Access Gateway is protecting the Web server, open a browser and enter the following URL:

```
http://lag.test.novell.com:80/
```

The first page of the Web server is displayed. If you get an error, verify the following:

- Check the times on the Access Gateway and the Identity Server. Their times need to be synchronized.
- Verify that the browser machine can resolve the DNS name of the Access Gateway.

2.3 Configuring the Protected Resource for Authentication

This section explains how to configure the Access Gateway so that users are prompted to log in when accessing the protected resource.

1 To return to the protected resource, click *Devices* > *Access Gateways* > *Edit* > *DigitalAirlines* > *DA* > *Protected Resources* > *everything*.

2 For the *Contract* option, select *Name/Password Form* from the drop-down list.

If the list is empty, you have not selected an Identity Server cluster configuration for the Access Gateway. See Step 3 on page 16.

3 Click *OK* to save the configuration.

4 Click the *Access Gateways* task, then click *Update*.

5 To test that accessing the resource now requires authentication, open a browser, then enter the URL to your protected resource:

```
http://lag.test.novell.com:80/
```

When you are prompted for login credentials, use a name and a password from a user on the LDAP server.

If you receive an error, verify the following:

- The Identity Server can resolve the DNS name of the Access Gateway.
- The Access Gateway can resolve the DNS name of the Identity Server.
- Time is synchronized between the Identity Server and the Access Gateway.

For other problems, see "General Authentication Troubleshooting Tips" in the *NetIQ Access Manager 3.2 SP2 Identity Server Guide*.

2.4 Basic Configuration for SSL VPN

This section explains how to create a basic configuration for the SSL VPN server.

- If you have installed the ESP-enabled SSL VPN, continue with Section 2.4.1, "Configuring Authentication for ESP-Enabled SSL VPN," on page 18.
- If you have installed the traditional SSL VPN, continue with Section 2.4.2, "Accelerating the Traditional SSL VPN Server," on page 19.

2.4.1 Configuring Authentication for ESP-Enabled SSL VPN

This section explains how to establish a trust relationship between the Identity Server and the Embedded Service Provider of the SSL VPN server.

Table 2-3 *ESP-Enabled SSL VPN Configuration Information*

What You Need To Know	Example	Your Value
Name of the Identity Server cluster	`idpa`	_____
DNS name of the SSL VPN machine	`sslvpn.test.novell.com`	_____
A certificate where the subject name matches the DNS name of the SSL VPN machine	For information on how to create such a certificate, see "Creating a Locally Signed Certificate" in the *NetIQ Access Manager 3.2 SP2 Administration Console Guide*.	
For more information, see "Configuring Authentication for the ESP-Enabled NetIQ SSL VPN" in the *NetIQ Access Manager 3.2 SP2 Setup Guide*.		

1. In the Administration Console, click *Devices* > *SSL VPNs* > *Edit*.
2. Select *Authentication Configuration* from the *Gateway Configuration* section.
3. Fill in the following fields:

   Identity Server Cluster: `idpa`

   In Table 2-3, this is the sample name of the Identity Server cluster.

   Authentication Contract: Select *Any Contract*.

   Embedded Service Provider Base URL: `https:sslvpn.test:8443/sslvpn`

   In Table 2-3, this is the DNS name for the SSL VPN server. It assumes you want to use HTTPS. If you want to use HTTP, select `http` and make sure the port is 8080.

   Redirect Requests from Non-Secure Port to Secure Port: Select this option if you are using HTTPS.

   SSL VPN Certificate: Click the icon and select the certificate that has a subject name that matches the DNS name of the SSL VPN server.

   Embedded Service Provider Certificate: Click the icon and select the certificate that has a subject name that matches the DNS name of the SSL VPN server.
4. Restart the Tomcat server when prompted.
5. Click *OK,* then click *Update* on the Configuration page.
6. Click *Update* on the Identity Server Configuration page.

2.4.2 Accelerating the Traditional SSL VPN Server

This section explains how to accelerate the traditional SSL VPN server in a path-based multi-homing configuration.

1. In the Administration Console, click *Devices* > *Access Gateways*, then click *Edit* > *[Name of Reverse Proxy]*.
2. In the *Proxy Service List*, click *New*, then provide the following values:

   Proxy Service Name: Specify *sslvpn*.

   Multi-Homing Type: Select *Path-Based*.

   Path: Specify */sslvpn*.

   Web Server IP Address: Specify the IP address of SSL VPN server.

   Host Header: If your SSL VPN server has a DNS name, select *Web Server Host Name*. Otherwise, select *Forward Received Host Name*.

   Web Server Host Name: Specify the DNS name of the SSL VPN server if you selected *Web Server Host Name* for the *Host Header* option.
3. Click *OK*.
4. In the *Proxy Service List*, click *sslvpn* > *Web Servers*.
5. Change the *Connect Port* from *80* to *8080*, then click *OK*.
6. In the *Proxy Service List*, select the *sslvpn*.
7. In the *Path List*, select the *sslvpn* path, then click *Enable SSL VPN*.
8. Fill in the following fields:

   Policy Container: Select *Master_Container*.

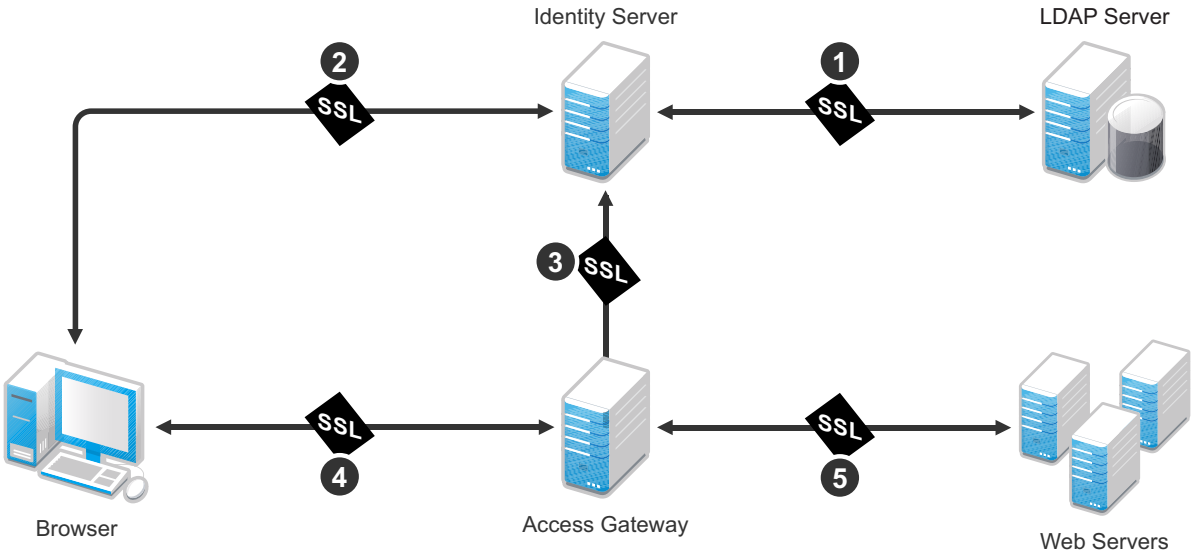
   Policy: Select *Create SSL VPN Default Policy*. In the Policy List window, click *Apply Changes*, then click *Close*.

   Name: Select *Create SSL VPN Default Protected Resource*.
9. Click *OK* twice, then update the Access Gateway and the SSL VPN server.

3 Configuring SSL

Access Manager has five communication channels that can be configured for SSL. Figure 3-1 illustrates these channels.

Figure 3-1 *Potential SSL Communication Channels*



The channels need to be configured according to their numeric values. You need to configure SSL between the Identity Server and the LDAP server before you configure SSL between the Identity Server and the browsers. The Identity Server must be configured for SSL before you configure the channel between the Access Gateway and the Identity Server for SSL.

The following procedures assume that you want to set up a new system using certificates created by the Access Manager Certificate Authority. To modify an existing system to use SSL, see "Enabling SSL Communication" in the *NetIQ Access Manager 3.2 SP2 Setup Guide*. To use certificates signed by an external CA, see "Using Externally Signed Certificates" in the *NetIQ Access Manager 3.2 SP2 Setup Guide*.

This section describes the following tasks:

- Section 3.1, "Configuring a New Identity Server Cluster with SSL," on page 21
- Section 3.2, "Configuring a New Access Gateway for SSL," on page 24

3.1 Configuring a New Identity Server Cluster with SSL

This section explains how to add your Identity Server to a cluster, how to configure the cluster to use SSL, and how to configure the cluster to communicate with the LDAP server so users can access their authentication credentials.

What You Need to Know	Example	Your Value
LDAP server information:		
DN of the administrator	`cn=admin,o=novell`	_____
Password of the administrator	`novell`	_____
IP address of the LDAP server	`10.10.10.16`	_____
DN of the user container	`ou=users,o=novell`	_____
DNS name of the Identity Server	`idpa.test.novell.com`	_____
Certificate name	`idpa_test`	_____
Certificate subject fields:		
Common name	`idpa.test.novell.com`	_____
Organizational unit	`o=novell`	_____
Organization	`test`	_____
City or town	`Provo`	_____
State or province	`Utah`	_____
Country	`US`	_____
Names you need to create:		
Identity Server cluster name	`idpa`	_____
User store name	`User Store`	_____
Replica name	`User Store Replica`	_____
Alias certificate name	`UserStoreRoot`	_____
Organization information for the Identity Server cluster:		
Name	`Access Manager`	_____
Display name	`Access Manager 3`	_____
URL	`idpa.am.novell.com`	_____

For more information, see "Creating a Basic Identity Server Configuration" in the *NetIQ Access Manager 3.2 SP2 Setup Guide*.

1. In the Administration Console, click *Devices* > *Identity Servers*.
2. Click *New Cluster*.
3. Specify a name such as `idpa`, select your Identity Server, then click *OK*.
4. Configure the Base URL of the Identity Server, using the DNS name of the Identity Server:

   `https://idpa.test.novell.com:8443/nidp`
5. On the *SSL Certificate* line, click the *Select Certificate* icon, then click *Replace*.
6. In the *Replace* box, click the *Select Certificate* icon.

7 On the Certificates page, click *New*.

8 Select *Use local certificate authority*.

9 Fill in the following fields:

Certificate name: `idpa_test`

Signature algorithm: Accept the default.

Valid from: Accept the default.

Months valid: Accept the default.

Key size: Accept the default.

10 Click the *Edit* icon on the *Subject* line.

11 Fill in the following fields:

Common name: `idpa.test.novell.com`

Organizational unit: `o=novell`

Organization: `test`

City or town: `Provo`

State or province: `Utah`

Country: `US`

12 Click *OK* twice.

13 Verify that the new certificate is selected, then click *OK*.

14 In the *Replace* box, click *OK*, then click *Close*.

15 To configure the organization information, click *Next*, then fill in the following fields:

Name: `Access Manager`

Display name: `Access Manager 3`

URL: `idpa.am.novell.com`

16 Click *Next*, then configure the user store:

Name: `User Store`

Admin name: `cn=admin,o=novell`

Admin password: `novell`

Confirm password: `novell`

Directory Type: Select a type from the drop-down menu.

17 In the *Server replicas* section, click *New*, then fill in the following fields:

Name: `User Store Replica`

IP Address: `10.10.10.16`

Use secure LDAP connections: Select this option.

Auto import trusted root: Click this link, follow the prompts, and specify `UserStoreRoot` for the alias.

18 Click *OK*, then make sure the Validation Status of the replica displays a green check mark. If the check mark is red, you have a configuration error:

- Check the distinguished name of the admin user, the password, and the IP address of the replica.
- Check for network communication problems between the Identity Server and the LDAP server.

19 In the *Search Contexts* section, click *New*, then specify the following:

Search context: `ou=users,o=novell`

Scope: `Subtree`

20 Click *OK*, click *Finish*, then restart Tomcat as prompted.

21 Wait for the health status of the Identity Server to turn green, then verify the configuration:

21a Enter the Base URL of the Identity Server in a browser.

```
https://idpa.test.novell.com:8443/nidp
```

21b Log in using the credentials of a user in the LDAP server.

The user portal appears.

If the URL returns an error rather than displaying a login page, verify the following:

- The browser machine can resolve the DNS name of the Identity Server.
- The browser machine can access port 8443.

3.2 Configuring a New Access Gateway for SSL

This section explains how to create a reverse proxy to protect the name and IP address of your Web server from being exposed to users, how to require SSL between the browsers and the reverse proxy, and how to require authentication to gain access to the Web server.

What You Need to Know	Example	Your Value
Name of the Identity Server cluster	`idpa`	_____
DNS name of the Access Gateway	`lag.test.novell.com`	_____
Web server information		
IP address	`10.10.16.16`	_____
DNS name	`digital.test.novell.com`	_____
Names you need to create		
Reverse proxy name	`DigitalAirlines`	_____
Proxy service name	`DA`	_____
Protected resource name	`everything`	_____

For more information, see "Configuring the Access Gateway" in the *NetIQ Access Manager 3.2 SP2 Setup Guide*.

1 In the Administration Console, click the *Access Gateways* task.

2 Click *Edit*, then click *Reverse Proxy/Authentication*.

3 Configure a reverse proxy:

- In the *Authentication Settings* section, select `idpa` from the drop-down list.
- In the *Reverse Proxy* section, click *New*, specify `DigitalAirlines`, then click *OK*.

4 To configure a proxy service, click *New* in the *Proxy Service* section, then fill in the following fields:

Proxy Service Name: `DA`

Published DNS Name: `lag.test.novell.com`

Web Server IP Address: `10.10.16.16`

Host Header: Select the *Web Server Host Name* from the drop-down list.

Web Server Host Name: `digital.test.novell.com`

5 On the Reverse Proxy page, configure a protected resource.

5a In the *Proxy Service List* section, click the name of proxy service (DA), then click the *Protected Resources* tab.

5b In the *Protected Resource List* section, click *New*, specify `everything`, then click *OK*.

5c For the contract, select *Secure Name/Password - Form*.

5d In the *URL Path* section, examine the path. It should be set to /* to match everything on the Web server.

5e Click *OK* twice.

6 On the Reverse Proxy page, enable SSL:

6a Select *Enable SSL with Embedded Service Provider*.

6b Select *Enable SSL between Browser and Access Gateway*.

6c Select *Redirect Requests from Non-Secure Port to Secure Port*.

6d Select *Auto-generate Key*, then click *OK*.

6e Ensure that the certificate is selected, then click *OK*.

7 Click *OK* until you return to the Access Gateway page.

8 On the Access Gateways page, click *Update*.

Wait for the health status to turn green. If it doesn't turn green, click the *Health* icon to discover the cause.

- If the Access Gateway cannot connect to the Web server, verify the IP address of the Web server.
- Use the `ping` command to verify that the Access Gateway can communicate with the Web server and the Identity Server.
- Verify that the Access Gateway can resolve the DNS name of the Identity Server.
- For other problems, see "General Authentication Troubleshooting Tips" in the *NetIQ Access Manager 3.2 SP2 Identity Server Guide*.

9 Click the *Identity Servers* task, then click *Update*.

10 To test that the Access Gateway is protecting the Web server, open a browser and enter the following URL:

```
https://lag.test.novell.com:443/
```

The first page of the Web server is displayed. If you get an error, verify the following:

- Check the times on the Access Gateway and the Identity Server. Their times need to be synchronized.
- Verify that the browser machine can resolve the DNS name of the Access Gateway.

4 Configuring Access Manager Components In A Multi-Tenant Network

4.1 Introduction

This document provides information about deploying Access Manager components in a multi-tenant or service provider environment, where Network Address Translation (NAT) protocol is used as one of the network configuration.

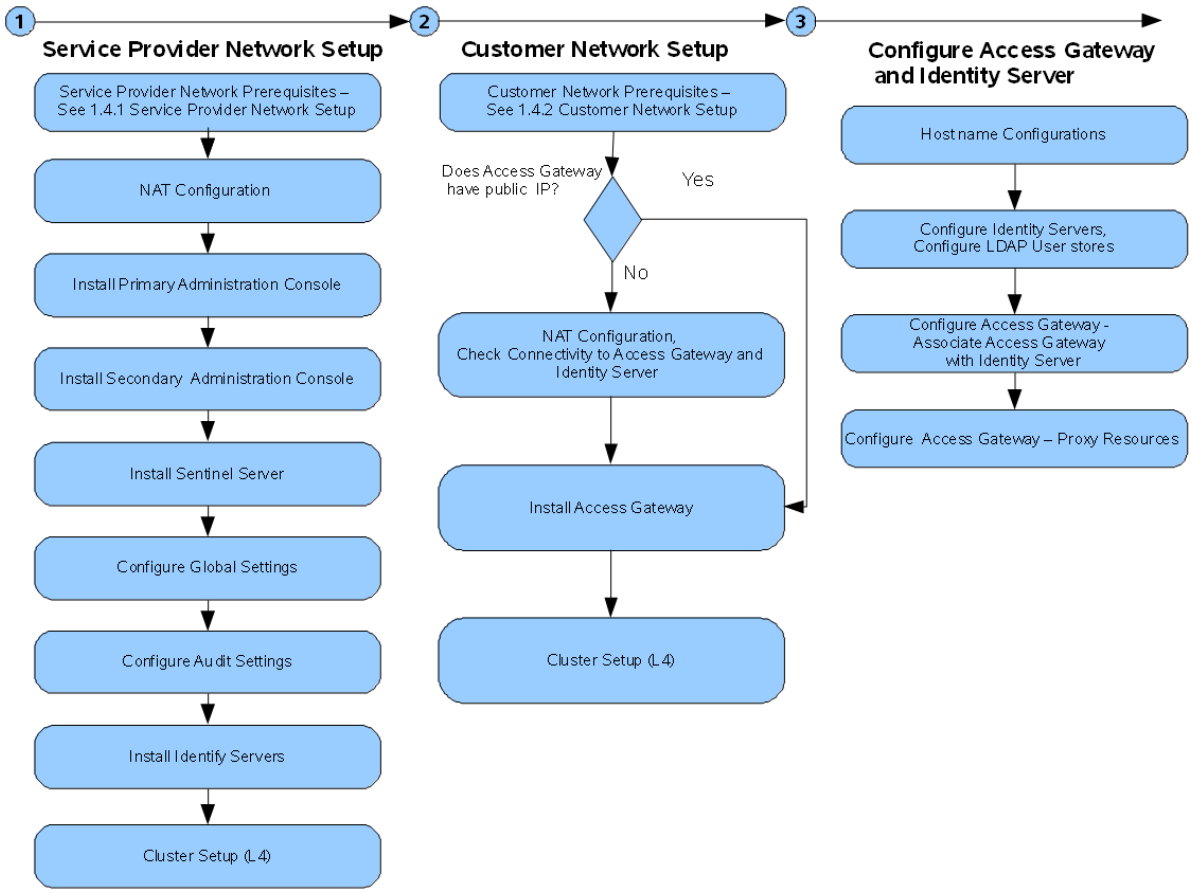
4.2 System Requirements

For more information on Installation requirements see *Novell Access Manager 3.1 SP2 Installation Guide* (http://www.novell.com/documentation/novellaccessmanager31/installation/?page=/documentation/novellaccessmanager31/installation/data/b6qs6jy.html)

4.3 Network Setup Flow Chart

The Network setup flow chart provides information about installing Access Manager components and configuring NAT in a multi-tenant or service provider network.

Figure 4-1 *Network Setup Flow Chart*



4.4 Network Prerequisites

The network prerequisites consists of both service provider and customer network setup.

- Section 4.4.1, “Service Provider Network Setup,” on page 28
- Section 4.4.2, “Customer Network Setup,” on page 29

4.4.1 Service Provider Network Setup

- ❒ Obtain Static IP addresses for Administration Console, Identity Server and Sentinel. If the IP address of the machine changes, the Access Manager component or components on that machine cannot start.
- ❒ Install OS, configure Network Time Protocol (NTP) server and check connectivity.
- ❒ Network time protocol server, which provides accurate time to the machines on your network. Time must be synchronized within one minute among the components, or the security features of the product disrupt the communication processes. You can install your own or use a publicly available server such as pool.ntp.org.

IMPORTANT: If time is not synchronized, users cannot authenticate and access resources and data corruption can also happen in user stores.

- ❒ An L4 switch if you are going to configure load balancing. This can be hardware or software (for example, a Linux machine running Linux Virtual Services).
- ❒ There should be IP connectivity between different Access Manager components Since the components can be in different private networks, the connectivity can be achieved through NAT, VPNs or combination of both.

4.4.2 Customer Network Setup

- ❒ A server configured with an LDAP directory (eDirectory 8.7 or later, Sun ONE, or Active Directory) that contains your system users. The Identity Server uses the LDAP directory to authenticate users to the system.
- ❒ Domain name server, which resolves DNS names to IP addresses and which has reverse lookups enabled.

  Access Manager devices know each other by their IP addresses, and some requests require them to match an IP address with the device's DNS name. Without reverse lookups enabled, these requests fail. In particular, Identity Servers perform reverse lookups to their user stores. If reverse lookups are not available, host table entries can be used.
- ❒ Obtain Static IP addresses for Administration Console, Identity Server and Sentinel. If the IP address of the machine changes, the Access Manager component or components on that machine cannot start.
- ❒ There should be IP connectivity between different Access Manager components Since the components can be in different private networks, the connectivity can be achieved through NAT, VPNs or combination of both.

5 Installing Access Manager Components in NAT Environments

The following sections describe the procedure to configure NAT:

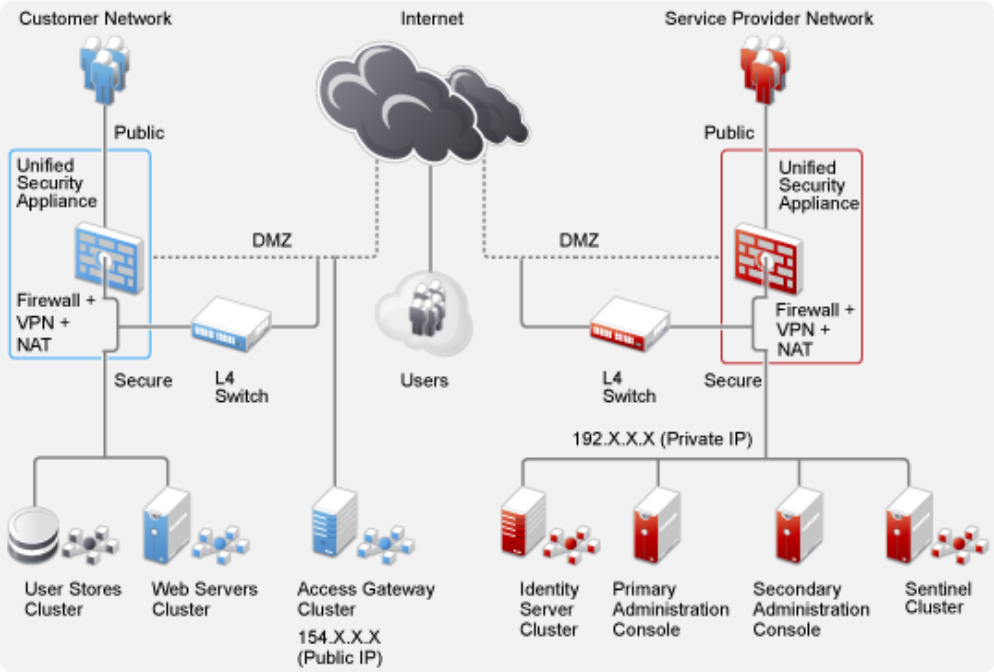
5.1 Deployment Scenarios

The NAT machine configuration supports the following deployment scenarios:

5.1.1 Administration Console in Private Network Behind NAT Configuration and Access Gateway in Public Network

This deployment scenario consists of a demilitarized zone where the NAT is configured behind for Administration Console that is Administration Console in private network and Access Gateway is configured in Public network.

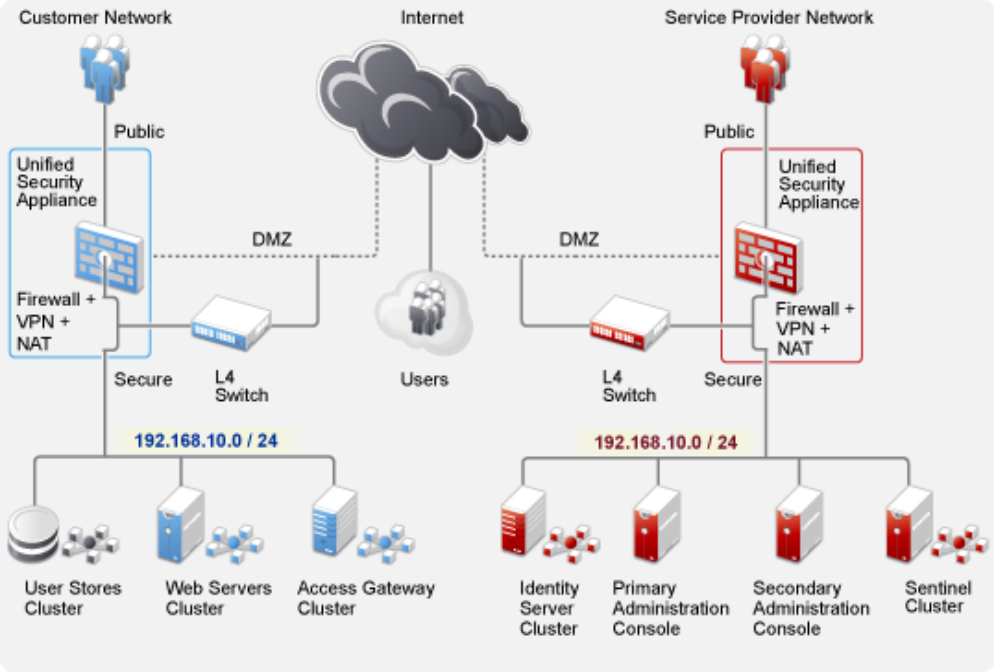
Figure 5-1 *Administration Console in Private Network and the Access Gateway in Public Network*



5.1.2 Both the Administration Console and Access Gateway IP Address Behind NAT Configuration In Conflicting Scenario

This deployment scenario consists of both the Administration Console and Access Gateway IP address behind NAT Configuration are in the conflicting scenario.

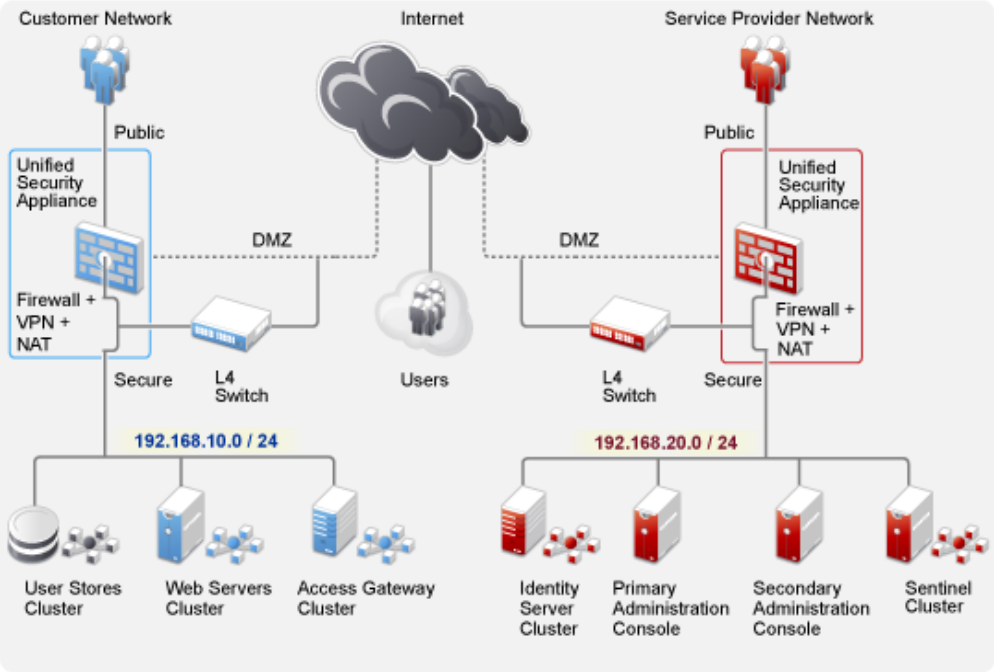
Figure 5-2 *The Administration Console and the Access Gateway IP Address in Conflicting Scenario*



5.1.3 The Administration Console is Behind NAT Configuration and the Access Gateway IP Address Through VPN Tunnel In Non-Conflicting Scenario

This deployment scenario consists of the Administration Console and Access Gateway IP addresses in the non-conflicting scenario. The Administration Console is behind NAT configuration and the Access Gateway IP Address is accessed through VPN tunnel.

Figure 5-3 *The Administration Console and the Access Gateway IP Address in Non-Conflicting Scenario*



5.2 Installing the Administration Console

1. Before installing Novell Access Manager components, check the network connectivity across these machines.
2. Verify the link latency and ensure that it is less than 100 milliseconds

   If the link latency is less than 100ms, it might lead to performance degradation.
3. Synchronize time across all the Access Manager components.

   The primary Administration Console should be configured to synchronize time with the corporate Network Time Protocol (NTP) server. The remaining machines should be configured to synchronize time with the primary Administration Console.

   3a Add the following entry to the `/etc/crontab` file on the primary Administration Console:

   ```
   */5 * * * * root sntp -P no -r <corporate NTP_Server> >/dev/null 2>&1
   ```

   3b Add the following entry to the `/etc/crontab` file of the other Access Manager machines:

   ```
   */5 * * * * root sntp -P no -r <Primary_Admin_Console_IP> >/dev/null 2>&1
   ```
4. Install the primary Administration Consoles by providing the Listening IP address for the primary Administration Console.

For more information on installing the Administration Console, see the *NetIQ Access Manager 3.2 SP2 Installation Guide*.

5 Install the secondary Administration Console and repeat the above procedures for secondary Administration Console IP address.

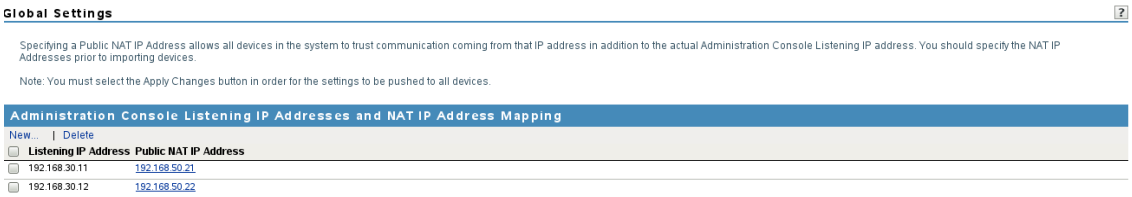
6 Continue with Section 5.3, "Configuring Global Settings," on page 35 to add both the primary and secondary Administration Consoles to the *Global Settings* configuration.

5.3 Configuring Global Settings

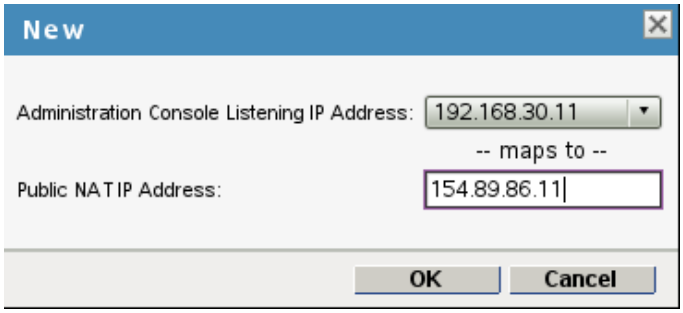
You need to map the private IP address of the Administration Console and to the public NAT IP address. You need to specify the NAT IP addresses before importing the Identity Server and the Access Gateway. You have to specify the NAT IP Addresses prior to importing devices. The devices that cannot reach the Private Administration Console IP address will use the NAT IP address.

1 Log in to the Administration Console.

2 Select *Access Manager* > *Global Settings*.



3 Click *New*.



4 Select the Administration Console Listening IP address from the drop-down lsit.

5 Specify the corresponding Public NAT IP address.

If you do not specify a Public NAT IP address or if a mapping already exists for the selected Administration Console IP address, the following message is displayed:

```
IP Address is not valid
```

6 Click *OK* to continue and apply the configuration changes.

7 Continue with Section 5.5, "Configuring Audit Server," on page 36 to configure auditing and logging.

5.4 Installing Sentinel Server

Sentinel is a security information and event management solution that receives information from many sources throughout an enterprise, standardizes it, prioritizes it and presents it to you to make threat, risk, and policy-related decisions. Sentinel automates log collection, analysis, and reporting processes to ensure that IT controls are effective supporting threat detection and audit requirements. Sentinel replaces these labor-intensive manual processes with automated, continuous monitoring of security and compliance events and IT controls.

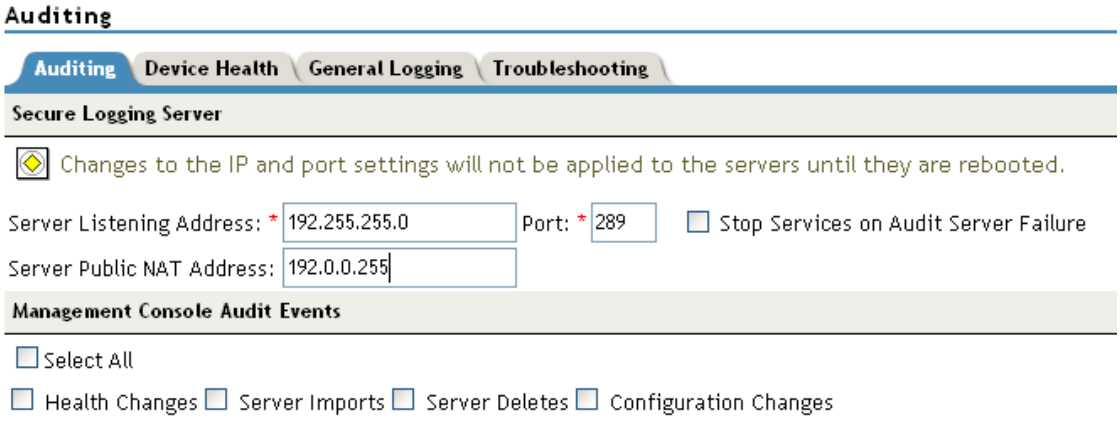
For more information on installing Sentinel Server, see Sentinel Installation Guide (http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/)

The Audit server Listening IP Address, NAT Public IP Address and Port numbers are configured in the Sentinel server. For more information on configuring the audit server, see Section 5.5, “Configuring Audit Server,” on page 36

5.5 Configuring Audit Server

The Secure Logging Server manages the flow of information to and from the auditing system. It receives incoming events and requests from the Platform Agents, logs information to the data store, monitors designated events, and provides filtering and notification services. You can configure the Secure Logging Server to automatically reset the critical system attributes according to the specified policy.

1. Log in to the Administration Console.
2. Select *Access Manager* > *Auditing* > *Novell Auditing*.



3. Fill in the following fields:

   Server Listening IP Address: Specify the private listening IP address. Specify the IP address or DNS name of the audit logging server that you want to use. By default, the system uses the primary Administration Console IP address. If you want to use a different Secure Logging Server, specify the IP address of that server.

Server Public NAT IP Address: Specify the NAT IP address of the relevant server. For example, if you want to use the Sentinel private IP address on Server Listening Address 11.0.0.124, then you need to specify the NAT IP address of the Sentinel server in Server NAT IP Address to map the private address to a public address.To use a Sentinel server or a Sentinel Log Manager server instead of Novell Audit, specify the IP address or DNS name of the Sentinel Collector.

- For more information on Sentinel, see the Sentinel 6.1 (http://www.novell.com/documentation/sentinel61/index.html).
- For more information on Sentinel Log Manager, see the Sentinel Log Manager 1.0 (http://www.novell.com/documentation/novelllogmanager10/).

Port: Specify the port that the Platform Agents use to connect to the Secure Logging Server. The default port value is 289. The Sentinel servers listens on port 1289

Stop Service on Audit Server Failure: If you enable this checkbox, then audit events are always sent to audit server. If audit server is offline or not reachable, when an audit event is generated the apache services will be shut down.

If you want to use a Sentinel server or a Sentinel Log Manager server instead of the Novell Audit server, specify the port number of your Sentinel Collector.

IMPORTANT: Whenever you change the port or IP address of the Secure Logging Server, you must update all the Access Gateways, then restart the Identity Server, Administration Console, Access Gateways, SSL VPN servers, and J2EE Agents before the configuration changes take affect.

---

4 In the *Management Console Audit Events* section, specify any or all of the following options to generate events:

Health Changes: Generates events whenever the health of server changes.

Server Imports: Generates events whenever a server is imported into the Administration Console.

Server Deletes: Generates whenever a server is deleted from the Administration Console.

Configuration Changes: Generates events whenever you change the server configuration.

Select All: Select this option to select all the audit events.

5 Click *OK*.

If you did not change the address or port of the Secure Logging Server, this completes the process. It might take up to fifteen minutes for the events you selected to start appearing in the audit files.

6 Restart all the Access Manager components imported into the Administration Console.

The Identity Server, Access Gateway, SSL VPN, and J2EE Agents do not start reporting events until they have been restarted.

5.6 Installing Identity Servers

The Identity Server facilitates authentication for all Access Manager components. This authentication is shared with internal or external service providers on behalf of the user, by means of assertions. Access Manager supports a number of authentication methods, such as name/password, RADIUS token-based authentication, X.509 digital certificates, Kerberos, and OpenID. You specify authentication methods in the contracts that you want to make available to the other components of Access Manager, such as the Access Gateway.

For more information on installing the Identity Servers, see the *NetIQ Access Manager 3.2 SP2 Installation Guide*

5.7 Configuring User Stores

User stores are LDAP directory servers to which end users authenticate. You must specify an initial user store when creating an Identity Server configuration. You use the same procedure for setting up the initial user store, adding a user store, or modifying an existing user store.

For more information on configuring the user stores, see the *NetIQ Access Manager 3.2 SP2 Identity Server Guide*

5.8 Installing Access Gateway

The Novell Access Gateway is a reverse proxy server (protected site server) that restricts access to Web-based content, portals, and Web applications that employ authentication and access control policies. It also provides single sign-on to multiple Web servers and Web applications by securely providing the credential information of authenticated users to the protected servers and applications. The Access Gateway lets you simplify, secure, and accelerate your Internet business initiatives. A typical Access Manager configuration includes an Identity Server with LDAP directories and an Access Gateway with a protected Web server.

For more information on installing Access gateway, see *NetIQ Access Manager 3.2 SP2 Installation Guide*

5.9 Configuring Access Gateway

When you are setting up the Access Gateway to protect Web resources, you create and configure reverse proxies, proxy services, and protected resources. The authentication contract, authentication procedure, Authorization policy, Identity Injection policy, and Form Fill policy are configured at the resource level so that you can enable exactly what the resource requires.

For more information on configuring the Access Gateway, see *NetIQ Access Manager 3.2 SP2 Access Gateway Guide*.

6 Troubleshooting the Access Manager Components in NAT Environemnt

The troubleshooting scenarios provides few debugging issues along with workaround solutions.

6.1 Access Gateway is Not Importing into Administration Console

1. Open `/tmp/novell_access_manager/ags_install_2010-07-12_14\:38\:35.log file.`
2. See the certificate error (For example - *invalid/expired certificate*).
3. Look for *successfully wrote:keystore message*.

To workaround this issue re-import the Access Gateway into Administration Console.

If the time is not synchronized between the Administration Console and Access Gateway, then synchronize the time and re-import.

6.2 After Importing the Access Gateway Service, the Embedded Service Provider Does not Start

This is an NAT configuration issue. After importing Access Gateway, the Access Gateway Service Embedded Service Provider does not start and an error message is displayed that the configuration information cannot be found. The status of Access Gateway is displayed in red or the configuration commands are found in pending state.

To workaround this issue:

1. Go to catalina.out xml file in Access Gateway and look for the last line which consists of configuration store details.
2. Check if the IP address of the Administration Console mentioned in this XML is reachable from the Access Gateway.

3 Configure Public NAT IP Address in *Administration Console >Global Settings*.

4 Restart jcc and esp on the Access Gateway.

6.3 Access Gateway Takes More Than Five Minutes to Complete Service Provider Refresh Command and Access Gateway Events Are Not Seen in Sentinel

The Access Gateway fails to start on Embedded Service Provider and an error message is displayed as follows: “Unable to read signing.keystore”.

1 Check the IP address in the `/etc/logevent.conf` file in the Audit Server.

2 Ensure the IP address is reachable from Access Gateway to Administration Console.

3 Check whether a health message is displayed as follows: “NAT is configured”. If not, verify the Global Settings.

4 Ensure Public NAT IP Address is configured in *Administration Console >Global Settings*, else configure and restart jcc and esp on Access Gateway.

5 Check the Audit Settings. Make sure both Private IP address and NAT IP address of Audit Server are configured.

6 Verify Global Settings and Audit Settings in the Administration Console.

6.4 The Access Gateway Service Fails to Start on the Embedded Service Provider

1 Check the jcc configure log on the Access Gateway for the *successfully wrote: signing.keystore* message.

2 Verify `/opt/novell/devman/jcc/certs/esp/<id>/signing.keystore` file exists and its size is more than 32 bytes

3 Use keyinfo script and keytool to check the certificates.

4 If any empty file exists delete it.

5 In the Administration Console, click *Auditing* > *TroubleShooting* > *Certificates*.

6 Enable the keystore device or cluster that has been deleted in the Access Gateway and it needs to be re-pushed.

7 Click *Re-Push Certificate*.

8 Restart Server Provider of the Access Gateway.

6.5 After installing the Identity Server, Communication to Access Gateway Fails, Due to port 8443 Listens on Loop Back Interface

When the Identity Server is installed on a separate machine, the server gets successfully imported into the Administration Console, port 8443 listens on the loop back interface but fails to communicate with the Access Gateway.

To workaround this issue, do the following:

1. Open the `server.xml` file
   - 1a **Linux:** `/etc/init.d/novell-tomcat5 restart`
   - 1b **Windows Server 2003:** `\Program Files\Novell\Tomcat\conf`
   - 1c **Windows Server 2008:** `\Program Files (x86)\Novell\Tomcat\conf`
2. Change the IP address given during the Identity Server installation.
3. Restart Tomcat
   - 3a **Linux:** `/etc/init.d/novell-tomcat5 restart`
   - 3b **Windows:** `net start "Apache Tomcat"`