Installation and Upgrade Guide

Access Manager 4.2

November 2015

NetIQ.

Legal Notice

Contents

About this Book and the Library

The *Installation Guide* provides an introduction to NetIQ Access Manager and describes the installation and upgrade procedures.

Intended Audience

This book is intended for Access Manager administrators. It is assumed that you have 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)

Other Information in the Library

The library provides the following information resources:

- *NetIQ Access Manager 4.2 Best Practices Guide*
- NetIQ Access Manager 4.2 Administration Guide
- NetIQ Access Manager 4.2 Developer Guide

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

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.

Installing Access Manager

Before you start installation, evaluate how you want to implement Access Manager.You can install components on a single server or on separate servers. For more information, see Chapter 1, “Planning Your Access Manager Environment,” on page 13.

The following is the sequence of installing Access Manager components:

1. Administration Console
2. Identity Server
3. Access Gateway

This part describes how to install Access Manager components and include the following chapters:

1 Planning Your Access Manager Environment

This section includes the following topics:

- “Deployment Models” on page 13
- “Access Manager Versus Access Manager Appliance” on page 14
- “Network Requirements” on page 21
- “Recommended Installation Scenarios” on page 22
- “Installing Access Manager Components in NAT Environments” on page 24
- “Setting Up Firewalls” on page 28
- “Protecting an Identity Server Through the Access Gateway” on page 35

Deployment Models

Access Manager Appliance is a new deployment model introduced from NetIQ Access Manager 3.2 onwards. It includes all major components such as Administration Console, Identity Server, and Access Gateway in a single soft appliance. This solution differs from the other Access Manager model where all components can be installed on separate systems. Access Manager Appliance enables organizations to rapidly deploy and secure Web and enterprise applications. This simplifies access to any application. The reduced deployment and configuration time gives quick time to value and helps to lower the total cost of ownership.

Some of the key differentiators that Access Manager Appliance offers over the Access Manager solution are:

- Quick installation and automatic configuration
- Single port configuration and common location to manage certificates
- Sample portal for administrator reference
- Fewer DNS names, SSL certificates, and IP addresses
- Reduced hardware requirements

For details about these differentiators and other features of Access Manager Appliance, see “Access Manager Versus Access Manager Appliance” on page 14.

The following diagrams describe differences between Access Manager and Access Manager Appliance:

Figure 1-1 *Typical Deployment of Access Manager*

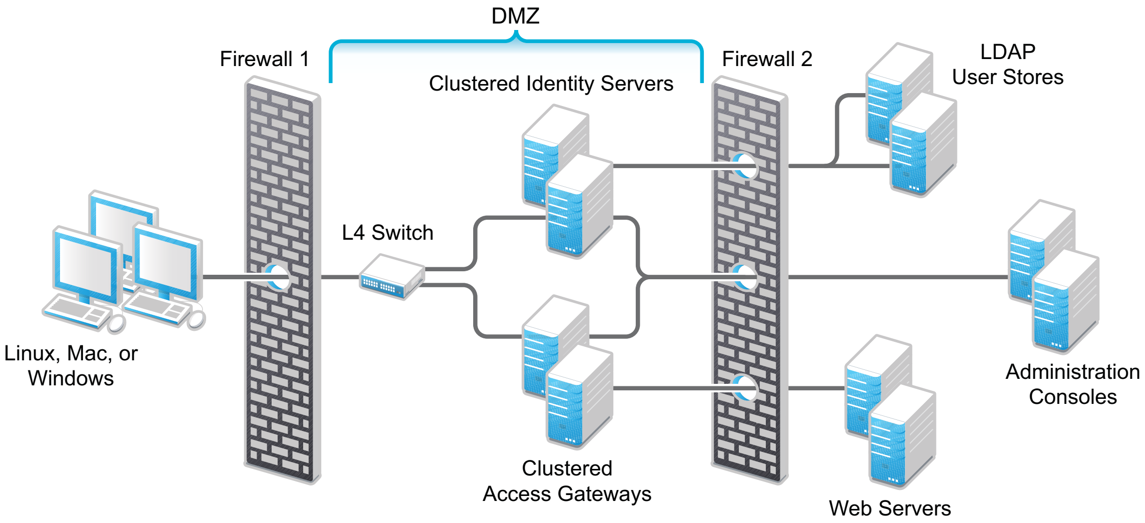
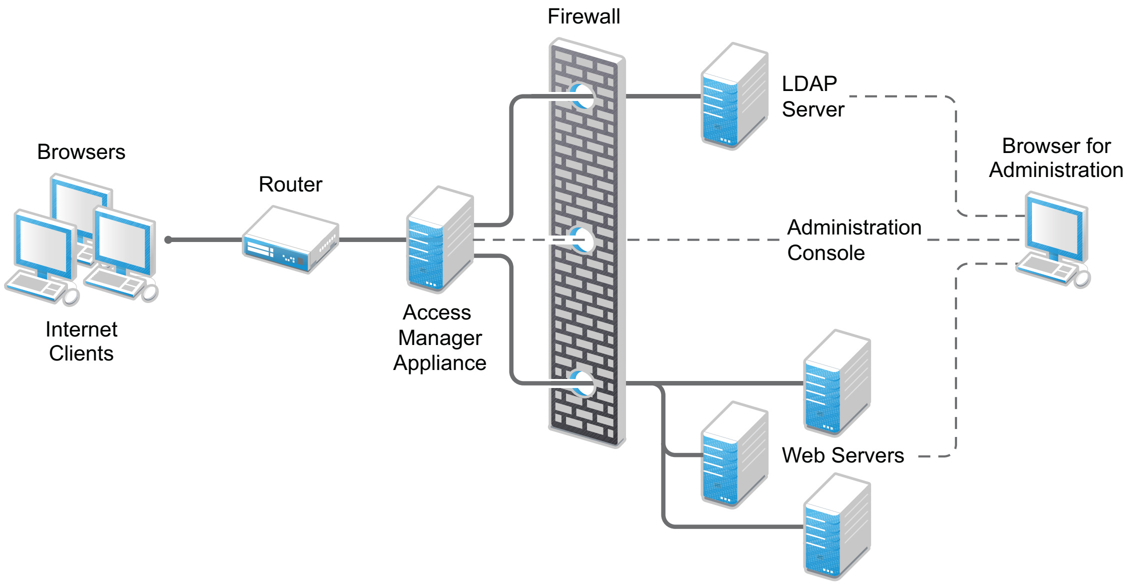


Figure 1-2 *Typical Deployment of Access Manager Appliance*



Access Manager Versus Access Manager Appliance

Both Access Manager and Access Manager Appliance deployment models use a common code base. But, the differences in the deployment method result in few similarities and differences in both models. The following table provides details to help you determine which solution fits your business:

Table 1-1 Access Manager Versus Access Manager Appliance

Feature	Access Manager Appliance	Access Manager
Virtualization Support	Supported on the virtual servers based on SUSE Linux Enterprise Server (SLES) 11 SP3, or SLES 12 with 64-bit operating system x86-64 hardware.	Supported on the virtual servers based on SUSE Linux Enterprise Server (SLES) 11 SP3, or SLES 12 with 64-bit operating system x86-64 hardware.
Host Operating System	A soft appliance that includes a pre-installed and configured SUSE Linux operating system. NetIQ maintains both the operating system and Access Manager patches through the patch update channel.	Operating System choice is more flexible. Install Administration Console, Identity Server, and Access Gateway on a supported operating system (SUSE, Red Hat, or Windows). The patch update channel maintains the patches for Access Manager. You must purchase, install, and maintain the underlying operating system.
Component Installation Flexibility	Access Manager components such as Administration Console, Identity Server, and Access Gateway cannot be selectively installed or uninstalled.	Each Access Manager component such as Administration Console, Identity Server, and Access Gateway are installed on independent host servers. Although the ability to install multiple components on a single host server exists, it is very limited and generally not recommended. A typical highly available deployment requires 6-8 or more virtual or physical servers (2 Administration Consoles, 2 Identity Servers, 2 Access Gateways).
Administration Console Access	Administration Console is installed on Access Manager Appliance along with all other components. If you use two network interfaces, access to the Administration Console can be limited to the private IP network bound to the internal network. The public interface is bound to an externally accessible network.	Administration Console can be installed on an independent host inside your private network but can still securely manage Access Manager components that reside in your DMZ or external network.
Scalability and Performance	Scales vertically on adding CPU and memory resources to each node. For more information, see Performance and Sizing Guidelines.	Scales both vertically and horizontally on adding nodes. For more information, see Performance and Sizing Guidelines.
High Availability	Supported	Supported

Feature	Access Manager Appliance	Access Manager
Upgrade	You can upgrade from one version of Access Manager Appliance to another version. However, upgrading from Access Manager to Access Manager Appliance is not supported.	You can upgrade from one version of Access Manager to another version. However, upgrading from Access Manager Appliance to Access Manager is not supported.
Migration from Access Manager to Access Manager Appliance or vice-versa	During migration from Access Manager Appliance to Access Manager, the policies can be exported but the rest of the configuration should be done manually.	During migration from Access Manager Appliance to Access Manager, the policies can be exported but the rest of the configuration should be done manually.
Disaster Recovery	You can use the backup and restore process to save your Access Manager Appliance configuration.	You can use the backup and restore process to save your Access Manager configuration.
Time to Value	Automates several configuration steps to quickly set up the system.	Requires more time to install and configure as the components are on different servers.
User Input required during installation	Access Manager Appliance is a software appliance that takes only a few basic parameters as input. Several options assume default values.	More flexibility during installation in terms of selectable parameters.
Installation and Configuration Phases	The installer takes care of configuration for each component. The system is ready for use after it is installed.	Separate installation and configuration phases for each component. After installation, each Access Manager component is separately configured.
Mode of release	Access Manager Appliance is released as a software appliance.	Access Manager is delivered in the form of multiple operating system-specific binaries.
NIC Bonding	IP address configuration is done through the Administration Console. So, NIC bonding is not supported.	NIC bonding can be done through the operating system and Access Manager in turn uses this configuration.
Networking: Port Details	The Administration Console and Identity Server are accelerated and protected by Access Gateways. Only HTTPS port 443 is required to access the Access Manager Appliance through a firewall.	Multiple ports need to be opened for deployment.
Networking: General	Administration Console must be in DMZ, but access can be restricted through the private interface.	As Administration Console is a separate device, access can be restricted or Administration Console can be placed in an internal network.

Feature	Access Manager Appliance	Access Manager
Certificate Management	Certificate management is simplified. All certificates and key stores are stored at one place making replacing or renewing certificates easier.	Changes are required at multiple places to replace or renew certificates.
Certificate Management: SAML Assertion Signing	Same certificate is used for all communication. (signing, encryption, and transport).	As there are multiple key stores, you can configure different certificates for the communication.
Associating different signing certificates for each service provider	Not supported	A unique signing certificate can be assigned to each service provider. In environments with a large number of trust relationships, this feature eases the process of replacing expiring certificates. Note: This is a feature that was introduced in Access Manager 3.2 SP2.
Associating different certificates to Identity Server	Not applicable because the Identity Server is accelerated by the Access Gateway.	Supported. The Identity Server can be behind the Access Gateway or can be placed separately in the DMZ.
Sample Portal	After a successful installation, a sample Web portal is deployed for the administrator's reference. The administrator can access the sample portal by using the http://hostname URL. This portal provides detailed example of Access Manager Appliance usage and policy configuration.	Not available.

Feature	Access Manager Appliance	Access Manager
Ready-made Access Manager	The following configuration is automatically done when Access Manager Appliance is installed: ◆ Importing Identity Server and Access Gatewaycomponents. ◆ Automatic cluster creation of Identity Server and Access Gateway component. ◆ Automatic configuration of Identity Server to bring it to green state. ◆ Automatic configuration of Access Gateways and Identity Server association. ◆ Automatic service creation to accelerate or protect the Identity Server, Administration Console, and sample portal. As the inter-component configuration is automated, the administrator only needs to add the existing user store and accelerate, protect, sso-enable existing Web applications.	Each component is manually configured and set up before Web applications can be federation enabled, accelerated, protected.
Updating Kernel with Security Patches	Supports installation of latest SLES operating system security patches.	You are fully responsible for all operating system maintenance including patching.
Clustering	For additional capacity and for failover, cluster a group of NetIQ Access Manager Appliances and configure them to act as a single server. You can cluster any number of Identity Servers and Access Gateways, and up to three of Administration Consoles. The first three nodes of Access Manager Appliance contain the Administration Console, Identity Server, and Access Gateway. Fourth installation onwards, the node has all components except for the Administration Console. A typical Access Manager Appliance deployment in a cluster is described in Figure 1-3 on page 19.	For additional capacity and for failover, cluster a group of Identity Servers and configure them to act as a single server. You can create a cluster of Access Gateways and configure them to act as a single server. Fault tolerance can be achieved by installing up to two secondary consoles. To deploy the existing solution in a cluster mode, at least 6 systems are required. A typical Access Manager deployment in a cluster is described in Figure 1-4 on page 20.

***Figure 1-3** Access Manager Appliance Cluster*

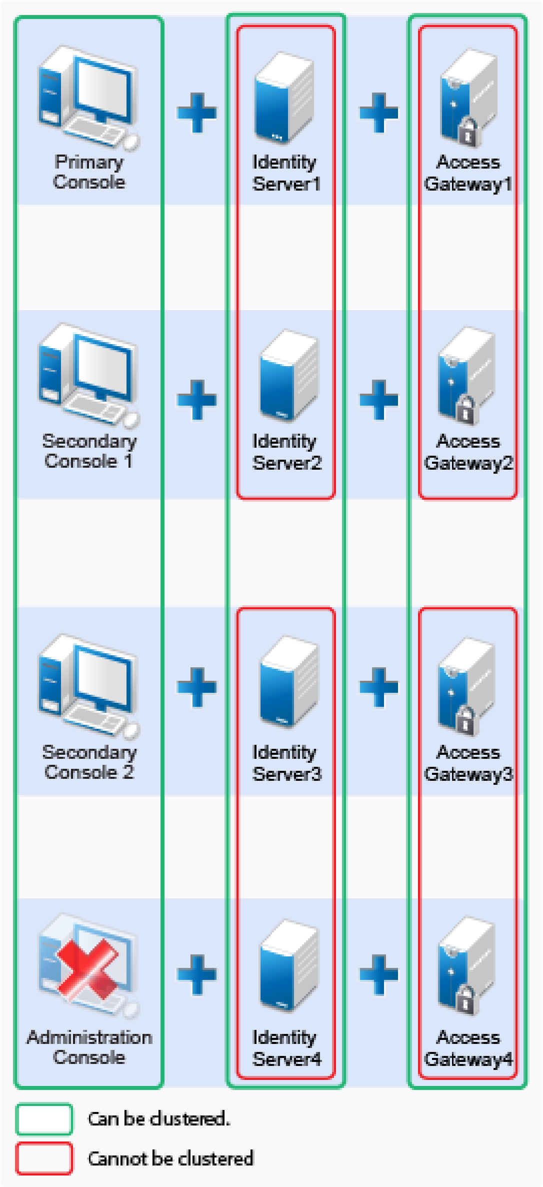
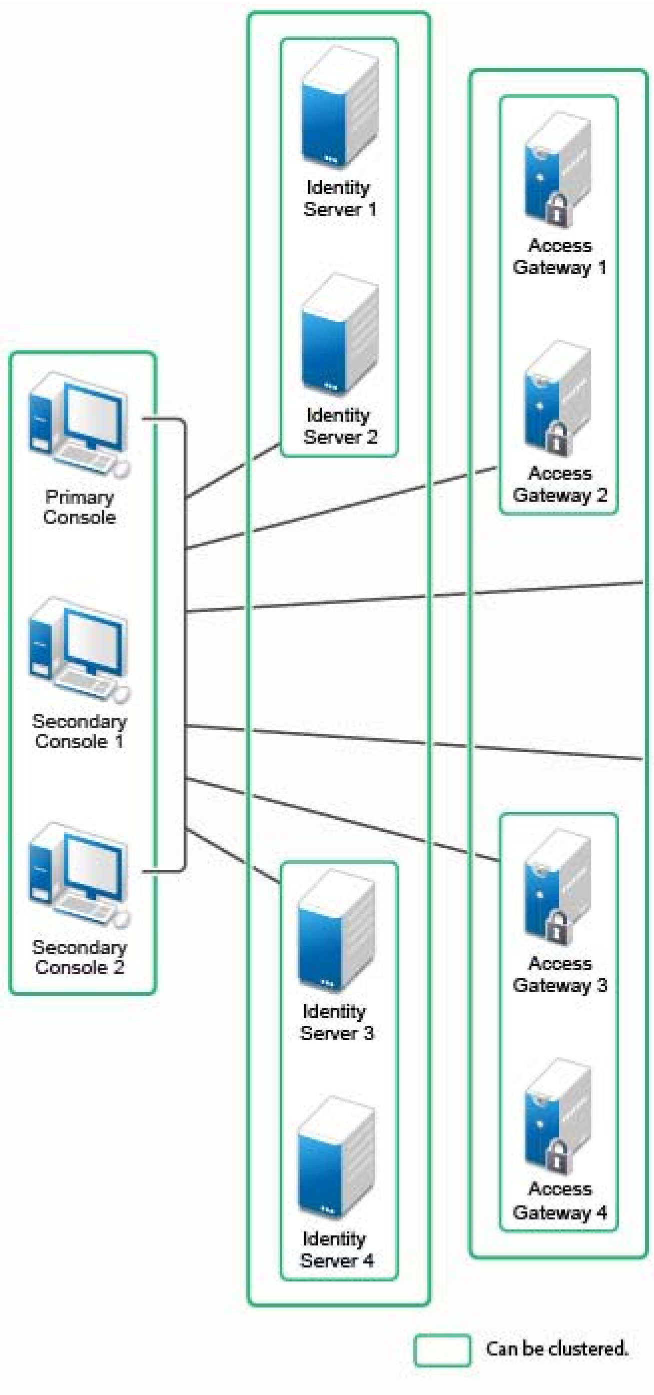


Figure 1-4 Access Manager Cluster



General Guidelines

- It is not possible to add an Access Gateway Service or Access Gateway Appliance to an Access Manager Appliance cluster.
- Deploying the Administration Console in a DMZ network limits access from a private interface or network.

- It is recommended to not change the primary IP Address of an Access Manager. This may result in corruption of the configuration store. However, you can modify the Listening IP address of reverse proxy or the outbound IP address used to communicate with the Web server. For more information, see Changing the IP Address of Access Manager Devices in the NetIQ Access Manager 4.2 Administration Guide .
- You cannot have different certificates for signing, encryption in a Federation setup.
- You cannot install any monitoring software to monitor statistics on an Access Manager Appliance.
- Clustering between Access Manager and Access Manager Appliance is not supported.

When to Choose Access Manager Appliance

The following are common usage patterns when you can deploy Access Manager Appliance:

- You are interested in deploying Access Manager, but need fewer servers.
- You are still on iChain because you prefer a single-server solution.
- You are new to Access Manager and are interested in providing secure access, but want to avoid the long process of designing, installing, and configuring a full-fledged Web access management solution.
- You do not have a Web access management or federation solution and you are considering moving to a Web access management solution.
- You represent a division of a large organization (for example, the Marketing division) that wants secure single sign-on access to a SaaS application such as Salesforce.
- You want to reduce server hardware and management cost by consolidating Access Manager services on fewer servers.
- You want to quickly set up a test environment to verify changes.
- You want to quickly setup and evaluate Access Manager.

Network Requirements

In addition to the servers on which software is installed, your network environment needs to have the following:

- A server configured with an LDAP directory (eDirectory, Sun ONE, or Active Directory) that contains your system users. The Identity Server uses the LDAP directory to authenticate users to the system.
- Web servers with content or applications that need protection.
- Clients with an Internet browser.
- 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).
- Static IP addresses for each machine used for an Access Manager component. If the IP address of the machine changes, the Access Manager component or components on that machine cannot start.
- 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.

- 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.

Recommended Installation Scenarios

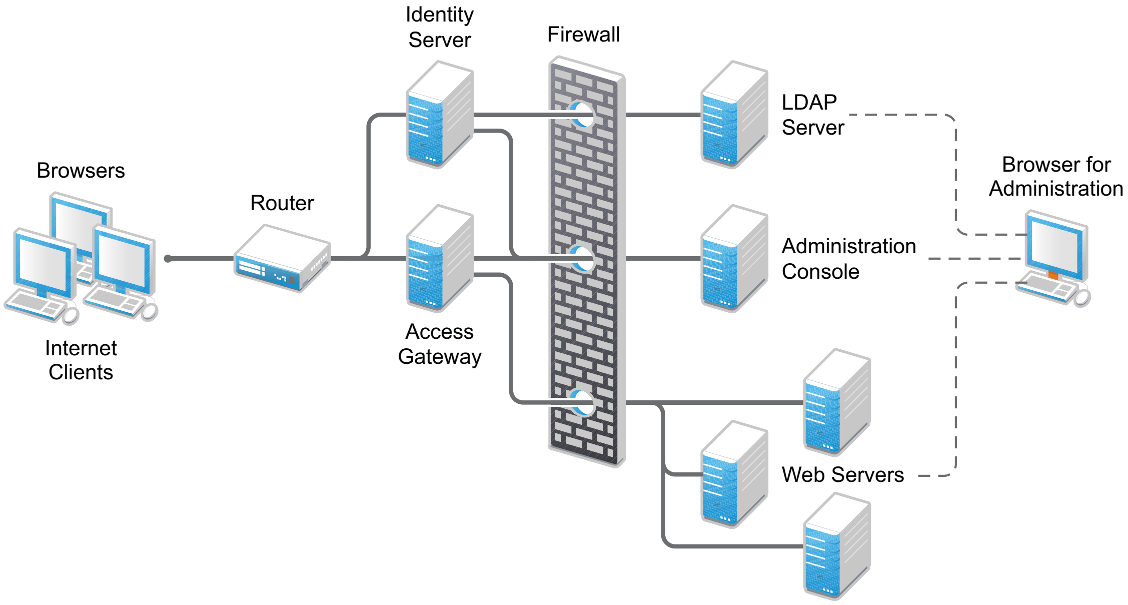
The following scenarios provide an overview of the flexibility built into Access Manager. Use them to design a deployment strategy that fits the needs of your company.

- "Basic Setup" on page 22
- "High Availability Configuration with Load Balancing" on page 23

Basic Setup

You need to protect the Administration Console from Internet attacks. It should be installed behind your firewall. For a basic Access Manager installation, you can install the Identity Server and the Access Gateway outside your firewall. Figure 1-5 illustrates this scenario:

***Figure 1-5** Basic Installation Configuration*



1. Install the Administration Console.

   The Administration Console and the Identity Server are bundled in the same download file or ISO image.

2. If your firewall is set up, open the ports required for the Identity Server and the Access Gateway to communicate with the Administration Console: TCP 1443, TCP 8444, TCP 1289, TCP 1290, TCP 524, TCP 636.

   For more information about these ports, see "Setting Up Firewalls" on page 28Chapter , "Setting Up Firewalls," on page 28.

3. Run the installation again and install the Identity Server on a separate server.

   Log in to the Administration Console and verify that the Identity Server installation was successful.

4. Install the Access Gateway.

   Log in to the Administration Console and verify that the Access Gateway imported successfully.

5. Configure the Identity Server and the Access Gateway. See Configuring Access Manager in the NetIQ Access Manager 4.2 Administration Guide .

   In this configuration, the LDAP server is separated from the Identity Server by the firewall. Make sure you open the required ports. See "Setting Up Firewalls" on page 28.

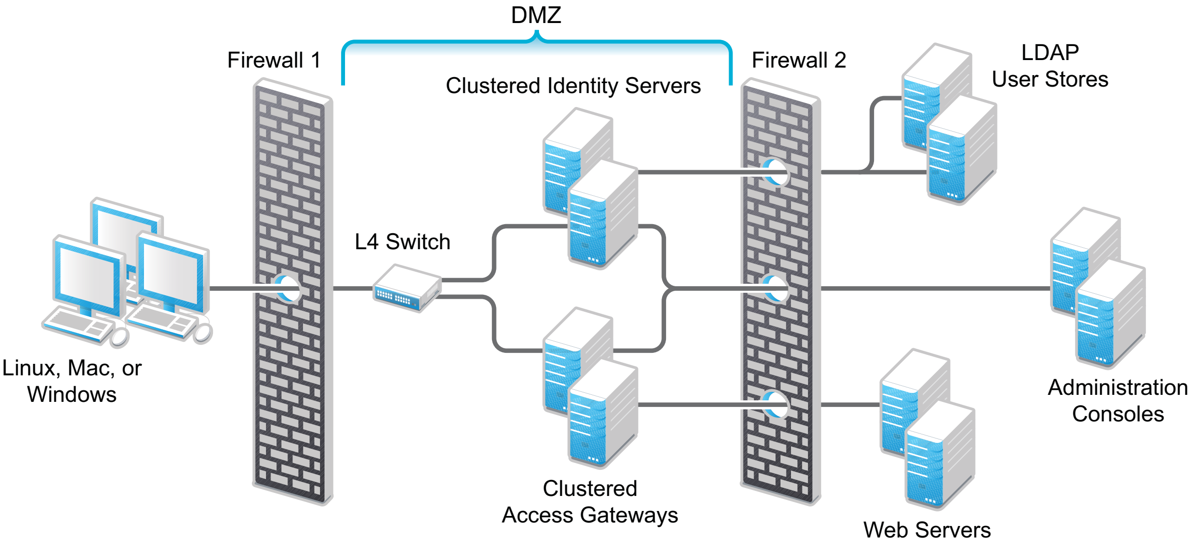
For information about setting up configurations for fault tolerance and clustering, see High Availability and Fault Tolerance in the NetIQ Access Manager 4.2 Administration Guide .

Firewall protects the LDAP server and the Administration Console, both of which contain a permanent store of sensitive data. Web servers are also installed behind the firewall for added protection. The Identity Server is not much of a security risk, because it does not permanently store any user data. NetIQ has tested and recommends this configuration. We have also tested this configuration with an L4 switch in place of the router so that the configuration can support clusters of Identity Servers and Access Gateways.

High Availability Configuration with Load Balancing

Figure 1-6 illustrates a deployment scenario where Web resources are securely accessible from the Internet. The scenario also provides high availability because both Identity Servers and Access Gateways are clustered and have been configured to use an L4 switch for load balancing and fault tolerance.

Figure 1-6 *Clustering Configuration for High Availability*



You can configure end users to communicate with Identity Servers and Access Gateways through HTTP or HTTPS. You can configure Access Gateways to communicate with Web servers through HTTP or HTTPS. Multiple Administration Consoles provide administration and configuration redundancy.

This configuration is scalable. As the number of users increase and the demands for Web resources increase, you can easily add another Identity Server or Access Gateway to handle the load, then add the new servers to the L4 switch. When the new servers are added to the cluster, they are automatically sent the cluster configuration.

Installing Access Manager Components in NAT Environments

This chapter 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. Topics include:

- "Network Prerequisites" on page 24
- "Network Setup Flow Chart" on page 25
- "Installing Access Manager Components in NAT Environments" on page 25
- "Configuring Network Address Translation" on page 27

Network Prerequisites

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 components on that machine cannot start.

❒ Install operating system, configure Network Time Protocol (NTP) server, and check connectivity.

❒ NTP 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. Because the components can be in different private networks, you can use NAT, VPNs, or combination of both to achieve connectivity.

Customer Network Setup

❒ A server configured with an LDAP directory (eDirectory 8.8.8.4 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.

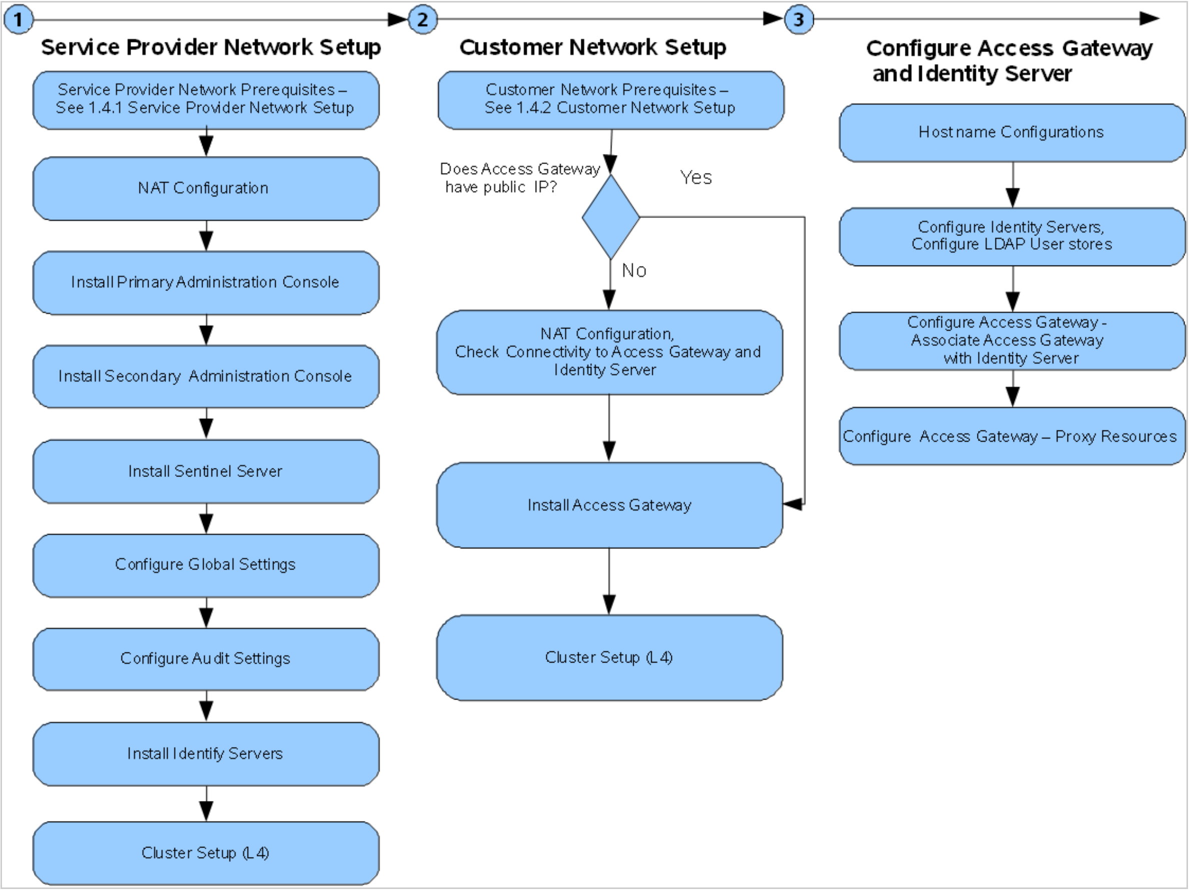
Access Manager devices know each other by their IP addresses, and some requests require them to match an IP address with the device's DNS name. Without reverse lookups enabled, these requests fail. In particular, Identity Servers perform reverse lookups to their user stores. If reverse lookups are not 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 components on that machine cannot start.
- ❒ There should be IP connectivity between different Access Manager components. Because the components can be in different private networks, you can use NAT, VPNs, or combination of both to achieve connectivity.

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 1-7 *Network Setup Flow Chart*



1
Service Provider Network Setup
Service Provider Network Prerequisites – See 1.4.1 Service Provider Network Setup
NAT Configuration
Install Primary Administration Console
Install Secondary Administration Console
Install Sentinel Server
Configure Global Settings
Configure Audit Settings
Install Identify Servers
Cluster Setup (L4)
2
Customer Network Setup
Customer Network Prerequisites – See 1.4.2 Customer Network Setup
Does Access Gateway have public IP?
Yes
No
NAT Configuration, Check Connectivity to Access Gateway and Identity Server
Install Access Gateway
Cluster Setup (L4)
3
Configure Access Gateway and Identity Server
Hostname Configurations
Configure Identity Servers, Configure LDAP User stores
Configure Access Gateway - Associate Access Gateway with Identity Server
Configure Access Gateway – Proxy Resources

Installing Access Manager Components in NAT Environments

Installing Access Manager in the NAT environment consists of the following steps:

1. “Installing the Administration Console” on page 26.
2. “Configuring Global Settings” on page 26
3. “Installing the Identity Servers” on page 47
4. “Installing the Access Gateway” on page 57

Installing the Administration Console

For installation requirements, see "Installing the Administration Console" on page 37.

1 Before installing 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 greater than 100ms, it might lead to performance degradation.

3 Synchronize time across all 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 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 about installing the Administration Console, see the "Installing the Administration Console on Windows" on page 42.

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

6 Continue with "Configuring Global Settings" on page 26 to add both the primary and secondary Administration Consoles to the **Global Settings** configuration.

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 list.

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.

Installing and Configuring the Identity Server

For information about how to install the Identity Server, see “Installing the Identity Servers” on page 47.

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 information about how to configure the Identity Server, see Configuring an Identity Server in the NetIQ Access Manager 4.2 Administration Guide .

Installing and Configuring the Access Gateway

For information about how to install Access Gateway, see “Installing the Access Gateway” on page 57.

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 information about configuring Access Gateway, see Configuring the Access Gateway in the NetIQ Access Manager 4.2 Administration Guide .

Configuring Network Address Translation

NetIQ Access Manager can be configured by using Network Address Translation (NAT), which enables the communication between the Administration Console from local network to other Access Manager devices such as Identity Server and Access Gateway. The devices can be in the external network or in another private network. The NAT address needs be to configured in router.

See your router documentation for more information.

- “Configuring the Administration Console Behind NAT” on page 27
- “Configuring Identity Server and Access Gateway Behind NAT” on page 28

Configuring the Administration Console Behind NAT

1 Log in to the Administration Console.

2 Go to **Access Manager** > **Global Settings**, then click **New**.

3 Select an IP address from the **Administration Console Public IP Address** list.

   This list contains primary and secondary Administration Console IP addresses.

4 Enter the respective NAT IP address for primary and secondary Administration Console in **Public NAT IP Address**.

   NOTE: If the NAT IP address is not provided or if a mapping exists for the selected Administration Console IP, a message `IP Address is not valid` is displayed.

5 Click **OK**.

   The Administration Console NAT IP is shared to other Access Manager devices.

For more information about configuring NAT, see Mapping the Private IP Address to Public IP Address in the NetIQ Access Manager 4.2 Administration Guide .

Configuring Identity Server and Access Gateway Behind NAT

During installation, the system prompts the following message to specify the NAT address for the component:

```
Is local NAT available for the <device name> y/n? [n]:
```

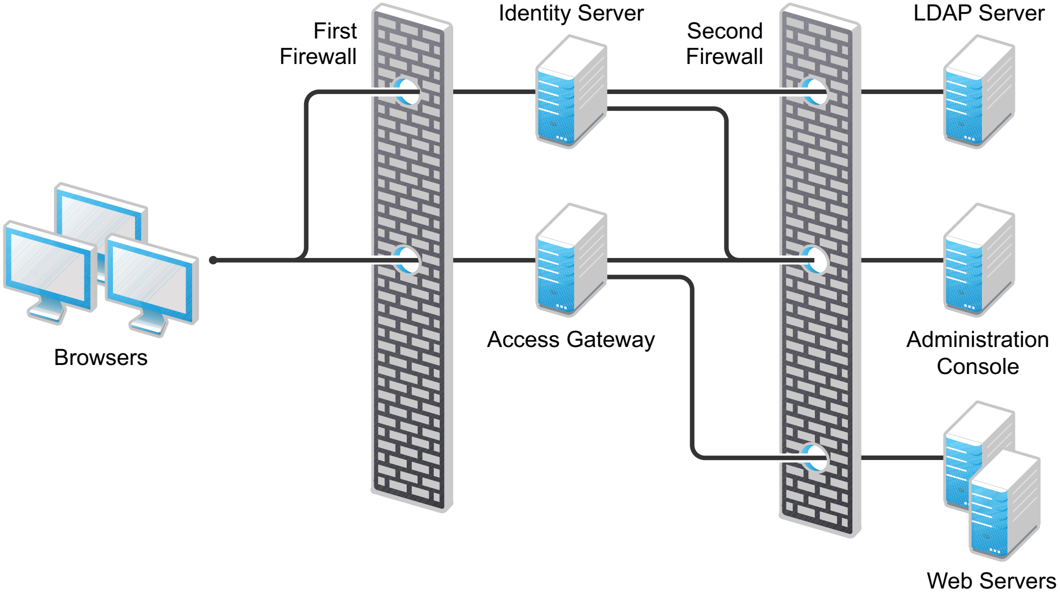
Enter Y and specify the NAT address. This enables the Administration Console to use this NAT address when communicating to this device.

Alternatively, if the device is already installed, then run the `reimport_nidp.sh` or `reimport_ags.sh` script to specify the NAT address.

Setting Up Firewalls

Access Manager should be used with firewalls. Figure 1-8 illustrates a simple firewall setup for a basic Access Manager configuration of an Identity Server, an Access Gateway, and an Administration Console.

Figure 1-8 *Access Manager Components between Firewalls*



The first firewall separates the Access Manager from the Internet, allowing browsers to access the resources through specific ports. The second firewall separates Access Manager components from Web servers they are protecting and the Administration Console.This is one of many possible configurations. This section describes the following:

- "Required Ports" on page 29
- "Sample Configurations" on page 33

Required Ports

The following tables list the ports that need to be opened when a firewall separates one component from another. Some combinations appear in more than one table. This allows you to discover the required ports whether a firewall is separating an Access Manager component from the Administration Console or a firewall is separating an Administration Console from the Access Manager component.

With these tables, you should be able to place Access Manager components of your system anywhere within your existing firewalls and know which ports need to be opened in the firewall.

Table 1-2 *When a Firewall Separates an Access Manager Component from a Global Service*

Component	Port	Description
NTP Server	UDP 123	Access Manager components must have time synchronized else the authentication fails. We recommend that you configure all components to use an network time protocol (NTP) server. Depending upon where your NTP server is located, you might need to open UDP 123, so that Access Manager components can use the NTP server.
DNS Servers	UDP 53	Access Manager components must be able to resolve DNS names. Depending upon where your DNS servers are located, you might need to open UDP 53, so that Access Manager components can resolve DNS names.
Remote Linux Administration Workstation	TCP 22	If you want to use SSH for remote administration of Access Manager components, open TCP 22 to allow communication from your remote administration workstation to your Access Manager components.
Remote Windows Administration Workstation	Configurable	If you want to use RDP or VNC for remote administration of Access Manager components, open the ports required by your application from the remote administration workstation to your Access Manager components. You need to open ports for console access and for file sharing. For console access, VNC usually uses TCP 5901 and RDP uses TCP 3389. For file sharing, UDP 135-139 are the default ports.

Table 1-3 *When a Firewall Separates the Administration Console from a Component*

Component	Port	Description
Access Gateway, Identity Server	TCP 1443	For communication from the Administration Console to the devices.
	TCP 8444	For communication from devices to the Administration Console.
	TCP 1290	For communication from devices to the Syslog server on the Administration Console.
	TCP 524	For NCP certificate management with NPKI. The port needs to be opened so that both the device and the Administration Console can use the port.
	TCP 636	For secure LDAP communication from devices to the Administration Console.
	HTTP 2443	For the installer to communicate with the Administration Console. You can close these port after installation is complete.
	HTTP 8443	
Importing an Access Gateway Appliance	ICMP	During an import, the Access Gateway Appliance sends two pings through ICMP to the Administration Console. When the import has finished, you can disable the ICMP echo requests and echo replies.
LDAP User Store	TCP 524	Required only if the user store is eDirectory. When configuring a new eDirectory user store, NCP is used to enable Novell SecretStore by adding a SAML authentication method and storing a public key for the Administration Console. It is not used in day-to-day operations.
	TCP 636	For secure LDAP communication from Administration Console to User Store.
Administration Console	TCP 524	Required to synchronize the configuration data store.
	TCP 636	Required for secure LDAP communication.
	TCP 8080, 8443	Used for Tomcat communication.
	TCP 705	Used by Sub Agent-Master Agent communication inside the Administration Console.
	UDP 161	Used for communication by an external Network Monitoring System with the Administration Console by using SNMP.

Component	Port	Description
Browsers	TCP 8080	For HTTP communication from browsers to the Administration Console.
	TCP 8443, 2443, 2080.	For HTTPS communication from browsers to the Administration Console. **NOTE:** 2443 and 2080 are optional ports required when the Administration Console and Identity Server are collocated.
	TCP 8028, 8030	To use iMonitor or DSTrace from a client to view information about the configuration store on the Administration Console.

Table 1-4 *When a Firewall Separates the Identity Server from a Component*

Component	Port	Description
Access Gateway	TCP 8080 or 8443	For authentication communication from the Access Gateway to the Identity Server. The default ports for the Identity Server are TCP 8080 and 8443. They are configurable. You need to open the port that you configured for the base URL of the Identity Server.
	TCP 80 or 443	For communication from the Identity Server to ESP of the Access Gateway. This is the reverse proxy port that is assigned to be ESP (see the Reverse Proxy /Authentication page). This is usually port 80 or 443.
Administration Console	TCP 1443	For communication from the Administration Console to devices. This is configurable.
	TCP 8444	For communication from the Identity Server to the Administration Console.
	TCP 1290	For communication from devices to the Syslog server on the Administration Console.
	TCP 524	For NCP certificate management with NPKI from the Identity Server to the Administration Console.
	TCP 636	For secure LDAP communication from the Identity Server to the Administration Console.
Identity Server	TCP 8443 or 443	For HTTPS communication. You can use iptables to configure this for TCP 443. See "Translating the Identity Server Configuration Port" on page 52.
	TCP 7801	For back-channel communication with cluster members. This port is configurable.
LDAP User Stores	TCP 636	For secure LDAP communication from the Identity Server to the LDAP user store.

Component	Port	Description
Service Providers	TCP 8445	If you have enabled identity provider introductions, open a port to allow HTTPS communication from the user’s browser to the service provider.
	TCP 8446	If you have enabled identity provider introductions, open a port to allow HTTPS communication from the user’s browser to the service consumer.
Browsers	TCP 8080	For HTTP communication from a browser to the Identity Server. You can use iptables to configure this for TCP 80. See“Translating the Identity Server Configuration Port” on page 52.
	TCP 8443	For HTTPS communication from a browser to the Identity Server. You can use iptables to configure this for TCP 443. See “Translating the Identity Server Configuration Port” on page 52.
CRL and OCSP Servers	Configurable	If you are using x.509 certificates that include an AIA or CRL Distribution Point attribute, you need to open the port required to talk to that server. Ports 80/443 are the most common ports, but the LDAP ports 389/636 can also be used.
Active Directory Server with Kerberos	TCP 88, UDP 88	For communication with the KDC on the Active Directory Server for Kerberos authentication.

Table 1-5 *When a Firewall Separates the Access Gateway from a Component*

Component	Port	Description
Identity Server	TCP 8080 or 8443	For authentication communication from the Access Gateway to the Identity Server. The default ports are TCP 8080 and 8443, which are configurable. You need to open the port of the base URL of the Identity Server.
	TCP 80 or 443	For communication from the Identity Server to ESP of the Access Gateway. This is the reverse proxy port that is assigned to be ESP (see the Reverse Proxy /Authentication page). This is usually port 80 or 443.
Administration Console	TCP 1443	For communication from the Administration Console to the Access Gateway. This is configurable.
	TCP 8444	For communication from the Access Gateway to the Administration Console.
	TCP 1290	For communication from devices to the Syslog server on the Administration Console.
	TCP 524	For NCP certificate management with NPKI from the Access Gateway to the Administration Console.
	TCP 636	For secure LDAP communication from the Access Gateway to the Administration Console.

Component	Port	Description
Access Gateway	TCP 7801	For back-channel communication with cluster members. This port is configurable. It is set by the Identity Server cluster configuration that the Access Gateway trusts. See Configuring a Cluster with Multiple Identity Servers in the NetIQ Access Manager 4.2 Administration Guide .
Browsers/Clients	TCP 80	For HTTP communication from the client to the Access Gateway. This is configurable.
	TCP 443	For HTTPS communication from the client to the Access Gateway. This is configurable.
Web Servers	TCP 80	For HTTP communication from the Access Gateway to the Web servers. This is configurable.
	TCP 443	For HTTPS communication from the Access Gateway to Web servers. This is configurable.

NOTE: On SLES 11 SP2 (or a higher version), you can use YaST to configure UDP ports and internal networks.

Sample Configurations

- "Access Gateway and Identity Server in DMZ" on page 33
- "A Firewall Separating Access Manager Components from the LDAP Servers" on page 34

Access Gateway and Identity Server in DMZ

- "First Firewall" on page 33
- "Second Firewall" on page 34

First Firewall

If you place a firewall between browsers and Access Gateway and Identity Server, you need to open ports so that browsers can communicate with the Access Gateway and the Identity Server and the Identity Server can communicate with other identity providers.

See, Figure 1-8 on page 28

***Table 1-6** Ports to Open in the First Firewall*

Port	Purpose
TCP 80	For HTTP communication.
TCP 443	For HTTPS communication.
Any TCP port assigned to a reverse proxy or tunnel.	
TCP 8080	For HTTP communication with the Identity Server. For information about redirecting the Identity Server to use port 80, see "Translating the Identity Server Configuration Port" on page 52.
TCP 8443	For HTTPS communication with the Identity Server. For information about redirecting the Identity Server to use port 443, see "Translating the Identity Server Configuration Port" on page 52.
TCP 8445	For HTTP Identity Provider introductions. If you do not enable Identity Provider introductions, you do not need to open this port.
TCP 8446	For HTTPS Identity Provider introductions. If you do not enable Identity Provider introductions, you do not need to open this port.

Second Firewall

The second firewall separates Web servers, LDAP servers, and the Administration Console from the Identity Server and the Access Gateway. You need the following ports opened in the second firewall:

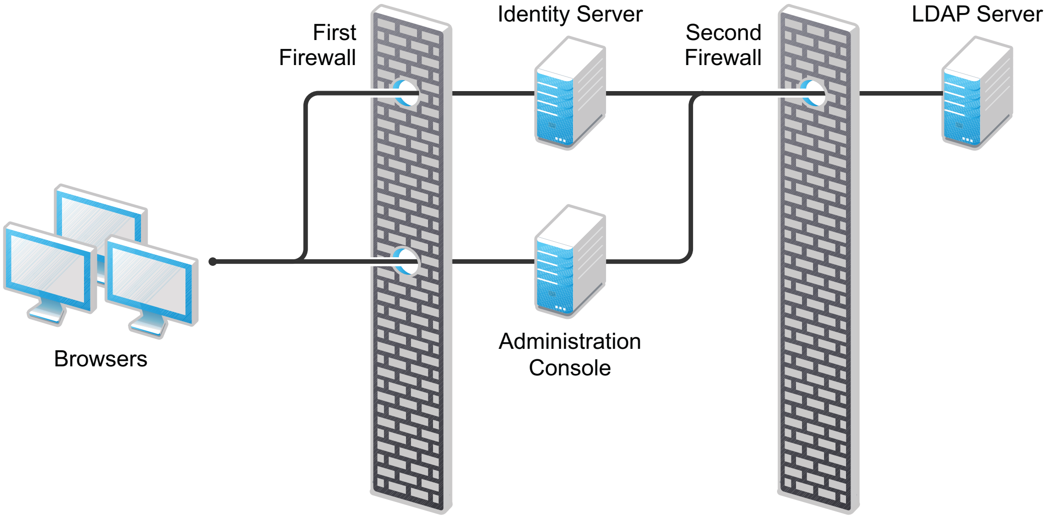
***Table 1-7** Ports to Open in the Second Firewall*

Port	Purpose
TCP 80	For HTTP communication with Web servers.
TCP 443	For HTTPS communication with Web servers.
Any TCP connect port assigned to a Web server or to a tunnel.	
TCP 1443	For communication from the Administration Console to the devices.
TCP 8444	For communication from the devices to the Administration Console.
TCP 1290	For communication from the devices to the Syslog server installed on the Administration Console. If you do not enable auditing, you do not need to open this port.
TCP 524	For NCP certificate management in NPKI. The port needs to be opened so that both the device and the Administration Console can use the port.
TCP 636	For secure LDAP communication of configuration information.

A Firewall Separating Access Manager Components from the LDAP Servers

You can configure your Access Manager components so that your Administration Console is on the same side of the firewall as your Access Manager components and have a firewall between them and the LDAP servers.

Figure 1-9 A Firewall Separating the Administration Console and the LDAP Server



In this configuration, you need to have the following ports opened in the second firewall for the Administration Console and the Identity Server.

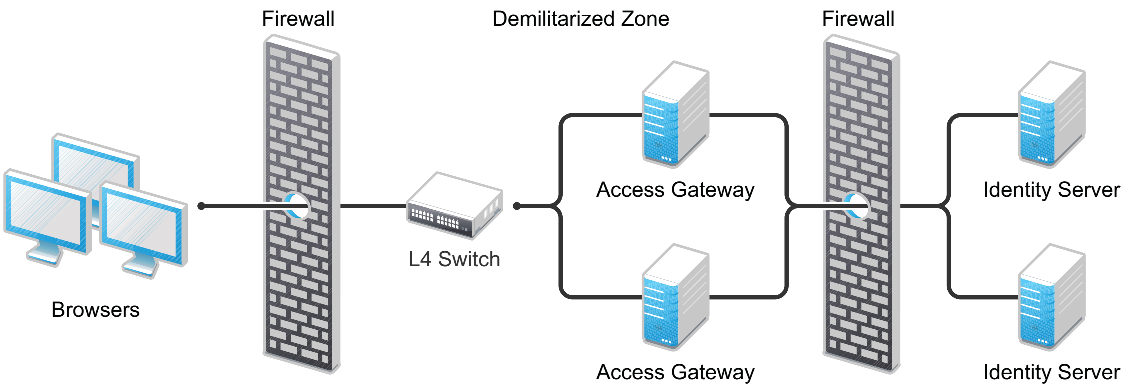
Table 1-8 Ports to Open in the Second Firewall

Ports	Purpose
TCP 636	For secure LDAP communication. This is used by the Identity Server and the Administration Console.
TCP 524	For configuring eDirectory as a new User Store. NCP is used to enable SecretStore by adding a SAML authentication method and storing a public key for the Administration Console. During day-to-day operations, this port is not used. If your LDAP server is Active Directory or Sun ONE, this port does not need to be opened.

Protecting an Identity Server Through the Access Gateway

For security reasons, you might want to set up your Access Manager configuration so that the Identity Server is a resource protected by an Access Gateway. This configuration reduces the number of ports you need to open between the outside world and your network. Figure 1-10 illustrates such a configuration.

***Figure 1-10** Identity Servers behind an Access Gateway*



With this configuration, you need an L4 switch to cluster the Access Gateways. However, you do not need an L4 switch to cluster the Identity Servers. When the Identity Server is configured to be a protected resource of the Access Gateway, the Access Gateway uses its Web server communication channel. Each Identity Server in the cluster must be added to the Web server list, and the Access Gateway uses its Web server load balancing and failover policies for the clustered Identity Servers.

Limitations: The following features are not supported with this configuration:

- The Identity Server cannot respond to Identity Provider introductions.
- Federation to an external service provider that requires the artifact profile with SOAP/Mutual SSL binding cannot be supported with this configuration.
- The proxy service that is protecting the Identity Server cannot be configured to use mutual SSL. For example with this configuration, X.509 authentication cannot be used for any proxy service. To perform X.509 authentication (which is a form of mutual SSL), a user's browser must have direct access to the Identity Server.
- The proxy service that is protecting the Identity Server cannot be configured to use NMAS.

For configuration details, see Configuring a Protected Identity Server Through Access Gateways in the NetIQ Access Manager 4.2 Administration Guide .

2 Installing the Administration Console

Administration Console is the first component you install. If you have iManager installed for other products, you still need to install this version on a separate server. The Administration Console is installed with an embedded version of eDirectory, which is used as the configuration store for Access Manager.

For a functioning system, you need an Administration Console for configuration and management, an Identity Server for authentication, and an Access Gateway for protecting resources. The Administration Console must be installed before you install any other Access Manager devices.

After you have installed the Administration Console, the installation scripts for the other components (Identity Server and Access Gateway) auto-import their configurations into the Administration Console.

This chapter explains how to install and configure the Administration Console. Topics include:

For information about installing a secondary Administration Console and fault tolerance, see Installing Secondary Versions of the Administration Console in the NetIQ Access Manager 4.2 Administration Guide .

Installing the Administration Console on Linux

Installation Requirements on Linux

- 4 GB RAM.
- Dual CPU or Core (3.0 GHz or comparable chip)
- 100 GB hard disk

  The hard disk should have ample space for logging in a production environment. This disk space must be in the local server not in the remote server.
- One of the following operating systems:
  - SUSE Linux Enterprise Server (SLES) 11 SP4 and SLES 12 with 64-bit operating system x86-64 hardware (physical or virtual). Ensure that the following packages are installed:

Package	Description
perl-gettext, gettext-runtime	The required library and tools to create and maintain message catalogs.
python	The basic Python library.
compat	Libraries to address compatibility issues. For information on enabling this repository, see TID 7004701 (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7004701&sliceId=1&docTypeID=DT_TID_1_1&dialogID=68926420&stateId=0%200%20130264119) Use the following command to verify: `rpm -qa | grep <package name>` Use YaST to install the packages.
binutils	The required set of tools to create and manage binary programs.
rsyslog	The required software for forwarding audit messages.
rsyslog-module-gtls	The required TLS encryption support module for rsyslog.
libXtst6-32bit	Has dependency on iManager

  - Red Hat Enterprise Linux (RHEL) 6.7 and 7.1 (64-bit) (physical or virtual). For installing the RHEL packages, see Appendix 5, “Installing Packages and Dependent RPMs on RHEL for Access Manager,” on page 69.

- Install the latest `net-snmp` package from the SLES or RedHat update channel.
- Zip and unzip utilities must be available for the backup and restore procedure.
- Ports 389 and 636 need to be free.
- Static IP address (if the IP address changes after devices have been imported, these devices can no longer communicate with the Administration Console.)
- The tree for the configuration store is named after the server on which you install the Administration Console. Check the hostname and rename the machine if the name is not appropriate for a configuration tree name.
- The Administration Console can be installed on the same server as the Identity Server. If you are planning to install an L4 switch on a SLES server by using the Linux Virtual Services software, you can also install the Administration Console on this server.
- The server on which you are installing Administration Console does not have any proxy configuration. If it contains a proxy configuration, ensure that the proxy server is working.
- Network requirements: See “Network Requirements” on page 21.

IMPORTANT: You cannot install the following with the Administration Console:

- OpenLDAP server. If it is installed, you must un-install it.
- LDAP software such as eDirectory.
- Other version of iManager. You also cannot add other iManager product plug-ins to this Administration Console.

- Because of library update conflicts, you cannot install Access Manager on a Linux User Management (LUM) machine.
- JRE. If you have a version installed, uninstall it.

Browser Support

- Internet Explorer 11 and later (Non Metro UI)
- Mozilla Firefox
- Chrome

Browser pop-ups must be enabled to use the Administration Console.

Installation Procedure

Installation time: about 20 minutes.

What you need to create during installation	A username and password for the Administrator.

NOTE: If the Administration Console and the Identity Server are installed on different servers, both use 8080 and 8443 ports. If the Administration Console and the Identity Server are installed on the same server, Identity Server uses 8080 and 8443 ports and Administration Console uses 2080 and 2443 ports.

1 If you have Red Carpet or auto update running, stop these programs before you install the Administration Console.

2 Verify that the machine meets the minimum requirements. See "Installation Requirements on Linux" on page 37.

3 Open a terminal window.

4 Access the install script as root:

4a Ensure that you have downloaded the software or you have the CD available.

For software download instructions, see the release-specific Readme.

4b Do one of the following:

- Insert the CD into the drive, then navigate to the device. Specify the following:

  ```
  cd /media
  ```

  Change to your CD-ROM drive, which is usually `cdrom` but can be something else such as `cdrecorder` or `dvdrecorder`, depending on your hardware.

- If you downloaded the `tar.gz` file, unzip it by using the following command:

  ```
  tar -xzvf <filename>
  ```

4c Change to the `novell-access-manager` directory.

5 At the command prompt, specify the following:

```
./install.sh
```

Ensure that you have adequate space in the system before you proceed with installation.

6 When you are prompted to install a product, select **1. Install Administration Console** and then press Enter.

7 Review and accept the License Agreement.

Novell Base and JDK for NetIQ are installed.

8. (Optional) The installer displays a warning if the host name of the system is mapped to the IP address 127.0.0.2 in the `/etc/hosts` file:

   ```
   An entry of 127.0.0.2 in the /etc/hosts file affects the Access Manager
   functionality. Do you want to proceed with removing it (y/n) [y]
   ```

   Specify `Y` to proceed.

   The host name mapping to 127.0.0.2 may cause certain Access Manager processes to encounter errors when they attempt to resolve the host name of the machine. To avoid these problems, remove the 127.0.0.2 entry from the`/etc/hosts` file.

9. Specify whether this is a primary Administration Console in a failover group. The first Administration Console installed becomes the primary console:

   You can install up to three Administration Consoles for replication and failover purposes. If this is not the primary console, you must provide the IP address of the primary Administration Console.

10. Specify the administration username.

    Press Enter to use *admin* as the default admin username, or change this to a username of your choice.

    NOTE: The Administration Console username does not accept special characters `#` (hash), `&` (ampersand), and `()`(round brackets).

11. Specify the administration password.

    Use alphanumeric characters only.

    NOTE: The Administration Console password does not accept special characters `:` (colon) and `"`” (double quotes).

12. Confirm the password, then wait for the system to install components.

    This may take several minutes depending on the speed of your hardware.

    NOTE: Platform Agent and Novell Audit are no longer supported. A new Access Manager 4.2 installation no longer installs Platform Agent and Novell Audit for auditing. If you upgrade from an older version of Access Manager to 4.2, Platform Agent is still available. It is recommended to use Syslog for auditing.

    The following components are installed:

Component	Description
Syslog	Responsible for packaging and forwarding the audit log entries to the configured Syslog Server. For more information, see Enabling Auditing in the NetIQ Access Manager 4.2 Administration Guide .
Tomcat for NetIQ	NetIQ packaging of the Java-based Tomcat Web server used to run servlets and JavaServer Pages (JSP) associated with NetIQ Access Manager Web applications.

Component	Description
Access Manager Configuration Store	An embedded version of eDirectory used to store user-defined server configurations, LDAP attributes, Certificate Authority keys, certificates, and other Access Manager attributes that must be securely stored.
iManager	The Web-based Administration Console that provides customized and secure access to server administration utilities. It is a modified version and cannot be used to manage other eDirectory trees.
Administration Console	A modification of iManager that enables management of all aspects of Access Manager. This component is not a standard iManager plug-in. It significantly modifies the tasks that iManager can perform.
Identity Server Administration Plug-In	Works in conjunction with the Administration Console to specifically manage the Identity Server.

13. Record the login URL.

    When installation completes, the login URL is displayed. It looks similar to the following:

    ```
    http://10.10.10.50:8080/nps
    ```

    Use this to configure Access Manager components.
14. Continue with "Configuring the Linux Administration Console Firewall" on page 41.

Configuring the Linux Administration Console Firewall

Before you can install other Access Manager components and import them into the Administration Console, or before you can log in to the Administration Console from a client machine, you must first configure the firewall on the Administration Console.

1. Click **Computer** > **YaST** > **Security and Users** > **Firewall**.

   This launches the Firewall Configuration screen.
2. Click **Allowed Services** > **Advanced**.
3. In the **TCP Ports** field, specify the ports to open.

   (Conditional) If you are installing the Administration Console and Identity Server on different machine, list the following additional ports in the **TCP Ports** field:

   - 8080
   - 8443
   - 3080
   - 3443

   (Conditional) If you are installing the Administration Console and Identity Server on the same machine, list the following additional ports in the **TCP Ports** field:

   - 2080
   - 2443

4 (Conditional) To import an Access Gateway into the Administration Console, list the following additional ports in the **TCP Ports** field:

- 1443
- 8444
- 1289
- 1290
- 524
- 636

If you are importing an Access Gateway Appliance, specify `icmp` in the **IP Protocols** field.

For specific information about the ports listed in Step 3 and Step 4, see Table 1-3 on page 30.

NOTE: The Administration Console is accessible on ports 2080 (HTTP) and 2443 (HTTPs) when Identity Server is installed on the same machine.

5 Restart Tomcat by running the following commands from the Administration Console command line.

```
/etc/init.d/novell-ac stop
```

```
/etc/init.d/novell-ac start
```

6 Continue with "Logging In to the Administration Console" on page 44.

Installing the Administration Console on Windows

- "Installation Requirements on Windows" on page 42
- "Installation Procedure" on page 42

Installation Requirements on Windows

- 4 GB RAM
- Dual CPU or Core (3.0 GHz or comparable chip)
- 100 GB hard disk

  The hard disk should have ample space for logging in a production environment. This disk space must be in the local server and not in the remote server.
- Windows Server 2012 R2, 64-bit operating system (physical or virtual), in either Standard or Enterprise Edition, with the latest patches applied.
- Static IP address
- Ports 389 and 636 need to be free

For information about browser support, see "Browser Support" on page 39.

For information about network requirements, see "Network Requirements" on page 21.

Installation Procedure

Installation time: about 20 minutes.

What you need to create during installation	A username and password for the Administrator.

NOTE: If the Administration Console and the Identity Server are installed on different servers, both use 8080 and 8443 ports. If the Administration Console and the Identity Server are installed on the same server, Identity Server uses 8080 and 8443 ports and Administration Console uses 2080 and 2443 ports.

1. Verify that the machine meets the minimum requirements. See "Installation Requirements on Windows" on page 42.
2. Close any running applications and disable any virus scanning programs.
3. (Conditional) To use a remote desktop for installation, use one of the following:
   - Current version of VNC viewer
   - Microsoft Remote Desktop with the `/console` switch for Windows XP SP2
   - Microsoft Remote Desktop with the `/admin` switch for Windows XP SP3
4. Download software and execute it.

   For software download instructions, see the release-specific Readme.
5. Read the introduction, then click **Next**.
6. Accept the license agreement, then click **Next**.
7. Select **Access Manager Administration Console**, then click **Next**.

   If you are also installing the Identity Server on this machine, you can also select **Access Manager Identity Server**.
8. Specify whether this is a primary Administration Console in a failover group, then click **Next**.

   The first Administration Console installed becomes the primary console.

   You can install up to three Administration Consoles for replication and failover purposes. If this is not the primary console, you must provide the IP address for the primary Administration Console.
9. Specify an administration user ID and password.
10. Specify the static IP address of the machine.
11. Click **Install**.

    The configuration database takes awhile to install and configure.
12. (Optional) After the installation completes, view the install log file found in the following location:

    Windows Server: `\Program Files (x86)\Novell\log\AccessManagerServer_InstallLog.log`
13. Restart the server.

    IMPORTANT: You must restart the server before installing any other Access Manager components.
14. Continue with "Configuring the Windows Administration Console Firewall" on page 43.

Configuring the Windows Administration Console Firewall

Before you can install other Access Manager components and import them into the Administration Console, or before you can log in to the Administration Console from a client machine, you must first configure the firewall on the Administration Console.

1. Click **Control Panel** > **Windows Firewall**.
2. Click **Advanced**, then for the Local Area Connection, click **Settings**.

3 For each port that needs to be opened, click **Add**, then Specify the following details:

Field	Description
Description of service	Specify a name. For example, Admin Console Access for port 8080 or Secure Admin Console Access for port 8443.
Name or IP address	Specify the IP address of the Administration Console.
External Port number for this service	Specify the port. Open the following ports: ◆ 8080 ◆ 8443

4 (Conditional) If you are importing an Access Gateway into the Administration Console, add the following ports:

- 1443
- 8444
- 1289
- 1290
- 524
- 636

For specific information about the ports listed in Step 3 and Step 4, see Table 1-3 on page 30.

5 (Conditional) If you are importing an Access Gateway Appliance, click **ICMP**, select all options, then click **OK** twice.

6 Run the following commands to restart Tomcat:

```
net stop Tomcat7
net start Tomcat7
```

7 Continue with "Logging In to the Administration Console" on page 44:

Logging In to the Administration Console

IMPORTANT: The Administration Console is a combination of iManager and a device manager. It has been customized for Access Manager so that it can manage the Access Manager components.

You cannot use it to log in to other eDirectory trees and manage them.

Do not download and add iManager plug-ins to this customized version. It may result in destroying the Access Manager schema, which can prevent you from managing Access Manager components. This can also prevent communication among the modules.

Do not start multiple sessions of the Administration Console on the same machine through the same browser. Browser shares session information and this can cause unpredictable issues in the Administration Console. You can, however, start different sessions with different brands of browsers.

Do not apply Group Policy Object (GPO) settings to your browser while accessing Administration Console because the GPO settings might not allow some contents to display.

To log in to:

1 Enable browser pop-ups.

2 On the Administration Console, ensure that ports 8080 and 8443 are open.

  For information about how to do this, see "Configuring the Linux Administration Console Firewall" on page 41 and "Configuring the Windows Administration Console Firewall" on page 43.

3 From a client machine external to your Administration Console server, launch browser and specify the Administration Console URL.

  Use the IP address established when you installed the Administration Console. It should include ports `8080` (HTTP) and `8443` (HTTPs) (if it is installed on a separate machine) and ports `2080` (HTTP) and `2443` (HTTPs) (when Identity Server is installed on the same machine) and the application `/nps`. If the IP address of your Administration Console for example is 10.10.10.50, specify the following:

```
http://10.10.10.50:8080/nps
```

4 Click **OK** to accept the certificate. You can select either the permanent or temporary session certificate option.

5 On the Login page, specify the administrator name and password that you defined during the Administration Console installation.

6 Click **Login**. Access Manager Dashboard opens.

  For more information about this view or about configuring the Administration Console, see Configuring the Default View in the NetIQ Access Manager 4.2 Administration Guide .

  IMPORTANT: All configuration and management tasks in the Access Manager documentation assume that you know how to log in to the Administration Console.

7 Continue with one of the following:

  - Before you can configure the system, you need to install other Access Manager components. You need to install at least one Identity Server and one Access Gateway. It is recommended to next install the Identity Server. See Chapter 3, "Installing the Identity Servers," on page 47.
  - If your Administration Console server has multiple interface cards, see "Enabling the Administration Console for Multiple Network Interface Cards" on page 45.

NOTE: You can provide fault tolerance for the configuration store on the Administration Console by installing secondary versions of the console. See "Installing Access Manager Components in NAT Environments" on page 24.

Enabling the Administration Console for Multiple Network Interface Cards

Making the Administration Console available for all network interface cards (NICs) is a security risk. However, you might want to allow this situation if, for example, the Identity Server has multiple NICs and is also available on all ports. You must modify the `server.xml` file:

1 Open the `server.xml` file, which is found in the following directory.

  Linux: `/opt/novell/nam/adminconsole/conf`

  Windows Server 2012 R2: `\Program Files (x86)\Novell\Tomcat\conf`

2 Locate the connector with the `NIDP_Name="connector"` set.

3 Delete the `address` attribute and save the file.

3 Installing the Identity Servers

Identity Server is the second component you install. You can install it on Linux or Windows. Clients that authenticate directly to the Identity Server can use any browser or operating system.

This chapter explains how to install the Identity Server. Topics include:

- "Prerequisites" on page 47
- "Installing the Identity Server on Linux" on page 48
- "Installing the Identity Server on Windows" on page 50
- "Verifying the Identity Server Installation" on page 51
- "Translating the Identity Server Configuration Port" on page 52

Prerequisites

- If you are installing Access Manager components on multiple machines, ensure that the time and date are synchronized on all machines.
- Ensure that the Administration Console is running. (See Chapter 2, "Installing the Administration Console," on page 37.)
- Do not perform any configuration tasks in the Administration Console during an Identity Server installation.
- If you installed the Administration Console on a separate machine, ensure that the DNS names resolve between the Identity Server and the Administration Console.
- When you are installing the Identity Server on a separate machine (recommended for production environments), ensure that the following ports are open on both the Administration Console and the Identity Server:

  8444
  1443
  1289
  1290
  524
  636

  For information about how to open ports, see "Configuring the Linux Administration Console Firewall" on page 41 and "Configuring the Windows Administration Console Firewall" on page 43.

  IMPORTANT: When you are installing the Identity Server on a machine with the Administration Console (not recommended for production environments), do not run simultaneous external installations of the Identity Server and Access Gateway. These installations communicate with the Administration Console. During installation, Tomcat is restarted, which can disrupt the component import process.

- Verify that the machine meets the minimum requirements. See "Installation Requirements on Linux" on page 48.
- You must establish a static IP address for your Identity Server to reliably connect with other Access Manager components. If the IP address changes, the Identity Server can no longer communicate with the Administration Console.

Installing the Identity Server on Linux

- "Installation Requirements on Linux" on page 48
- "Installation Procedure" on page 49

Installation Requirements on Linux

- 4 GB RAM
- Dual CPU or Core (3.0 GHz or comparable chip)
- 100 GB hard disk

  This amount is recommended to ensure ample space for logging in a production environment. This disk space must be local and not remote.
- One of the following operating systems:
  - SUSE Linux Enterprise Server (SLES) 11 SP4 and SLES 12 with 64-bit operating system x86-64 hardware. (physical or virtual). Ensure that the following packages are installed:
    - rsyslog-module-gtls
    - rsyslog
    - binutils
  - Red Hat Enterprise Linux (RHEL) 6.7 and 7.1 (64-bit) (physical or virtual). For installing the RHEL packages, see *Appendix 5, "Installing Packages and Dependent RPMs on RHEL for Access Manager," on page 69.*
- gettext
- python (interpreter)
- Static IP address.

IMPORTANT:

- No LDAP software, such as eDirectory or OpenLDAP, can be installed. (A default installation of SLES installs and enables OpenLDAP.)
- Because of library update conflicts, you cannot install Access Manager on a Linux User Management (LUM) machine.

For information about network requirements, see "Network Requirements" on page 21.

Installation Procedure

Installation time: about 10 minutes.

What you need to know to install the Identity Server	◆ Username and password of the administrator. ◆ (Conditional) IP address of the Administration Console if it is installed on a separate machine.

1. Open a terminal window.
2. Log in to as a `root` user.
3. Access the install script.
   - **3a** Ensure that you have downloaded the software or that you have the CD available.

     For software download instructions, see the release-specific Readme.
   - **3b** Do one of the following:
     - If you are installing from CD or DVD, insert the disc into the drive, then navigate to the device. The location might be `/media/cdrom`, `/media/cdrecorder`, or `/media/dvdrecorder`, depending on your hardware.
     - If you downloaded the `tar.gz` file, unzip the file by using the following command:

       ```
       tar -xzvf <filename>
       ```
   - **3c** Change to the `novell-access-manager` directory.
4. At the command prompt, run the following install script:

   ```
   ./install.sh
   ```
5. When you are prompted to install a product, specify 2, **Install Identity Server**, then press Enter.

   This selection is also used for installing additional Identity Servers for clustering behind an L4 switch. You need to run this install for each Identity Server you add to the cluster.

   NOTE: The Administration Console is accessible on ports 2080 (HTTP) and 2443 (HTTPs) if the Identity Server is installed on the same machine.

   The following warning is displayed:

   ```
   Warning: If NAT is present between this machine and Administration Console,
   configure NAT in the Administration Console.
   Exit this installation if NAT is not configured in the Administration Console.
   Would you like to continue (y/n)?
   ```

   For more information about how to configure NAT, see “Configuring the Administration Console Behind NAT” on page 27.
6. Specify Y to proceed.
7. Review and accept the License Agreement.
8. Specify the IP address, user ID, and password for of the primary Administration Console. Specify the local NAT IP address if local NAT is available for the Identity Server.

   If the installation program rejects the credentials and IP address, ensure that the correct ports are open on both the Administration Console and the Identity Server, as described in “Prerequisites” on page 47.
9. The following components are installed:

Component	Description
Access Manager Server Communication	Enables network communications, including identifying devices, finding services, moving data packets, and maintaining data integrity.
Identity Server	Provides authentication and identity services for the other Access Manager components and third-party service providers.
Identity Server Configuration	Allows the Identity Server to be securely configured by the Administration Console. If the installation process terminates at this step, the probable cause is a failure to communicate with the Administration Console. Ensure that you specified the correct IP address.
Access Manager Server Communications Configuration	Enables the Identity Server to auto-import itself into the Administration Console.

10 Continue with one of the following:

- Verify the installation. See "Verifying the Identity Server Installation" on page 51
- Install an Access Gateway. See "Installing the Access Gateway Appliance" on page 59 or "Installing the Access Gateway Service" on page 62.
- Configure the Identity Server. See Setting Up a Basic Access Manager Configuration in the NetIQ Access Manager 4.2 Administration Guide .

NOTE: After you install an Identity Server, you must create a cluster configuration. See Identity Servers Cluster in the NetIQ Access Manager 4.2 Administration Guide .

Installing the Identity Server on Windows

- "Installation Requirements on Windows" on page 50
- "Installation Procedure" on page 51

Installation Requirements on Windows

- 4 GB RAM
- Dual CPU or Core (3.0 Ghz or comparable chip)
- 100 GB hard disk

  This amount is recommended to ensure ample space for logging in a production environment. This disk space must be local and not remote.
- Windows Server 2012 R2 (physical or virtual), 64-bit operating system, in either Standard or Enterprise Edition, with the latest patches applied
- Static IP address

IMPORTANT: No LDAP software, such as eDirectory or OpenLDAP, can be installed. (A default installation of SLES installs and enables OpenLDAP)

For information about network requirements, see "Network Requirements" on page 21.

Installation Procedure

Installation time: about 10 minutes.

What you need to know to install the Identity Server	◆ Username and password of the administrator. ◆ (Conditional) IP address of the Administration Console if it is installed on a separate machine.

1 Verify that the machine meets the minimum requirements. See "Installation Requirements on Windows" on page 50.

   Ensure that you have read and implemented prerequisites specified in "Prerequisites" on page 47.

2 Close any running applications and disable any virus scanning programs.

3 (Conditional) If you have installed the Administration Console on this server, ensure that you have restarted the server before installing the Identity Server.

4 Download software and run it.

   For software download instructions, see the release-specific Readme.

5 Read the introduction, then click **Next**.

6 Accept the license agreement, then click **Next**.

7 Select **Access Manager Identity Provider**, then click **Next**.

   A warning is displayed: `If NAT is present between this machine and Administration Console, the NAT configuration needs to be done in Administration Console`.

8 Specify the IP address, user ID, and password for the primary Administration Console.

9 (Optional) Specify the Identity Server Local NAT IP address, if the device is behind NAT.

10 Click **Next**, review the summary, and click **Install**.

11 (Conditional) If you are installing the Identity Server on a machine that contains a previous installation of the Administration Console, you are asked whether the program should overwrite an existing file in the `\Program Files\Novell` directory. Specify yes.

12 Continue with one of the following:

   - Verify the installation. See "Verifying the Identity Server Installation" on page 51
   - Install an Access Gateway. See "Installing the Access Gateway Appliance" on page 59 or "Installing the Access Gateway Service" on page 62.
   - Configure the Identity Server. See Configuring an Identity Server in the NetIQ Access Manager 4.2 Administration Guide .

NOTE: After you install an Identity Server, you must create a cluster configuration. See Identity Servers Cluster in the NetIQ Access Manager 4.2 Administration Guide .

Verifying the Identity Server Installation

1 Log in to the Administration Console.

   See "Logging In to the Administration Console" on page 44.

2 Click **Devices** > **Identity Servers**.

Translating the Identity Server Configuration Port

If your Identity Server must communicate through a firewall, you must either set up a hole in your firewall for TCP ports 8080 or 8443 (default ports used respectively for non secure and secure communication with Identity Server), or configure the Identity Server service to use TCP port 80 or 443.

- "Changing the Port on a Windows Identity Server" on page 52
- "Changing the Port on a Linux Identity Server" on page 52

Changing the Port on a Windows Identity Server

On a Windows Identity Server, you need to set the port in the Base URL and save the changes. You then need to modify the `server.xml` file located in the Tomcat configuration directory:

1. In the Administration Console, click **Devices** > **Identity Server > Edit**, and configure the base URL with HTTPS as the protocol, and the TCP port as 443.
2. Click **OK**, then update the Identity Server.
3. In a terminal window, open the `server.xml` file.

   Windows Server 2012 R2: `\Program Files (x86)\Novell\Tomcat\conf`
4. Change the ports from 8080 and 8443 to 80 and 443.
5. Restart the Tomcat service.

   ```
   net stop Tomcat7
   ```

   ```
   net start Tomcat7
   ```

Changing the Port on a Linux Identity Server

On a Linux Identity Server, the Identity Server service (hosted on Tomcat) runs as a non-privileged user on Linux and cannot therefore bind to ports below 1024. In order to allow requests to port 80/443 while Tomcat is listening on 8080/8443, the preferred approach is to use iptables to perform a port translation. Port translation allows the base URL of the Identity Server to be configured for port 443 and to listen on this port, and the iptables translates it to port 8443 when communicating with Tomcat.

- If you have disabled the SUSE Linux Enterprise Server (SLES) firewall and do not have any other Access Manager components installed on the Identity Server, you can use a simple iptables script to translate the ports. See "A Simple Redirect Script" on page 53.
- If you have configured the SLES firewall or have installed other Access Manager components on the Identity Server, you use a custom rule script that allows for multiple port translations. See "Configuring iptables for Multiple Components" on page 55.

These sections describe two solutions out of many possibilities. For more information about iptables, see the following:

- "Iptable Tutorial 1.2.2"
- "NAM Filters for iptables Commands"

A Simple Redirect Script

This simple solution works only if you are not using iptables to translate ports of other applications or Access Manager components. For a solution that works with multiple components, see "Configuring iptables for Multiple Components" on page 55.

1. In the Administration Console, click **Devices** > **Identity Server > Edit**, and configure the base URL with HTTPS as the protocol, and the TCP Port as 443.
2. Click **OK**, then update the Identity Server.
3. At a terminal window, log in as the `root` user.
4. Create a file to hold the iptables rule and place it in the `/etc/init.d` directory.

   For example, `/etc/init.d/AM_IDP_Redirect`. Ensure it has execute rights. You can use CHMOD as appropriate.

   An example of a redirect startup file for this purpose might be:

```
#!/bin/sh
# Copyright (c) 2010 Novell, Inc.
# All rights reserved.
#
#! /bin/sh
#! /etc/init.d/idp_8443_redirect
# ### BEGIN INIT INFO
# Provides: idp_8443_redirect
# Required-Start:
# Required-Stop:
# Default-Start: 2 3 5
# Default-Stop: 0 1 6
# Description: Redirect 8443 to 443 for Novell IDP
### END INIT INFO #

# Environment-specific variables.
IPT_BIN=/usr/sbin/iptables
INTF=eth0
ADDR=10.10.0.1

. /etc/rc.status



# First reset status of this service
rc_reset

case "$1" in
    start)
        echo -n "Starting IP Port redirection"
        $IPT_BIN -t nat --flush
        $IPT_BIN -t nat -A PREROUTING -i $INTF -p tcp --dport 80 -j DNAT --to
${ADDR}:8080
        $IPT_BIN -t nat -A PREROUTING -i $INTF -p tcp --dport 443 -j DNAT --to
${ADDR}:8443
        $IPT_BIN -t nat -A OUTPUT -p tcp -d $ADDR --dport 443 -j DNAT --to
${ADDR}:8443
        $IPT_BIN -t nat -A OUTPUT -p tcp -d $ADDR --dport 80 -j DNAT --to
${ADDR}:8080
        rc_status -v
        ;;
    stop)
```

```
        echo -n "Flushing all IP Port redirection rules"
        $IPT_BIN -t nat --flush
        rc_status -v
        ;;
    restart)
        $0 stop
        $0 start
        rc_status
        ;;
    *)
        echo "Usage: $0 {start|stop|restart}"
        exit 1
        ;;
esac
rc_exit
```

For more information about init scripts for SUSE Linux Enterprise Server 10, see "Section 20.2.2 Init Scripts" in the *SUSE Linux Enterprise Server 10 Installation and Administration Guide* (http://www.novell.com/documentation/sles10/index.html).

For more information about init scripts for SUSE Linux Enterprise Server 11, see "Section 7.2.2 Init Scripts" in the *SLES 11 Administration Guide*.

5 Modify the environment-specific variables found in the following lines:

```
# Environment-specific variables.
IPT_BIN=/usr/sbin/iptables
INTF=eth0
ADDR=10.10.0.1
```

6 To ensure that the iptables rule is active after rebooting, start YaST, click **System**, > **System Services (Runlevel)**, select **Expert Mode**, select the file you created, enable runlevels boot, 3 and 5 for the file, then start the service.

7 To verify that your script is running, enter the following command:

```
ls /etc/init.d/rc3.d | grep -i AM_IDP_Redirect
```

8 Reboot the Identity Server machine.

9 After rebooting, verify that port 443 is being routed to the Identity Server by entering the following command:

```
iptables -t nat -nvL
```

You should see an entry similar to the following:

```
pkts bytes target     prot opt in     out     source               destination
17   748    DNAT      tcp  --  eth0   *      0.0.0.0/0            0.0.0.0/0
tcp dpt:443 to:10.10.0.1:8443
```

This entry states that eth0 is routing TCP port 443 to IP address 10.10.0.1.

10 (Conditional) If your Identity Server cluster configuration contains more than one Identity Server, repeat these steps on each server in the cluster.

Configuring iptables for Multiple Components

If you need to use iptables for multiple components (the host machine, the Identity Server), you need to centralize the commands into one manageable location. The following sections explain how to use the SuSEFirewall2 option in YaST to centralize the commands.

The Identity Server uses requires pre-routing commands.

Adding the Identity Server Commands

1. In the Administration Console, click **Devices** > **Identity Server > Edit**, and configure the base URL with HTTPS as the protocol, and the TCP port as 443.
2. Click **OK**, then update the Identity Server.
3. On the Identity Server, edit the `/etc/sysconfig/SuSEfirewall2` file.

   3a Change the FW_CUSTOMRULES="" line to the following:

   ```
   FW_CUSTOMRULES="/etc/sysconfig/scripts/SuSEfirewall2-custom"
   ```

   3b Save the changes and exit.
4. Open the `/etc/sysconfig/scripts/SuSEfirewall2-custom` file in an editor.

   This is the custom rules file you specified in Step 3.
5. Add the following lines under the `fw_custom_before_port_handling()` section:

   ```
   iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j DNAT --to
   10.10.0.1:8443
   iptables -t nat -A OUTPUT -p tcp -o eth0 --dport 443 -j DNAT --to
   10.10.0.1:8443
   true
   ```

   The first command rewrites all incoming requests with a destination TCP port of 443 to TCP port 8443 on the 10.10.0.1 IP address for eth0. Modify the IP address to match the IP address of your Identity Server.

   The second command rewrites the health checks.
6. Save the file.
7. At the system console, restart the firewall by executing the following command:

   ```
   /etc/init.d/SuSEfirewall2_setup restart
   ```
8. After rebooting, verify that port 443 is being routed to the Identity Server by entering the following command:

   ```
   iptables -t nat -nvL
   ```

   You should see an entry similar to the following:

   ```
   pkts bytes target    prot opt in    out    source            destination
   17   748 DNAT      tcp  --  eth0   *      0.0.0.0/0          0.0.0.0/0
   tcp dpt:443 to:10.10.0.1:8443
   ```

   This entry states that eth0 is routing TCP port 443 to IP address 10.10.0.1:8443.
9. (Conditional) If your Identity Server cluster configuration contains more than one Identity Server, repeat these steps on each server in the cluster.

4 Installing the Access Gateway

You can install the Access Gateway in one of the following two modes:

- Appliance: Operating system is installed with the Access Gateway software.
- Service: The Access Gateway installed on a machine with an existing operating system.

This chapter explains the difference between Access Gateway Appliance and Access Gateway Service and how to install the Access Gateway. Topics include:

- “Feature Comparison of Different Types of Access Gateways” on page 57
- “Installing the Access Gateway Appliance” on page 58
- “Installing the Access Gateway Service” on page 62
- “Verifying the Access Gateway Installation” on page 66

Feature Comparison of Different Types of Access Gateways

Access Manager includes the Access Gateway Appliance and Access Gateway Service. The Access Gateway Appliance installs its own embedded Linux operating system. Whereas, the Access Gateway Service runs on top of an existing installation of a Linux or Windows operating system. Both types of gateways support similar functionalities, but they differ slightly in the way some of these features are supported. For example, both can be configured for the following features:

- Protecting Web resources with contracts, Authorization, Form Fill, and Identity Injection policies.
- Providing fault tolerance by clustering multiple gateways of the same type.
- Providing fault tolerance by grouping multiple Web servers, so that if one Web server goes down, the content can be retrieved from another server in the group.
- Rewriting URLs so that the names and IP addresses of the Web servers are hidden from the users making requests.
- Generating alert, audit, and logging events with notify options.

Most differences between Access Gateway Appliance and Access Gateway Service result from the differences required for an appliance and for a service. An appliance can know, control, and configure many features of the operating system. A service that runs on top of an operating system can query the operating system for some information, but it cannot configure or control the operating system. For the service, operating system utilities must be used to configure system parameters and hardware. For the appliance, the operating system features that are important to the appliance, such as time, DNS servers, gateways, and network interface cards, can be configured in the Administration Console.

This table describes the differences between Access Gateway Appliance and Access Gateway Service. Only your network and Web server configurations can determine whether the differences are significant.

Table 4-1 *Differences between Access Gateway Appliance and Access Gateway Service:*

Feature	Access Gateway Appliance	Access Gateway Service
Platform support	SLES 11 SP4 only	◆ SLES 11 SP4 ◆ SLES 12 ◆ Red Hat Enterprise Linux 6.7 ◆ Red Hat Enterprise Linux 7.1 ◆ Windows 2012 R2
Network configuration ◆ DNS servers ◆ Gateways ◆ Network interface cards ◆ Host names	Configurable from the Administration Console. By default after the installation, only one network interface card will be displayed in the Administration Console. To detect other network interface card, do the following: ◆ Configure a primary IP Address in YaST for the remaining interfaces. ◆ Click **Devices > Access Gateways > Select the device > New IP > click OK**.	Configurable with standard operating system utilities.
Date and time	Configurable from the Administration Console.	Configurable with standard operating system utilities.
Cache directory	Uses Apache-caching. The cached files are stored in clear text. The operating system must be configured to protect this directory. For more information about the Apache model, see “Caching Guide”.	Uses filesystem provided by Apache mod_cache module. For more information about the Apache model, see “Caching Guide”.

Installing the Access Gateway Appliance

- “Access Gateway Appliance Requirements” on page 58
- “Installing the Access Gateway Appliance” on page 59

Access Gateway Appliance Requirements

The Access Gateway Appliance runs 64bit operating system on x86-64 hardware supported by SLES 11 SP4. Install it on a separate server because it clears the hard drive and sets up a soft appliance environment.

The Access Gateway Appliance requires the following hardware:

- 4 GB RAM
- Dual CPU or Core (3.0 GHz or comparable chip)
- 100 GB hard disk

The hard disk should have ample space for logging in a production environment. This disk space must be local and not remote.

- A static IP address for your Access Gateway server and an assigned DNS name (host name and domain name).

For information about network requirements, see "Network Requirements" on page 21.

For a list of hardware that SLES 11 SP4 for x86-64 hardware supports, open YES CERTIFIED Bulletin (http://developer.novell.com/yessearch/Search.jsp), select Service Pack 4 for SUSE® SLES 11 in NetIQ Product, and search for your other hardware requirements.

The Access Gateway Appliance has no software requirements. The installation program re-images the hard drive, embeds the Linux operating system, then configures the embedded operating system for optimal performance.

Installing the Access Gateway Appliance

Installation time: 15 to 30 minutes, depending upon the hardware.

What you need to know	◆ Username and password of the administrator. ◆ IP address of the Administration Console. ◆ Static IP address for the Access Gateway. ◆ DNS name (host and domain name) for the Access Gateway that resolves to the IP address. ◆ Subnet mask that corresponds to the IP address for the Access Gateway. ◆ IP address of your network's default gateway. ◆ IP addresses of the DNS servers on your network. ◆ IP address or DNS name of an NTP server.

The Access Gateway Appliance can be installed on all supported hardware platforms for SUSE Linux Enterprise Server (SLES) 11 SP4 or a higher version.

IMPORTANT: After the Access Gateway Appliance installation, upgrade the Linux kernel to the latest security patch to avoid any security vulnerabilities. For more information, see Chapter 10, "Getting the Latest Security Patches," on page 103.

This section provides the following information about how to install the Access Gateway Appliance:

- "Prerequisites" on page 59
- "Installing the Access Gateway Appliance" on page 60
- "Creating Custom Partitions" on page 61

Prerequisites

- Ensure that you have backed up all data and software on the disk to another machine. The Access Gateway Appliance installation completely erases all the data on your hard disk.

- Ensure that the server meets the minimum hardware requirements. See "Access Gateway Appliance Requirements" on page 58.
- (Optional) If you want to try any advanced installation options such as driver installation or network installation, see the SUSE Linux Enterprise Server 11 Installation Guide (https://www.suse.com/documentation/sles11/book_sle_deployment/data/book_sle_deployment.html).

Installing the Access Gateway Appliance

1. Insert the Access Gateway Appliance CD into the CD drive and boot from CD. The boot screen appears.
2. By default, the **Boot From Hard Disk** option is selected. Use the Down-arrow key to select **Install Appliance**.
3. Press Enter.
4. Review the agreement on the License Agreement page, then click **I Agree**.
5. Select the region and time zone on the Clock and Time Zone page.
6. (Conditional) If the date and time are not the same as the date and time on the Administration Console, click Change, adjust the date and time.
7. Click **Next**.
8. Configure the following details on the Appliance Configuration page:

Field	Description
Host Name	The hostname of the Access Gateway Appliance server. **IMPORTANT:** Do not use `linux` as hostname. If you do, the Access Gateway is not imported
Domain Name	The domain name for your network.
IP Address	The IP address of the Access Gateway.
Subnet Mask	The subnet mask of the Access Gateway Appliance network.
Default Gateway	The IP address of the default gateway.
DNS Server	The IP address of your DNS server. You must configure at least one DNS server. Specify the IP address of additional your additional DNS server, if you have configured. This is an optional configuration.
In the Root Password section, specify password.	
In the NTP Server Configuration section, specify the name of the NTP server.	
In the NAT Settings section, specify the Access Gateway Local NAT IP Address, if the device is behind NAT.	
In the Administration Console configuration section, specify the following:	
IP Address	The IP address of the Administration Console. The Access Gateway Appliance is imported into this Administration Console.
Username	The name of the Administration Console user.
Password	Specify the password for the user.

9 Click **Next**. The Installation Settings page appears.

This page displays the options and software you selected in the previous steps. Use the Overview tab for a list of selected options, or use the Expert tab for more details. Ensure that all default partitions recommended adhere to the guidelines mentioned in Table 4-2 on page 61.

NOTE: Do not change the software selections listed on this screen.

10 (Optional) To modify the installation settings for partitions, click **Change**. For more information about partitions, see "Creating Custom Partitions" on page 61.

11 Click **Install** > **Install**.

This process might take 15 to 30 minutes, depending on the configuration and hardware.

The machine reboots after the installation is completed. It runs an auto import script, and then the Access Gateway Appliance is imported to the Administration Console.

12 Continue with one of the following sections:

- Verify the installation. See "Verifying the Access Gateway Installation" on page 66
- Configure the Access Gateway. See Configuring the Access Gateway in the NetIQ Access Manager 4.2 Administration Guide .

The Access Gateway Appliance is installed with the following default partitions:

- **boot:** The size is automatically calculated and the mount point is `/boot`.
- **swap:** The size is double of the size of RAM and the mount point is `swap`.

The remaining disk space after the creation of the /boot and swap partitions is allocated as the extended drive. The extended drive has the following partitions:

- **root:** The default size is one-third the size of the extended drive and the mount point is `/`.
- **var:** The default size is one-third the size of the extended drive and the mount point is `/var`.

The Access Gateway Appliance does not support configuring multiple network interfaces during installation. The eth0 interface is configured by default. If you require multiple interfaces, you can configure them through the Administration Console after installation.

Creating Custom Partitions

Linux allows you to have four primary partitions per hard disk. The Access Gateway Appliance requires a swap partition, a var partition, and a root partition. For a machine with a large hard disk (100 GB or larger), we recommend creating the following partitions:

Table 4-2 *Access Gateway Appliance Partitions*

Partition Type	Requirements
root	This partition contains the boot files, system files, and log files. You should assign 40% of available disk space to this partition. This space should be more than 40 GB.
swap	Create a swap partition that is twice the size of RAM installed on the machine.
var	This partition is used for log files and caching objects of the Access Gateway. Allocate the remaining space for this partition, which should be more than 50 GB. Assign the remaining disk space to var.

To create your custom partitions:

1 In the Installation Settings page, click **Change**, then select **Partitioning**. (See Step 10 on page 61.)

  This page lists the partition settings as currently proposed.

2 Select **Custom partitioning**, then click **Next**.

3 (Conditional) If the installation program discovers any existing partitions, select the hard disk, click **Delete**, then confirm the deletion of the partitions.

4 Create a root partition as follows:

  4a Click **Add**, select the primary or extended partition, then click **OK**.

  4b Specify the following details:

  Format: Ensure that **Format** is selected.

  You must format the partition after you have modified the partition size during installation.

  File system: Select **Ext3** for the type.

  Custom Size: Specify a value.

  Mount Point: Select **/**.

  4c Click **Finish**.

5 Create a swap partition as follows:

  5a Select the hard drive, click **Create**, select the primary or extended partition, then click **OK**.

  5b Specify the following details:

  Format: Ensure that **Format** is selected.

  File system: Select **Swap** for the type.

  Custom Size: Specify `a value`.

  Mount Point: Leave the default value of **swap**.

  5c Click **Finish**.

6 Create a var partition as follows:

  6a Select the hard drive, click **Add**, select the primary or extended partition, then click **OK**.

  6b Specify the following details:

  Format: Ensure that **Format** is selected.

  File system: Select **Ext3** for the type.

  Custom Size: Specify a value.

  Mount Point: Select **/var**.

  6c Click **Finish**.

7 Click **Accept** to create partitions with the specified values.

8 In the installation Summary page, verify that the partitions you specified are listed, then continue with Step 11 on page 61.

Installing the Access Gateway Service

- "Installing the Access Gateway Service on Linux" on page 63
- "Installing the Access Gateway Service on Windows" on page 65

Installing the Access Gateway Service on Linux

IMPORTANT: Because of library update conflicts, you cannot install Access Manager on a Linux User Management machine.

- "Linux Requirements" on page 63
- "Prerequisites" on page 63
- "Installation Procedure" on page 64

Linux Requirements

- One of the following operating systems:
  - SUSE Linux Enterprise Server (SLES) 11 SP4 and SLES 12 (64-bit) (physical or virtual).
  - Red Hat Enterprise Linux (RHEL) 6.7 (64-bit) (physical or virtual) and 7.1 (64-bit) (physical or virtual)
- 4 GB RAM.
- Dual CPU or Core (3.0 GHz or comparable chip).
- 2 to10 GB hard disk space per reverse proxy that requires caching and for log files. The amount varies with rollover options and logging level that you configure.
- A static IP address and a DNS name. The ActiveMQ module of the Access Gateway Service must be able to resolve the machine's IP address to a DNS name. If the module can't resolve the IP address, the module does not start.
- Other Access Manager components should not be installed on the same machine.
- For installing the RHEL packages, see Appendix 5, "Installing Packages and Dependent RPMs on RHEL for Access Manager," on page 69.
- (Only for SLES) Ensure that the following rpms or higher versions are installed:
  - rsyslog-module-gtls-5.10.1-0.7.49
  - rsyslog-5.10.1-0.7.49
  - binutils 2.23.1-0.17.18

  IMPORTANT

  - SLES installation libraries may be distributed across multiple CDs or DVDs. In **YaST > Software > Software Repositories** select the required CD or DVD to install the rpm files. If the rpm files are not available on the SLES server, the Access Manager installation process takes care of installing these rpm files from the SLES repository.
  - To search if an rpm is installed, use `rpm -qa | grep` <*rpm name*>. For example, `rpm - qa | grep libapr-util`.

For information about network requirements, see "Network Requirements" on page 21.

Prerequisites

- An Administration Console must be installed before you install the Access Gateway Service. See Section 2, "Installing the Administration Console," on page 37.
- An Identity Server must be installed and configured before installing the Access Gateway Service. See, Section 3, "Installing the Identity Servers," on page 47.

- Verify that the server meets the minimum requirements. See "Installing the Access Gateway Service on Linux" on page 63.
- Verify that the time on the machine is synchronized with the time on the Administration Console. If the times differ, the Access Gateway Service does not import into the Administration Console.
- If a firewall separates the machine and the Administration Console, ensure that the required ports are opened. See Table 1-3 on page 30.
- Because the Access Gateway Service is running as a service, the default ports (80 and 443), which the Access Gateway Service uses might conflict with the ports of other services running on the machine. If there is a conflict, you need to decide which ports each service can use.
- (Windows Server 2012) If the Web server (IIS) has been installed by default during the Windows Server 2012 install. The Access Gateway Service installation program detects its presence from the registry and issues a shutdown command. Even if you have never activated the Web server and if even it is not running, the shutdown command is issued. Because the Access Gateway Service cannot be installed while the IIS server is running, the installation program needs to ensure that it is not running.

NOTE: The Access Gateway Service clustering is supported for devices that are on the same operating system.

Installation Procedure

Installation time: about 10 minutes.

What you need to know	- Username and password of the administrator. - IP address of the Administration Console.

IMPORTANT: The Access Gateway Service must be installed on a separate machine.

1 Log in to the Novell Customer Center (http://www.novell.com/center) and follow the link that allows you to download software. For an evaluation version, download the media kit from Novell Downloads (http://download.novell.com/index.jsp).

2 Copy the file to your machine.

For the filename, see the NetIQ Access Manager Readme.

3 Prepare your machine for installation:

Make your operating system installation media available.

The installation program checks for Apache dependencies and installs any missing packages.

4 Start installation by running the following script:

```
./ag_install.sh
```

5 Review and accept the License Agreement.

6 Specify the IP address, user ID, and password of the primary Administration Console.

7 (Optional) Specify the local NAT IP address if the local NAT is available for the Access Gateway.

8 Continue with one of the following sections:

- Verify the installation. See "Verifying the Access Gateway Installation" on page 66
- Configure the Access Gateway. See Configuring the Access Gateway in the NetIQ Access Manager 4.2 Administration Guide .

Installing the Access Gateway Service on Windows

- "Windows Requirements" on page 65
- "Installation Procedure" on page 65

Windows Requirements

- Windows Server 2012 R2, 64-bit operating system in Standard Edition with the latest patches applied (physical or virtual)
- 4 GB RAM
- Dual CPU or Core (3.0 GHz or comparable chip)
- 2 to10 GB per reverse proxy that requires caching and for log files. The amount varies with rollover options and logging level that you configure
- A static IP address and a DNS name. The ActiveMQ module of the Access Gateway Service must be able to resolve the machine's IP address to a DNS name. If the module cant resolve the IP address, the module does not start.

  You can verify this by using the `nslookup` command. Enter this command with hostname in the command prompt and it should return the IP address of the host
- Other Access Manager components should not be installed on the same machine

For information about network requirements, see "Network Requirements" on page 21.

For prerequisites, see "Prerequisites" on page 59.

Installation Procedure

Installation time: about 10 minutes.

What you need to know	◆ Username and password of the administrator. ◆ IP address of the Administration Console.

IMPORTANT: The Access Gateway Service must be installed on a separate server.

1 Log in to the NetIQ Customer Center (http://www.novell.com/center) and follow the link that allows you to download software. For an evaluation version, download the media kit from NetIQ Downloads (https://dl.netiq.com/index.jsp).

2 Copy the file to your machine.

   For the filename, see the release-specific NetIQ Access Manager Readme.

3 Disable any virus scanning programs.

4 To use a remote desktop for installation, use one of the following:

   - Current version of VNC viewer
   - Microsoft Remote Desktop with the `/console` switch for Windows XP SP2
   - Microsoft Remote Desktop with the `/admin` switch for Windows XP SP3

5 Double click the executable file.

   A warning is displayed stating `If NAT is present between console, the NAT configuration needs to be done in Administration Console`.

If NAT is configured then ensure that you configure the same in the Administration Console. Else, click **Continue** >**Next**.

6. Review the readme, and click **Next**.
7. Review and accept the License Agreement, then click **Next**.
8. Specify the IP address, user ID, and password of the primary Administration Console.
9. (Conditional) Specify the local IP address, if your machine has more than one IP address, which the Access Gateway Service will use for communication with the Administration Console.
10. (Optional) Specify the Access Gateway Local NAT IP address, if the device is behind NAT.
11. Click **Next**.
12. Configure disk cache. This holds the caching objects of the Access Gateway.

    NOTE: The Access Gateway Appliance uses the mod_cache module filesystem provided by Apache for storing the caching objects. If you want to change the size of this cache after installation, see TID on Changing the Cache Size of an Access Gateway Appliance after Installation.

13. Click **Next**, then review the installation summary.
14. Click **Install**.
15. Review the log information at the following location:

    ```
    C:\Program Files\Novell\log
    ```

16. Click **Next** > **Done**.
17. To verify that the Access Gateway Service imported into the Administration Console, wait for few minutes, log in to the Administration Console, then click **Devices** > **Access Gateways**.

    At this point, the Access Gateway Service is not configured.

18. Continue with one of the following:
    - "Verifying the Access Gateway Installation" on page 66
    - Configure the Access Gateway. See Configuring the Access Gateway in the NetIQ Access Manager 4.2 Administration Guide .
    - Install another Access Manager component.

Verifying the Access Gateway Installation

1. Log in to the Administration Console.

   See "Logging In to the Administration Console" on page 44.

2. Click **Devices** > **Access Gateways**.

   If the installation was successful, the IP address of your Access Gateway appears in the Server list.

   The Health status indicates the health state after the Access Gateway is imported and registers with the Administration Console.

   NOTE: The Access Gateway Appliance health is displayed as green instead of yellow, even before a trust relationship is established between an Embedded Service Provider and the Access Gateway. You must establish a trust relationship with the Identity Server before you proceed with any other configuration.

If an Access Gateway starts to import into the Administration Console but fails to complete the process, the following message appears:

```
Server gateway-<name> is currently importing. If it has been several minutes
after installation, click repair import to fix it.
```

If you have waited at least ten minutes, but the message doesn't disappear and the Access Gateway does not appear in the list, click the **repair import** link.

5 Installing Packages and Dependent RPMs on RHEL for Access Manager

The following table lists RHEL packages and their dependent RPMs required for each component.

NOTE:

To avoid RPM dependency issues, NetIQ Corporation recommends installing the package along with its respective dependent RPMs.

The version of RPMs varies based on the base operating system version of RHEL. The following table lists RPMs for RHEL 7.1 and 7.2.

You must install these RPMs in the same sequence as they appear in the table:

Package	Dependent RPM
iManager	
glibc-2.17-78.el7.i686.rpm	◆ nss-softokn-freebl-3.16.2.3-9.el7.i686
compat-libstdc++-33-3.2.3-69.el6.i686.rpm	◆ glibc-2.17-55.el7.i686.rpm ◆ libgcc-4.8.2-16.el7.i686.rpm
compat-libstdc++-33-3.2.3-69.el6.x86_64.rpm	◆ glibc-2.17-55.el7.i686.x86_64.rpm ◆ libgcc-4.4.7-3.el6.x86_64.r
libstdc++-4.8.2-16.el7.i686.rpm These RPMs are required for the Administration Console also.	◆ glibc-2.17-55.el7.i686.rpm ◆ libgcc-4.8.2-16.el7.i686.rpm
libstdc++-4.4.7-3.el6.x86_64.rpm (Part of the RHEL base installation)	◆ glibc-2.17-55.el7.i686.x86_64.rpm ◆ libgcc-4.8.2-16.el7.i686.rpm.x86_64.rpm
libstdc++-4.8.3-9.el7.i686	◆ glibc-2.17-78.el7.i686 ◆ libgcc-4.8.3-9.el7.i686
libstdc++-4.8.3-9.el7.x86_64	◆ libgcc-4.8.3-9.el7.x86_64
libXau-1.0.8-2.1.el7.x86_64.rpm	◆ glibc-2.17-55.el7.i686.rpm
libxcb-1.9-5.el7.x86_64.rpm	◆ glibc-2.17-55.el7.i686.rpm ◆ libXau-1.0.8-2.1.el7.x86_64.rpm
libX11-1.6.0-2.1.el7.x86_64.rpm	◆ glibc-2.17-55.el7.i686.rpm ◆ libXau-1.0.8-2.1.el7.x86_64.rpm
libXext-1.3.2-2.1.el7.x86_64.rpm	◆ libX11-1.6.0-2.1.el7.x86_64.rpm ◆ glibc-2.17-55.el7.i686.rpm

Package	Dependent RPM
libXi-1.7.2-2.1.el7.x86_64.rpm	libX11-1.6.0-2.1.el7.x86_64.rpm libXext-1.3.2-2.1.el7.x86_64.rpm glibc-2.17-55.el7.i686.rpm
libXtst-1.2.2-2.1.el7.x86_64.rpm	libX11-1.6.0-2.1.el7.x86_64.rpm libXext-1.3.2-2.1.el7.x86_64.rpm libXi-1.7.2-2.1.el7.x86_64.rpm glibc-2.17-55.el7.i686.rpm
libXtst6-32bit	Has dependency on iManager
libXtst-1.2.2-2.1.el7.i686.rpm	libX11-1.6.3-2.el7.i686.rpm libXi-1.7.4-2.el7.i686.rpm libXext-1.3.3-3.el7.i686.rpm
libX11-1.6.3-2.el7.i686.rpm	libxcb-1.11-4.el7.i686.rpm
libxcb-1.11-4.el7.i686.rpm	libXau-1.0.8-2.1.el7.i686.rpm
libXrender-0.9.8-2.1.el7.i686.rpm	No dependency
Administration Console	
gettext-0.18.2.1-4.el7.x86_64	No dependency
glibc-2.17-78.el7.i686.rpm	nss-softokn-freebl-3.16.2.3-9.el7.i686
libstdc++-4.8.2-16.el7.i686.rpm	glibc-2.17-55.el7.i686.rpm libgcc-4.8.2-16.el7.i686.rpm
ncurses-libs-5.9-13.20130511.el7.i686.rpm	glibc-2.17-55.el7.i686.rpm
libgcc-4.8.2-16.el7.i686.rpm	No dependency
rsyslog-7.4.7-7.el7_0.x86_64	No dependency
rsyslog-gnutls-7.4.7-7.el7_0.x86_64	No dependency
binutils-2.23.52.0.1-30.el7.x86_64	No dependency
gperftools-libs-2.4-7.el7.x86_64	No dependency
Identity Server	
glibc-2.17-78.el7.i686.rpm	nss-softokn-freebl-3.16.2.3-9.el7.i686
libstdc++-4.8.2-16.el7.i686	glibc-2.17-55.el7.i686.rpm libgcc-4.8.2-16.el7.i686.rpm
ncurses-libs-5.9-13.20130511.el7.i686.rpm	glibc-2.17-55.el7.i686.rpm
libgcc-4.8.2-16.el7.i686.rpm	No dependency
rsyslog-7.4.7-7.el7_0.x86_64	No dependency
rsyslog-gnutls-7.4.7-7.el7_0.x86_64	No dependency

Package	Dependent RPM
binutils-2.23.52.0.1-30.el7.x86_64	◆ No dependency
Access Gateway	
glibc-2.17-78.el7.i686.rpm	◆ nss-softokn-freebl-3.16.2.3-9.el7.i686
db4-4.7.25-17.el6.x86_64.rpm (Part of the RHEL base installation)	◆ glibc-2.17-55.el7.i686.x86_64.rpm
apr-1.4.8-3.el7.x86_64.rpm	◆ glibc-2.17-55.el7.i686.x86_64.rpm
apr-util-1.5.2-6.el7.x86_64.rpm	◆ apr-1.4.8-3.el7.x86_64.rpm ◆ glibc-2.17-55.el7.i686.x86_64.rpm
libtool-ltdl-2.4.2-20.el7.x86_64.rpm	◆ glibc-2.17-55.el7.i686.x86_64.rpm
unixODBC-2.3.1-10.el7.x86_64.rpm	◆ libtool-ltdl-2.4.2-20.el7.x86_64.rpm ◆ glibc-2.17-55.el7.i686.x86_64.rpm
libesmtp-1.0.6-7.el7.x86_64.rpm	◆ glibc-2.17-55.el7.i686.x86_64.rpm
rsyslog-7.4.7-7.el7_0.x86_64	◆ No dependency
rsyslog-gnutls-7.4.7-7.el7_0.x86_64	◆ No dependency
binutils-2.23.52.0.1-30.el7.x86_64	◆ No dependency
patch-2.7.1-8.el7.x86_64.rpm	◆ No dependency

Use the following command to verify whether a package is installed on RHEL:

```
rpm -qa | grep <package name>
```

Use the following command to install a RPM:

```
rpm -ivh  <rpm name>
```

Use the following command to install all RPMs together:

```
rpm -ivh  <rpm name> <rpm name> <rpm name >...
```

NOTE: The version of RPMs varies based on the base operating system version of RHEL.

Perform the following steps to install packages and their dependent RPMs while installing RHEL:

1 Mount the RHEL CD-ROM by running the following command and go to the `Packages` folder.:

```
mount /dev/cdrom /mnt
```

NOTE: If the RHEL CD-ROM is auto mounted, the mount path will be `/media/RHEL_x.x x86_64 Disc 1`. (The x in RHEL_x.x represents the version number) Unmount the default mount path by using the `unmount /media/RHEL_x.x\ x86_64\ Disc\ 1/`command and then mount the RHEL CD-ROM by using `mount /dev/cdrom /mnt`.

2 If you have a locally mounted ISO image, you can install RPMs for Access Manager by providing the mount path to the installer. The `install.sh` scripts prompts for the mounted disc if it identifies that the required RPMs are not installed. Provide the mount path to the installer with an ending /. For example, `/mnt/`.

NOTE: Installer will install only RPMs required for Access Manager components. You need to install iManager RPMs separately.

Install RPMs for SNMP after installing RPMs for the Administration Console. See "RHEL Packages and Their Dependent RPMs for SNMP" on page 72.

You must install RPMs in the same sequence as these appear in the table.

RHEL Packages and Their Dependent RPMs for SNMP

The RHEL base installation does not install the net-snmp package by default. Install the following packages manually to make the net-snmp service (Master Agent) functional:

- net-snmp-libs-5.7.2-18.el7.x86_64.rpm
- net-snmp-5.5-44.el6.x86_64

Use the following procedure to install these packages to avoid any dependency issue:

1 Mount the RHEL CD-ROM by running the following command:

```
mount /dev/cdrom /mnt
```

2 Run the following commands:

```
yum install --nogpgcheck net-snmp-libs-5.7.2-18.el7.x86_64.rpm
```

```
yum install --nogpgcheck net-snmp-5.5-44.el6.x86_64
```

3 After installation, run `/etc/init.d/novell-snmpd start`. This will succeed for a successful installation.

6 Uninstalling Components

This section discusses the following topics related to installation:

- “Uninstalling the Identity Server” on page 73
- “Reinstalling an Identity Server to a New Hard Drive” on page 74
- “Uninstalling the Access Gateway” on page 75
- “Uninstalling the Administration Console” on page 76

Uninstalling the Identity Server

Uninstalling the NetIQ Identity Server is a two-step process:

1. Removing the Identity Server from the Administration Console. See “Deleting Identity Server References” on page 73.
2. Removing the Identity Server software from the Linux or Windows machine. See “Uninstalling the Linux Identity Server” on page 73 or “Uninstalling the Windows Identity Server” on page 74.

Deleting Identity Server References

As part of the full Identity Server uninstall process, you must delete the Identity Server from the Administration Console. The Identity Server must first be removed from the cluster configuration, then it can be deleted from the Administration Console. You must do this before removing the software from the machine.

1 In the Administration Console, click **Devices** > **Identity Servers**.

2 Select the Identity Server that you want uninstalled, then click **Stop**.

3 Wait for its health to turn red, then select the server and click **Actions** > **Remove from Cluster**.

4 Update the cluster configuration.

5 Select the Identity Server that you are going to uninstall, then click **Actions** > **Delete**.

6 Continue with “Uninstalling the Linux Identity Server” on page 73 or “Uninstalling the Windows Identity Server” on page 74.

Uninstalling the Linux Identity Server

If you have installed the Identity Server with the Administration Console, you can select to uninstall only the Identity Server or to uninstall both.

1 On your Linux Identity Server, insert the Access Manager installation CD.

2 Navigate to the `novell-access-manager` directory.

3 Enter `./uninstall.sh` to initiate the uninstallation script.

4 Select 2 to uninstall the Identity Server.

5 Enter the name and password of the admin user. (When Administration Console and Identity Server are installed on the same server)

Uninstall removes the Identity Server. A log file is created at `/tmp/novell_access_manager_uninstall.log`.

Uninstalling the Windows Identity Server

If you have installed the Identity Server with the Administration Console, you can select to uninstall only the Identity Server or to uninstall both.

1 Exit any applications and disable any virus scanning programs.

2 Access the Control Panel, click **Add or Remove Programs**, then select to remove the AccessManagerServer program.

3 Read the introduction, then click **Next**.

4 Specify the credentials for the admin user, then click **Next**.

5 Select one of the following, then click **Next**.

Complete Uninstall: Select this option if you have installed both the Identity Server and the Administration Console on the same machine and you want to uninstall both.

Uninstall Specific Features: Select this option to uninstall only the Identity Server.

6 (Conditional) If you selected to uninstall specific features, select one of the following, then click **Uninstall**.

- **Administration Console:** Select this option to uninstall the Administration Console. You cannot uninstall the Administration Console without also uninstalling the Identity Server.
- **Identity Server:** Select this option to uninstall only the Identity Server.

If the unistall fails because the primary Administration Console is not available to validate the credentials, see Troubleshooting the Uninstall of the Windows Identity Server in the NetIQ Access Manager 4.2 Administration Guide .

7 (Conditional) If the Administration Console was installed with the Identity Server and you selected only to uninstall the Identity Server, reboot the machine.

Reinstalling an Identity Server to a New Hard Drive

If your Identity Server hard drive fails, you must reinstall the Identity Server (see Chapter 3, “Installing the Identity Servers,” on page 47) and leave the Identity Server configuration intact in the Administration Console. In order to preserve the existing keystores, perform the following steps before installing the Identity Server on the new hard drive.

1 Stop the server.

In the Administration Console, click **Access Manager > Identity Servers**. Select the server and click **Stop**. Allow a few seconds for the server to stop.

2 Select the server, then click **Actions > Remove from configuration**.

3 Select the server, then click **Actions > Delete**.

4 Reinstall the Identity Server. (See Chapter 3, “Installing the Identity Servers,” on page 47.)

5 On the Identity Servers page, select the server, then click **Actions > Assign to Cluster**.

6 Select the Identity Server cluster configuration, then click **Assign**.

7 Click **OK**.

Uninstalling the Access Gateway

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

2 If the Access Gateway belongs to a cluster, you need to remove it from the cluster.

2a Select the Access Gateway, then click **Actions** > **Remove from Cluster**:

2b Confirm the action, then click **OK**.

3 On the Access Gateways Servers page, select the name of the server, then click **Actions** > **Delete** > **OK**.

This removes the configuration object for the Access Gateway from the Administration Console.

4 On the Identity Servers page, update the Identity Server status for the Identity Server cluster configuration that was using this Access Gateway.

See Updating an Identity Server Configuration in the NetIQ Access Manager 4.2 Administration Guide .

5 Complete one of the following:

- If you are uninstalling the Access Gateway Appliance machine, re-image the machine by booting to a CD containing the desired operating system software.
- If you are uninstalling the Windows Access Gateway Service, continue with "Uninstalling the Windows Access Gateway Service" on page 75.
- If you are uninstalling the Linux Access Gateway Service, continue with "Uninstalling the Linux Access Gateway Service" on page 75.

Uninstalling the Windows Access Gateway Service

1 Exit any applications and disable any virus scanning programs.

2 Access the Control Panel, click **Add or Remove Programs** and select to remove the AccessGateway program.

3 Click **Next**.

4 Specify the credentials for the admin user, then click **Uninstall**.

If the uninstall fails because the program cannot authenticate to the Administration Console, see Troubleshooting the Uninstall of the Access Gateway Service in the NetIQ Access Manager 4.2 Administration Guide .

Uninstalling the Linux Access Gateway Service

1 On your Linux Access Gateway Service, insert the Access Manager installation CD.

2 Navigate to the `novell-access-gateway` directory.

3 Enter `./uninstall.sh` to initiate the uninstallation script.

4 Enter the name of the admin user.

5 Enter the password of the admin user.

Uninstall removes the Access Gateway Service. A log file is created at `/tmp/novell_access_manager_uninstall.log`.

If the uninstall fails, see Troubleshooting the Uninstall of the Access Gateway Service in the NetIQ Access Manager 4.2 Administration Guide .

Uninstalling the Administration Console

Only the primary version of the Administration Console contains the certificate authority. If you uninstall this version, you can no longer use Access Manager for certificate management. You need to promote a secondary console to be the primary console. See Installing Secondary Versions of the Administration Console in the NetIQ Access Manager 4.2 Administration Guide .

IMPORTANT: If you are uninstalling all Access Manager devices, the primary Administration Console should be the last device you uninstall. The uninstall programs for the other devices contact the primary Administration Console and validate the admin's credentials before allowing the device to be removed.

Select the process that corresponds to your platform:

- "Uninstalling the Linux Administration Console" on page 76
- "Uninstalling the Windows Administration Console" on page 77

Uninstalling the Linux Administration Console

1 Insert CD 1 into the drive.

2 Log in as the `root` user or equivalent.

3 At the command prompt of the Access Manager directory, enter the following:

```
./uninstall.sh
```

4 Select one of the following options:

Option	Description
1	Novell Access Manager Administration
2	Novell Identity Server
3	Novell Access Gateway
6	Forcefully uninstall all products (not recommended) Use this option after a failed installation; otherwise use options 1 through 4 to uninstall Access Manager components. **WARNING:** Using this option when you have a cluster of Administration Consoles can cause synchronization and update problems with the configuration store. If you use it to remove an Administration Console, you need to run dsrepair to remove the missing replica from the replica ring.
Q	Quit without uninstalling

5. After running the `./uninstall.sh` script, go to **Auditing** > **Troubleshooting** > **Other Known Device Manager Servers**, then remove the entry for this secondary Administration Console from the servers list.

   A log file is created at `/tmp/novell_access_manager_uninstall.log`.

Uninstalling the Windows Administration Console

When you uninstall the Administration Console, any other Access Manager components on the machine must also be uninstalled.

1. Exit any applications and stop any virus scanning programs.
2. Access the Control Panel, click **Add or Remove Programs**, then select to remove the AccessManagerServer program.
3. Read the introduction, then click **Next**.
4. Specify the credentials for the admin user, then click **Next**.
5. Click **Complete Uninstall**, then click **Next**.

II Upgrading Access Manager

This section discusses how to upgrade Access Manager to the newer version. You must take a backup of the existing configurations before upgrading or migrating Access Manager components.

For more information, see “Back Up and Restore” in the *NetIQ Access Manager 4.2 Administration Guide* .

NOTE

- The SSL VPN component is removed from Access Manager 4.1 onwards. If you are upgrading to Access Manager 4.2 from 4.0.x or earlier, ensure that you manually remove the proxy services and protected resources that refer to SSL VPN.
- Access Manager indicates Access Gateway cluster health in yellow if you do not remove the proxy services and protected resources that refer to SSL VPN.
- Platform Agent and Novell Audit are no longer supported. A new Access Manager 4.2 installation no longer installs Platform Agent and Novell Audit for auditing. If you upgrade from an older version of Access Manager to 4.2, Platform Agent is still available. It is recommended to use syslog for auditing.

IMPORTANT: If you attempt to upgrade from 4.1.2 to 4.2, the upgrade process terminates abruptly. To resolve this issue, perform the following steps:

1. Extract the 4.1 installer files and locate `upgrade_utility_functions.sh` file.
2. Locate the section that includes the following line:
   ```
   supportedVersions="|3.2.3\|4.0.0\|4.0.2\|4.1.0.0\|4.1.1.0\|4.1.1.1\|4.2.0.0"
   ```
3. Modify the **supportedVersion** section by adding 4.1.2 as the supported upgrade platform in the following manner:
   ```
   supportedVersions="|3.2.3\|4.0.0\|4.0.2\|4.1.0.0\|4.1.1.0\|4.1.1.1\|4.2.0.0\|4
   .1.2.0"
   ```
4. Upgrade the components using the information in Part II, “Upgrading Access Manager,” on page 79.

This part describes how to upgrade Access Manager components and include the following chapters:

7 Prerequisites

Before performing an upgrade, ensure that the following prerequisites are met:

- Any option that is configured through the `nidpconfig.properties` file will be overwritten after upgrade. Hence, ensure to back up the `nidpconfig.properties` file before upgrading to 4.2. After the upgrade, replace the new `nidpconfig.properties` file with the backed up file.
- Access Manager 4.2 onwards, some of the options are supported only through the Administration Console. After the upgrade, you must configure those options through the Administration Console. For the list of options that must be configured through Administration Console, see Configuring Identity Server Global Options, Configuring ESP Global Options, Defining Options for SAML 2.0 in the NetIQ Access Manager 4.2 Administration Guide .
- The upgrade process overwrites all customized JSP files. If you have customized JSP files for the Identity Server or the Access Gateway, you must perform manual steps to maintain the customized JSP files. For more information, see “Maintaining Customized JSP Files for Identity Server” on page 81 or “Maintaining Customized JSP Files for Access Gateway” on page 83.
- If you have customized any changes to `tomcat.conf` or `server.xml`, you must back up the files. After the upgrade, restore the files.
- If you have installed the unlimited strength java crypto extensions before upgrade, you must re-install it after the upgrade because a new Java version will be used.
- If you are using Kerberos, ensure that you back up the `/opt/novell/nids/lib/webapp/WEB-INF/classes/kerb.properties` file.

Maintaining Customized JSP Files for Identity Server

Access Manager 4.2 contains a new default user portal and a new set of default login pages. The new login pages have a different look and feel compared to the default login pages of Access Manager 4.1 or prior. If you have customized the legacy user portal, you can maintain the customized JSP pages in the following two ways:

- Using Customized JSP Pages from Access Manager 4.1 or Prior
- Using Customized JSP Pages from Access Manager 4.1 or Prior and Enabling the New Access Manager Portal

Using Customized JSP Pages from Access Manager 4.1 or Prior

1. Before upgrade, create a copy of all JSP files inside the `/opt/novell/nidp/lib/webapp/jsp` directory and place the copy somewhere else.

   WARNING: The upgrade overwrites all existing JSP files.

2. Upgrade Identity Server.
3. Create an empty folder `legacy` in Identity Server: `/opt/novell/nids/lib/webapp/WEB-INF/legacy`.

NOTE: If you do not create the `legacy` folder, Access Manager uses the logic of the default new login pages.

4 Copy your all backed up JSP files into the `/opt/novell/nids/lib/webapp/jsp` directory.

5 Refresh the browser to see the changes.

Using Customized JSP Pages from Access Manager 4.1 or Prior and Enabling the New Access Manager Portal

1 Before upgrade, create a copy of all JSP files inside the `/opt/novell/nidp/lib/webapp/jsp` directory and place the copy somewhere else.

WARNING: The upgrade overwrites all existing JSP files.

2 Upgrade Identity Server.

3 Create an empty folder `legacy` in Identity Server: `/opt/novell/nids/lib/webapp/WEB-INF/legacy`.

NOTE: If you do not create the `legacy` folder, Access Manager uses the logic of the default new login pages.

4 Copy your all backed up JSP files into the `/opt/novell/nids/lib/webapp/jsp` directory.

5 Find the customized `nidp.jsp` and `content.jsp` files and make the following changes in both files:

5a In the top Java section of the JSP file, find the `ContentHandler` object that looks similar to the following:

```
ContentHandler handler = new ContentHandler(request,response);
```

5b In the code, add the following Java line under `ContentHandler`:

```
boolean bGotoAlternateLandingPageUrl =
handler.gotoAlternateLandingPageUrl();
```

5c Find the first instance of `<script></script>` in the `JSP` file that is not `<script src></script>`, then insert the following line in to the JavaScript section between the `<script></script>` tags:

```
<% if (bGotoAlternateLandingPageUrl) { %>
        document.location = "<%=handler.getAlternateLandingPageUrl()%>";
<%  } %>
```

This redirects control to the default portal page that contains appmarks.

5d Save the file.

5e Repeat the steps for the second JSP file.

6 Refresh the browser to see the changes.

Maintaining Customized JSP Files for Access Gateway

If you have customized the JSP files for Access Gateway, you must perform the following steps to maintain the customized files:

1. Before upgrade, create a copy of all JSP files inside the `/opt/novell/nesp/lib/webapp/jsp` directory and place the copy somewhere else.

   WARNING: The upgrade overwrites all existing JSP files.

2. Upgrade Access Gateway.
3. Create an empty folder `legacy` in Access Gateway: `/opt/novell/nesp/lib/webapp/WEB-INF/legacy`.

   NOTE: If you do not create the `legacy` folder, Access Manager uses the logic of the default new login pages.

4. Copy your all backed up JSP files into the `/opt/novell/nesp/lib/webapp/jsp` directory.
5. Refresh the browser to see the changes.

8 Upgrading Access Manager

If you are on Access Manager 3.1 SP4 or 3.1 SP5 and want to move to 4.2, you must first migrate the Access Manager components to version 4.0, and then you can upgrade to 4.2. For more information about how to migrate to Access Manager 4.0, see Migrating Access Manager in the NetIQ Access Manager 4.0 Migration and Upgrade Guide.

When you upgrade the Access Manager components, first back up your configuration and then move the Administration Console. You can then upgrade the various devices that you have imported into the Administration Console.

NOTE: We recommend that you upgrade all members of a cluster before moving to another type of device. When the nodes in the cluster are running on different release versions, you must not change any configuration through Administration Console.

You must upgrade the Access Manager components in the following sequence:

1. Primary Administration Console
2. Secondary Administration Console (If you have installed Administration Console on other servers for fault tolerance).
3. Identity Server
4. Access Gateway

This table lists Access Manager upgrade and migration path:

Access Manager Version	Migration/Upgrade Path to Access Manager 4.2
3.1.x	Migrate to 4.0 and then upgrade to 4.2
3.2 SP3 or higher	Direct upgrade
4.0.x or higher	Direct upgrade
4.1.x or higher	Direct upgrade

NOTE: For information about the latest supported upgrade paths, see the specific Release Notes on the Access Manager Documentation website.

- "Upgrading Access Manager on Linux" on page 85
- "Upgrading Access Manager on Windows" on page 94

Upgrading Access Manager on Linux

- "Upgrading the Evaluation Version to the Purchased Version" on page 86
- "Upgrading Access Manager" on page 88

Upgrading the Evaluation Version to the Purchased Version

If you have downloaded the evaluation version and want to keep your configuration after purchasing the product, you need to upgrade each of your components with the purchased version. The upgrade to the purchased version automatically changes your installation to a licensed version.

After you have purchased the product, log in to the NetIQ Customer Center and follow the link that allows you to download the product. Then use the following sections for instructions on upgrading the components:

- "Upgrading Administration Console" on page 86
- "Upgrading Identity Server" on page 87
- "Upgrading Access Gateway Appliance" on page 88
- "Upgrading Access Gateway Service" on page 93

Upgrading Administration Console

If Identity Server is installed on the same machine as Administration Console, Identity Server is automatically upgraded with Administration Console.

1. Open a terminal window.
2. Log in as the `root` user.
3. Download the upgrade file from dl.netiq.com and extract the `tar.gz` file using the following command: `tar -xzvf <filename>`.

   NOTE: For information about the name of the upgrade file, see the specific Release Notes on the Access Manager Documentation website.

   ---
4. Change to the directory where you unpacked the file, then enter the following command in a terminal window:

   ```
   ./upgrade.sh
   ```
5. The system displays the confirmation message along with the list of installed components. For example, if the Administration Console and Identity Server are installed on the same machine, the following message is displayed:

   ```
   The following components were installed on this machine

   1. Access Manager Administration Console
   2. Identity Server
   Do you want to upgrade the above components (y/n)?
   ```
6. Type **Y** and press Enter.

   The system displays an information message to enable Syslog on the Auditing user interface of the Administration Console after the upgrade.
7. Type **Y** to continue with the upgrade, then press Enter.
8. Enter the Access Manager Administration Console user ID.
9. Enter the Access Manager Administration Console password.
10. Re-enter the password for verification.
11. The system displays the following message when the upgrade is complete:

```
Upgrade completed successfully.
```

The upgrade logs are located in the `/tmp/novell_access_manager/` directory. The logs have time stamping.

If you encounter an error, see Troubleshooting Linux Administration Console Upgrade in the NetIQ Access Manager 4.2 Administration Guide .

Upgrading Identity Server

Use the following procedure to upgrade stand-alone Identity Server. If you have installed both Identity Server and Administration Console on the same machine, see "Upgrading Administration Console" on page 89.

NOTE: If you have modified the JSP file to customize the login page, logout page, and error messages, you can restore the JSP file after installation. You should sanitize the restored JSP file to prevent XSS attacks. For more information, see Preventing Cross-site Scripting Attacks in the NetIQ Access Manager 4.2 Administration Guide .

1. Open a terminal window.
2. Log in as the `root` user.
3. Download the upgrade file from dl.netiq.com and extract the `tar.gz` file using the following command: `tar -xzvf <filename>`.

   NOTE: For information about the name of the upgrade file, see the specific Release Notes on the Access Manager Documentation website.

4. Change to the directory where you unpacked the file, then enter the following command in a terminal window:

   ```
   ./upgrade.sh
   ```

5. The system displays the following confirmation message:

   ```
   The following components were installed on this machine

   1. Identity Server

   Do you want to upgrade the above components (y/n)?
   ```

6. Type Y and press Enter.

   The system displays a warning to back up all JSPs before proceeding with the upgrade:

7. Type Y to continue with the upgrade, then press Enter.
8. Enter the Access Manager Administration Console user ID.
9. Enter the Access Manager Administration Console password.
10. Re-enter the password for verification.
11. The system displays the following message when the upgrade is complete:

    ```
    Upgrade completed successfully.
    ```

    The upgrade logs are located in the `/tmp/novell_access_manager/` directory. The logs have time stamping.

Upgrading Access Gateway Appliance

1. Open a terminal window.
2. Log in as the `root` user.
3. Download the upgrade file from dl.netiq.com and extract the `tar.gz` file using the following command: `tar -xzvf <filename>`.

   NOTE: For information about the name of the upgrade file, see the specific Release Notes on the Access Manager Documentation website.

4. Change to the directory where you unpacked the file, then enter the following command in a terminal window:

   ```
   ./ma_upgrade.sh
   ```

5. Enter the Access Manager Administration Console user ID.
6. Enter the Access Manager Administration Console password
7. Re-enter the password for verification

   The upgrade logs are located in the `/tmp/novell_access_manager/` directory. The logs have time stamping.

Upgrading Access Manager

You must be on Access Manager 3.2 SP3 or a higher version to upgrade to 4.2. For upgrading, you need to upgrade the components in the following order:

- "Upgrading Administration Console" on page 89
- "Upgrading Identity Server" on page 90
- "Upgrading Access Gateway Appliance" on page 92
- "Upgrading Access Gateway Service" on page 93

While you are upgrading the components, take care of the following points:

- Ensure that you are on Access Manager 3.2 SP3 or a higher version.
- You must backup the files that you have customized.
- Ensure that you follow the procedure given below for both Linux and Red Hat:

1. Open the `nds.conf` file available under `/etc/opt/novell/eDirectory/conf/`.
2. Delete all the duplicate lines from the file. For example the file may contain two lines of n4u.server.vardir=/var/opt/novell/eDirectory/data. Delete one of them.
3. Restart eDirectory using `/etc/init.d/ndsd restart` command.

NOTE: If you have enabled history for risk-based authentication in Access Manager 4.1, you must upgrade the database for risk-based authentication after upgrading to 4.2. You can find the upgrade script here: `/opt/novell/nids/lib/webapp/WEB-INF/RiskDBScript.zip`.

MySQL: Run `netiq_risk_mysql_upgrade.sql`

Oracle: Run `netiq_risk_oracle_upgrade.sql`

Upgrading Administration Console

NOTE: Access Manager by default supports Tomcat 8.0.24 and OpenSSL 1.0.1p. Due to this, Identity Server and Access Gateway disable requests from clients that are on versions lower than TLS1. However, Access Gateway can continue communication with web servers that are on versions lower than TLS1.

If Identity Server is installed on the same machine as Administration Console, Identity Server is automatically upgraded with Administration Console. If you are upgrading this configuration and you have custom JSP pages, you can backup these files or allow the upgrade program to back them up for you.

1. Back up any customized JSP pages and related files.

   Even though the upgrade program backs up the JSP directory and its related files in the `/root/nambkup` folder, it is a good practice to backup these files.

   ```
   /var/opt/novell/tomcat/webapps/nidp/jsp
   ```

2. Open a terminal window.
3. Log in as the `root` user.
4. Download the upgrade file from dl.netiq.com and extract the `tar.gz` file using the following command: `tar -xzvf <filename>`.

   NOTE: For information about the name of the upgrade file, see the specific Release Notes on the Access Manager Documentation website.

5. Change to the directory where you unpacked the file, then enter the following command in a terminal window:

   ```
   ./upgrade.sh
   ```

6. The system displays the confirmation message along with the list of installed components. For example, if the Administration Console and Identity Server are installed on the same machine, the following message is displayed:

   ```
   The following components were installed on this machine

   1. Access Manager Administration Console
   2. Identity Server
   Do you want to upgrade the above components (y/n)?
   ```

7. Type Y and press Enter.

   The system displays an information message to enable Syslog on the Auditing user interface of Administration Console after the upgrade.

8. Type Y to continue with the upgrade, then press Enter.
9. Enter the Access Manager Administration Console user ID.
10. Enter the Access Manager Administration Console password.
11. Re-enter the password for verification.
12. The system displays the following message when the upgrade is complete:

    ```
    Upgrade completed successfully.
    ```

13. (Optional) To view the upgrade files:
    - To view the upgrade log files, see the files in the `/tmp/novell_access_manager` directory.

- If you selected to back up your configuration and used the default directory, see the zip file in the `/root/nambkup` directory. The log file for this backup is located in the `/var/log` directory.
- If the Identity Server is installed on the same machine, the JSP directory was backed up to the `/root/nambkup` directory. The file is prefixed with `nidp_jps` and contains the date and time of the backup.

NOTE: If you have customized the Java settings in the `/opt/novell/nam/idp/conf/tomcat.conf` file, then after the upgrade, you must copy the customized setting to the new file. For more information about copying the customized setting, refer Step 13 on page 91 of "Upgrading Identity Server" on page 90.

If you encounter an error, see Troubleshooting Linux Administration Console Upgrade in the NetIQ Access Manager 4.2 Administration Guide .

Upgrading Identity Server

Use the following procedure to upgrade stand-alone Identity Server. If you have installed both Identity Server and Administration Console on the same machine, see "Upgrading Administration Console" on page 89.

IMPORTANT: Ensure to complete the following actions before you begin:

- If you are upgrading Access Manager components on multiple machines, ensure that the time and date are synchronized on all machines.
- Make sure that Administration Console is running. However, you must not perform any configuration tasks in Administration Console during an Identity Server upgrade.

1 Back up any customized JSP pages and related files.

Even though the upgrade program backs up the JSP directory and its related files in the `/root/nambkup` folder, it is a good practice to backup these files.

2 Open a terminal window.

3 Log in as the `root` user.

4 Download the upgrade file from dl.netiq.com and extract the `tar.gz` file using the following command: `tar -xzvf <filename>`.

NOTE: For information about the name of the upgrade file, see the specific Release Notes on the Access Manager Documentation website.

5 Change to the directory where you unpacked the file, then enter the following command in a terminal window:

```
./upgrade.sh
```

6 The system displays the following confirmation message:

```
The following components were installed on this machine

1. Identity Server

Do you want to upgrade the above components (y/n)?
```

7 Type **Y** and press Enter. A Warning message regarding backup and restore is displayed.

8 Type Y to continue with the upgrade, then press Enter.

9 Enter the Access Manager Administration Console user ID.

10 Enter the Access Manager Administration Console password.

11 Re-enter the password for verification.

12 The system displays the following message when the upgrade is complete:

```
Upgrade completed successfully.
```

13 Restore any customized files from the backup taken earlier. To restore files, copy files to the respective locations:

- `/opt/novell/nam/idp/webapps/nidp/jsp`
- `/opt/novell/nam/idp/webapps/nidp/html`
- `/opt/novell/nam/idp/webapps/nidp/images`
- `/opt/novell/nam/idp/webapps/nidp/config`
- `/opt/novell/nam/idp/webapps/nidp/WEB-INF/lib`
- `/opt/novell/nam/idp/webapps/nidp/WEB-INF/web.xml`
- `/opt/novell/nam/idp/webapps/nidp/WEB-INF/classes`
- `/opt/novell/nam/idp/webapps/nidp/WEB-INF/conf`
- `/opt/novell/java/jre/lib/security/bcslogin.conf`
- `/opt/novell/java/jre/lib/security/nidpkey.keytab`
- `/opt/novell/nids/lib/webapp/classUtils`
- `/opt/novell/nam/idp/conf/server.xml`

  Also, add the following line to the `server.xml` file to use the new features on the user portal. For information about new features of user portal, refer Access Manager 4.2 Release Notes.

  ```
  <Connector NIDP_Name="localConnector" URIEncoding="utf-8"
  acceptCount="100" address="127.0.0.1" connectionTimeout="20000"
  maxThreads="600" minSpareThreads="5" port="8088" protocol="HTTP/1.1" />
  ```

  An example below shows that the IP address is removed and ciphers added.`<Connector NIDP_Name="connector" port="8443" address="" ciphers="SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA, ...   ../>`

- `/opt/novell/nam/idp/conf/tomcat.conf`

NOTE: If you are using Kerberos and you have renamed `nidpkey.keytab` and `bcsLogin.conf` with any other name, ensure that you modify the `upgrade_utility_functions.sh` script located in the `novell-access-manager-x.x.x.x-xxx/scripts` folder with these names before upgrading Access Manager.

NOTE: If you have customized the Java settings in the `/opt/novell/nam/idp/conf/tomcat.conf` file, then after the upgrade, you must copy the customized setting to the new file.

NOTE: If you have modified the JSP file to customize the login page, logout page, and error messages, you can restore the JSP file after installation. You should sanitize the restored JSP file to prevent XSS attacks. For more information, see Preventing Cross-site Scripting Attacks in the NetIQ Access Manager 4.2 Administration Guide .

Upgrading Access Gateway Appliance

Prerequisite: If you are on 3.2.3 or higher, before upgrading to 4.2, you must first upgrade the base operating system of Access Gateway Appliance to the latest operating system that is included in the 4.2 Access Gateway appliance ISO. For more information about how to upgrade, see Section 9, “Upgrading the Operating System for Access Gateway Appliance,” on page 101.

1 Back up any customized JSP pages and related files.

Even though the upgrade program backs up the JSP directory and its related files in the /root/nambkup folder, it is a good practice to backup these files.

2 Open a terminal window.

3 Log in as the root user.

4 Download the upgrade file from dl.netiq.com and extract the tar.gz file using the following command: tar -xzvf <filename>.

NOTE: For information about the name of the upgrade file, see the specific Release Notes on the Access Manager Documentation website.

5 Change to the directory where you unpacked the file, then enter the following command in a terminal window:

```
./ma_upgrade.sh
```

6 A Warning message regarding backup and restore is displayed. If you have customized any files, take a backup and restore them after installation.

7 Would you like to continue this upgrade? Type Y to continue.

8 Do you want to restore custom login pages? Type Y to confirm.

9 Enter the Access Manager Administration Console user ID.

10 Enter the Access Manager Administration Console password

11 Re-enter the password for verification

12 The system displays the following message when the upgrade is complete:

```
Upgrade completed successfully.
```

13 Restore any customized files from the backup taken earlier. To restore the files, copy the files to the respective locations below:

- /opt/novell/nam/mag/webapps/nesp/WEB-INF/web.xml
- /opt/novell/nam/mag/webapps/nesp/jsp
- /opt/novell/nam/mag/webapps/nesp/html
- /opt/novell/nam/mag/webapps/nesp/images
- /opt/novell/nam/mag/webapps/agm/WEB-INF/config/current
- /opt/novell/nam/mag/webapps/nesp/config

- `/opt/novell/devman/jcc/scripts/presysconfig.sh`
- `/opt/novell/devman/jcc/scripts/postsysconfig.sh`

Upgrading Access Gateway Service

- "Prerequisites for Access Gateway Service" on page 93
- "Process" on page 93

Prerequisites for Access Gateway Service

- Manually back up the `/opt/novell/nam/mag/conf/tomcat.conf` and the `/opt/novell/nam/mag/conf/server.xml` files.

  The `ag_upgrade.sh` script takes care of backing up the remaining customized files automatically. These files get automatically backed up at the `/root/nambkup` folder and includes apache configuration and error pages.

Process

1. Download the `AM_42_AccessGatewayService_Linux_64.tar.gz` file from the NetIQ download site and extract it by using the following command:

   `tar -xzvf <AM_42_AccessGatewayService_Linux_64.tar.gz>`
2. Run the `ag_upgrade.sh` script from the folder to start the upgrade.
3. Specify the following information:

   User ID: Specify the name of the administration user for the Administration Console.

   Password and Re-enter Password: Specify and re-enter the password for the administration user account.

   The Access Gateway Service is upgraded. The following message is displayed when upgrade is complete:

   ```
   Starting Access Manager services...
   Backup of customized files are available at /root/nambkup. Restore them if
   required.
   ```
4. View the log files. The install logs are located in the `/tmp/novell_access_manager/` directory.
5. Restore any customized files from the backup taken earlier as part of steps in "Prerequisites for Access Gateway Service" on page 93.

   To restore the files, copy the content of the following files to the corresponding file in the new location.

Old File Locations	New File Location
`/root/novell_access_manager/apache2/` (contains apache var files)	`/opt/novell/apache2/share/apache2/error`
`/root/novell_access_manager/nesp/` (contains modified error pages)	`/var/opt/novell/tomcat/webapps/nesp/jsp/`

server.xml:

If you have modified any elements or attributes in the 3.2.x, 4.0.x or 4.1.x environment the corresponding changes will need to be applied to the 4.2 `server.xml` file.

Typical changes done to the `server.xml` include modifying the '`Address=`' to restrict the IP address the application will listen on, or '`maxThreads=`' attributes to modify the number of threads.

In the following example, 3.2..x has customized `maxThreads` value.

```
<<Connector port="9009" enableLookups="false" redirectPort="8443"
protocol="AJP/1.3" address="127.0.0.1" minSpareThreads="25" maxThreads="700"
backlog="0" connectionTimeout="20000, ...   ../>
```

Make a note of the customizations and copy paste the changed values in the 4.2 `server.xml` file

tomcat.conf:

Copy any elements or attributes that you have customized in the `tomcat7.conf` file to the `tomcat.conf` file.

For example, if you have included the environment variable to increase the heap size by using `-Xmx/Xms/Xss` attributes in the `tomcat7.conf` file, copy this variable to the 4.2 `/opt/novell/nam/idp/conf/tomcat.conf` file.

6. Modify the required properties in `/opt/novell/nam/mag/webapps/agm/WEB-INF/agm.properties` using back up file `/root/novell_access_manager/agm/agm.properties`. If you have customized the `agm.properties` file from the backup taken in 3.2.x, 4.0.x or 4.1.x, ensure that you apply the same to the new 4.2 `/opt/novell/nam/mag/webapps/agm/WEB-INF/agm.properties` file. An example below shows the how to enable the backend webserver's webpage caching and the cache location.

   ```
   apache.disk.cache.enabled=yes
   ```

   ```
   apache.disk.cache.root=/var/cache/novell-apache2
   ```

7. Change the ownerships of the following files (with read access to tomcat user) using the following commands:

   ```
   chown -R novlwww:novlwww /var/opt/novell/tomcat/webapps/nesp/jsp/
   ```

   ```
   chown -R novlwww:novlwww /opt/novell/nam/mag/webapps/agm/WEB-INF/
   agm.properties
   ```

8. On the newly added Access Gateway Service, restart Tomcat using the `/etc/init.d/novell-mag restart` or `rcnovell-mag restart` command.

NOTE: If you have customized the Java settings in the /opt/novell/nam/idp/conf/tomcat.conf file, then after the upgrade, you must copy the customized setting to the new file.

Upgrading Access Manager on Windows

- “Prerequisites” on page 95
- “Upgrading the Evaluation Version to the Purchased Version” on page 95
- “Upgrading Access Manager” on page 95

Prerequisites

In addition to the following prerequisites, ensure that you also meet the hardware requirements. For more information about hardware requirements, see the component-specific requirements in the Part I, “Installing Access Manager,” on page 11.

❒ Before upgrading, back up your configuration using the `ambkup.bat` file. For instructions, see Backing Up the Access Manager Configuration in the NetIQ Access Manager 4.2 Administration Guide .

  If the upgrade fails, you need a way to recover your configuration. As a backup can be restored to only the version on which it was created, you must restore your Access Manager components to that version. You can then restore the configuration with the backup file and work with NetIQ Technical Support to solve the upgrade problem before attempting to upgrade again.

Upgrading the Evaluation Version to the Purchased Version

If you have downloaded the evaluation version and want to keep your configuration after purchasing the product, you need to upgrade each of your components with the purchased version. The upgrade to the purchased version automatically changes your installation to a licensed version.

After you have purchased the product, log in to the Novell Customer Center (http://www.novell.com/center) and follow the link that allows you to download the product. Then follow the instructions in “Upgrading Access Manager” on page 95 for upgrading components.

Upgrading Access Manager

Log in to the NetIQ Downloads page and follow the link that allows you to download the product.

- “Upgrading Administration Console” on page 95
- “Upgrading Identity Server” on page 97
- “Upgrading Access Gateway Service” on page 98

NOTE: If you have enabled history for risk-based authentication in Access Manager 4.1, you must upgrade the database for risk-based authentication after upgrading to 4.2. You can find the upgrade script here: `C:\Program Files\(x86)\Novell\Tomcat\webapps\nidp\WEB-INF\RiskDBScript.zip`.

MySQL: Run `netiq_risk_mysql_upgrade.sql`

Oracle: Run `netiq_risk_oracle_upgrade.sql`

Upgrading Administration Console

If you have installed Administration Console and Identity Server on the same server, you must upgrade both of them at the same time.

1. Manually back up your current Access Manager configuration using `ambkup.bat` file. For instructions, see Back Up and Restore in the NetIQ Access Manager 4.2 Administration Guide .
2. If the Identity Server is installed on the same server, manually back up the JSP pages and related files in the `C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp` directory.
3. If you have customized the `tomcat.conf` file or the `server.xml` file, back up these files before upgrading. These files are overwritten during the upgrade process.

IMPORTANT: We recommend that you have your own backup of customized files.

4 Run the installation program. When the installation program detects an installed version of the Administration Console, it automatically prompts you to upgrade.

5 Read the Introduction, then click **Next**.

6 Accept the License Agreement, then click **Next.**

7 Select the component to upgrade that is currently installed, then click **Next**.

8 Type **Y** and press Enter.

The system displays an information message to enable Syslog on the Auditing user interface of the Administration Console after the upgrade.

9 Type **Y** to continue with the upgrade, then press Enter.

10 At the upgrade prompt, click **Continue.**

11 Specify the following information for the administrator account on the Administration Console:

Administration user ID: Specify the name of the administration user for the Administration Console.

Password and Re-enter Password: Specify and re-enter the password for the administration user account.

12 Decide whether you want the upgrade program to create a backup of your current configuration:

- If you have a recent backup, click **Continue**. If you choose to not create a backup when you do not have a recent backup and you then encounter a problem during the upgrade, you may be forced to re-create your configuration.
- If you do not have a recent backup, click **Run Config Backup**. The program creates a backup and stores it in the root of the operating system drive in the `nambkup` directory.

13 Review the summary, then click **Install.**

14 If the upgrade seems to hang and you have been performing other tasks on the desktop, click the installation screen and check for a warning message. Some subcomponents of Access Manager do not send warning messages to the Installation screen when the focus of the mouse is not on the installation window.

15 When you are prompted, reboot the server.

16 View the upgrade log file found in the following location:

```
C:\Program Files(x86)\Novell\log\AccessManagerServer_InstallLog.log
```

17 If the Identity Server installed on the same server, copy any custom login pages to the `C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp` directory. For more information, refer "Upgrading Identity Server" on page 97.

18 Restore any customized files from the backup taken earlier.

To restore the files, copy the content of the following files to the corresponding file in the new location.

server.xml

If you have customized the `server.xml` file from the backup taken in 3.2 SP3, 4.0.x or 4.1.x, ensure that you apply the same to the new 4.2 `server.xml` located at `C:\Program Files (x86)\Novell\Tomcat\conf\` directory.

An example below shows that the IP address is removed and ciphers added.`<Connector NIDP_Name="connector" port="8443" address="" ciphers="SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA, ...   ../>`

Tomcat properties:

Go to `C:\Program Files\Novell\Tomcat\bin\tomcat7w`. Double-click the `tomcat7w` file and make a note of any elements or attributes customized in 3.2 SP3, 4.0.x or 4.1.x

On the 4.2 server, go to `C:\Program Files\Tomcat\bin\tomcat8w`. Change the values and attributes as required.

Upgrading Identity Server

If you have installed only Identity Server on the server, use the following procedure to upgrade Identity Server.

1 Manually back up the JSP pages and related files in the `C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp` directory.

IMPORTANT: We recommend that you have your own backup of the customized files.

2 If you have customized the `tomcat.conf` file or the `server.xml` file at `C:\Program Files (x86)\Novell\Tomcat\conf\`, back up these files before upgrading. The registries and the file are overwritten during the upgrade process.

3 Download and run `AM_42_AccessManagerService_Win64.exe` file from NetIQ.

This file starts the installation program. When the program detects an installed version of the Identity Server, it automatically prompts you to upgrade.

4 On the Introduction page, click **Next.**

5 Accept the License Agreement.

6 At the upgrade prompt, click **Continue**.

7 Type **Y** and press Enter.

The system displays an information message to enable Syslog after the upgrade.

8 Type **Y** to continue with the upgrade, then press Enter.

9 Specify the following information for the Administration Console:

Administration user ID: Specify the name of the administration user for the Administration Console.

Password and Re-enter Password: Specify and re-enter the password for the administration user account.

10 If you have customized login pages, decide whether you want your customized pages restored automatically. Be aware that any new feature introduced in the JSP files that have the same name as your files are lost when your file overwrites the installed file with the automatic restore.

You may want to wait until after the upgrade, then compare your customized file with the newly installed file. You can then decide whether you need to modify your file before restoring it.

NOTE: Ensure that you sanitize the restored customized JSP file to prevent XSS attacks. For more information about how to sanitize the JSP file, see Preventing Cross-site Scripting Attacks in the NetIQ Access Manager 4.2 Administration Guide .

11 Review the summary, then click **Install**.

12 View the upgrade log file found in the following location:

```
C:\Program Files (x86)\Novell\log\AccessManagerServer_ InstallLog.log
```

13 Copy any custom login pages to the `C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp` directory.

14 Restore any customized files from the backup taken earlier.

To restore the files, copy the content of the following files to the corresponding file in the new location.

server.xml

If you have customized the `server.xml` file from the backup taken in 3.2 SP3, 4.0.x, or 4.1.x, ensure that you apply the same to the new `server.xml` located at `C:\Program Files (x86)\Novell\Tomcat\conf\` directory.

Also, add the following line to the `server.xml` file to use the new features on the user portal. For more information about the new user portal, refer Access Manager 4.2 Release Notes.

```
<Connector NIDP_Name="localConnector" URIEncoding="utf-8" acceptCount="100"
address="127.0.0.1" connectionTimeout="20000" maxThreads="600"
minSpareThreads="5" port="8088" protocol="HTTP/1.1" />
```

An example below shows that the IP address is removed and ciphers added.`<Connector NIDP_Name="connector" port="8443" address="" ciphers="SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA, ...   ../>`

Tomcat properties:

Go to `C:\Program Files\Novell\Tomcat\bin\tomcat7w`. Double-click the `tomcat7w` file and make a note of any elements or attributes customized in 3.2 SP3, 4.0.x, or 4.1.x.

On the 4.2 server, go to `C:\Program Files\Tomcat\bin\tomcat8w`. Change the values and attributes as required.

15 Restart tomcat server using the Windows service. Go to **Start** > **Control Panel** > **System and Security** > **Administrative Tools** > **Services**.

IMPORTANT: If NetIQ Access Manager is federated with other service providers or if the users are redirected to Access Gateway protected resources from the Identity Server using the target_url, you may see errors regardless of successful authentication. The ConfigUpgrade script enables ‘Allow any target’ for the ‘Intersite Transfer Service’ configuration service for all the service providers.

Upgrading Access Gateway Service

You can upgrade by using the same installer you used to install the product. The program detects that Access Gateway Service is already installed and prompts you to upgrade.

1 Download and run `AM_42_AccessGatewayService_Win64.exe` file from NetIQ.

2 Run the installation program. When the installation program detects an installed version of the Access Gateway, it automatically prompts you to upgrade.

3 Answer `Yes` to the prompt to upgrade.

4 Read the Introduction, then click **Next.**

5 Review the Readme information, then click **Next**.

6 Accept the License Agreement, then click **Next.**

7 Specify the following information:

User ID: Specify the name of the administration user for the Administration Console.

Password and Re-enter Password: Specify the password and re-enter the password for the administration user account.

8 Review the installation summary, then click Install.

Access Gateway Service is upgraded.

9 View the log files. The install logs are located in the `C:\Program Files\Novell\log` and `C:\agsinstall.log` directories.

10 Restore any customized files from the backup taken earlier.

To restore the files, copy the content of the following files to the corresponding file in the new location.

server.xml:

If you have customized the `server.xml` file from the backup taken in 3.2 SP3, 4.0.x, or 4.1.x, ensure that you apply the same to the new `server.xml` located at `C:\Program Files\Novell\Tomcat\conf\` directory.

An example below shows that the IP address is removed and ciphers added.`<Connector NIDP_Name="connector" port="8443" address="" ciphers="SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA, ...   ../>`

Tomcat properties:

Go to `C:\Program Files\Novell\Tomcat\bin\tomcat7w`. Double-click the `tomcat7w` file and make a note of any elements or attributes customized in 3.2 SP3, 4.0.x, or 4.1.x.

On the 4.2 server, go to `C:\Program Files\Novell\Tomcat\bin\tomcat8w`. Change the values and attributes as required.

11 Restart the tomcat server by using the Windows service. Go to **Start** > **Control Panel** > **System and Security** > **Administrative Tools** > **Services**.

9 Upgrading the Operating System for Access Gateway Appliance

Access Gateway Appliance bundles the latest SUSE kernel. During fresh installation of Access Gateway Appliance, the latest kernel is installed automatically. You must upgrade the base operating system before upgrading Access Gateway Appliance.

NOTE: After upgrading, you also need to re-register the new channel. For more information, see "Setting Up the 4.2 Channel" on page 102.

Perform the following steps to upgrade the base operating system:

1 Get the Access Gateway 4.2 Appliance ISO and mount it in the Access Manager server where you want to upgrade. For example, if you want to mount on `/root/iso`, use the following command:

```
mount -o loop /dev/dvd /root/iso/
```

NOTE: Create `/root/iso` by using the `mkdir -p /root/iso` command before executing the above command.

2 Use the following command to add the mounted ISO as the upgrade repository:

```
zypper ar /root/iso/ 42agapp
```

3 Refresh the new repository by using the following command:

```
zypper ref
```

4 Use the following command to upgrade the base operating system from the repository you added:

```
zypper dup --from 42agapp
```

5 You will be prompted a dependency resolution for `open-iscsi` and `crash-sial-6.0.7-0.10.1.x86_64`. Select **1** from the solutions.

6 Accept the license. The operating system will start upgrading.

7 After upgrade, view the notification.

8 Restart Access Gateway Appliance.

Setting Up the 4.2 Channel

If you had an existing channel for an older version of Access Manager and SLES operating system, then after upgrading to the latest operating system and Access Manager 4.2, you must re-register the new channel.

Perform the following steps to set up the SLES 11 SP4 channel.

1. Upgrade the base Operating System to SLES 11 SP4. For more information about upgrading the base operating system, see Chapter 9, “Upgrading the Operating System for Access Gateway Appliance,” on page 101.
2. Upgrade the Access Gateway Appliance.
3. If the version mentioned in the `/etc/products.d/NAM_APP.prod` file is other than 4.2, edit the file and change the version to 4.2. The line will look like the following:

   ```
   <version>4.2</version>
   ```
4. Remove all the old NCC credentials using the following commands:

   ```
   rm /etc/zypp/credentials.d/NCCcredentials
   ```

   ```
   rm /etc/zypp/repos.d/nu*
   ```

   ```
   rm /etc/zypp/services.d/nu*
   ```
5. Use the `zypper lr` command to verify that the old channel is removed.
6. Re-register to get the latest updates. For more information, see “Installing or Updating Security Patches for the Access Gateway Appliance” on page 103.
7. Use the `zypper lr` command to verify if the new channel `NAM42-APP-Updates` is added.

10 Getting the Latest Security Patches

The OpenSSL open source project team regularly releases updates to known OpenSSL vulnerabilities. Access Gateway uses the OpenSSL library for cryptographic functions. It is recommended that Access Gateway updated with the latest OpenSSL patch.

Prerequisites

- ❐ Before upgrading the kernel, ensure that you have updated the operating system to a supported version.
- ❐ The Access Gateway Appliance installs a customized version of SLES 11 SP4. If you want to install the latest patches as they become available, you must have a Novell user account to receive the Linux updates.
- ❐ Ensure that you have obtained the activation code for Access Manager from Novell Customer Center.

WARNING: Installing additional packages other than security updates breaks your support agreement with Novell. If you encounter a problem, Novell Support can require you to remove the additional packages and to reproduce the problem before receiving any help with your problem.

- "Installing or Updating Security Patches for the Access Gateway Appliance" on page 103
- "Updating Security Patches for Access Gateway Service" on page 106

Installing or Updating Security Patches for the Access Gateway Appliance

To get the latest security updates for Access Gateway Appliance, you can follow any of these options:

- "Registering to Novell Customer Center" on page 103
- "Configuring Subscription Management Tool for The Access Gateway Appliance" on page 104

Registering to Novell Customer Center

To get the latest security updates for Access Gateway Appliance, the user must register with the Novell Customer Center by using the activation code obtained with the product:

If you face issues while using the activation code to register, see Resetting your ZEN Updater and Novell Customer Center Key Registration.

1 Go to **YaST > Support > Novell Customer Center Configuration**.

2 Select **Configure Now (Recommended)**. In addition to the options that are selected by default, select **Registration Code**.

3 Click **Next**.

The Manual Interaction Required screen appears. It might take a few minutes to connect to the server.

This screen indicates that to activate the product, you must provide a valid e-mail ID associated with the Novell account and the activation code.

4. Click **Continue**.
5. To specify the e-mail address, activation code and system name in the relevant fields:

   5a Select the relevant option, then press **Enter**. A text field appears in the bottom left corner of the screen.

   5b Specify value for the selected option in this text field, then press **Enter** to return to the screen.

   5c Repeat these steps for each field.
6. Click **Submit** after you have specified all the relevant information to complete the registration.
7. Enter `Q` to close the window.
8. Enter `Y` at the prompt.

   The Manual Interaction Required screen is displayed. It indicates that the software repositories are created. You will receive a message from the Novell Customer Center Configuration indicating that the configuration was successful.
9. Click **OK** to return to YaST Control Center.
10. Click **Quit** to exit YaST.
11. Open a shell prompt and specify the following command to verify if the repository named `NAM4x-APP-Updates` was created:

    ```
    zypper lr
    ```

    An output similar to the following appears

    ```
    # | Alias                                 | Name
    | Enabled | Refresh
    --+--------------------------------------+-----------------------------------
    1 | NetIQAccessGatewayAppliance-4.x.x-x | NetIQAccessGatewayAppliance-4.x.x-x
    | Yes     | No
    2 | nu_novell_com:NAM4x-APP-Updates       | NAM4x-APP-Updates
    | Yes     | Yes
    ```
12. Run the `zypper up` command to install the patches
13. After the patches are installed, restart the machine.
14. Confirm that all the patches are installed by running `zypper up` command again.

Configuring Subscription Management Tool for The Access Gateway Appliance

Access Gateway Appliance can be configured to register against local Subscription Management Tool (SMT) server and download software updates from there instead of communicating directly with the Novell Customer Center and the NU servers.

To use an SMT server for client registration and as a local update source, you must configure the SMT server in your network first. The SMT server software is distributed as an add-on for SUSE Linux Enterprise Server. For information about configuring the SMT server, see Subscription Management Tool (SMT) for SUSE Linux Enterprise 11.

The following sections describe the configuration required for Access Gateway Appliance:

- "SMT Configuration" on page 105
- "Configuring Access Gateway Appliance" on page 105

SMT Configuration

You must configure the SMT server and set up subscription for `NAM4x-APP-Updates` channel to receive the updates for Access Gateway Appliance.

1. Install the SMT server in a SLES 11 SP4 Server. For more information, see Subscription Management Tool (SMT) for SUSE Linux Enterprise 11.
2. Log in to you Novell Customer Center account.
3. Select **My Products > Mirroring Credentials**, then click **Generate Credentials**.
4. Copy the mirroring credentials before logging out of your Novell Customer Center account.
5. Run the *SMT Configuration* tool from YAST, then specify the mirroring credentials.
6. Run the **SMT Management** tool.

   The `NAM4x-APP-Updates, sle-11-x86_64` repository is displayed in the **Repositories** tab.
7. Select `sle-11-x86_64`, then click **Toggle Mirroring** to ensure mirroring is selected for this repository.
8. Click **Mirror Now**. This step ensures that the *NAM4x-APP-Updates* channel updates are mirrored from **nu.novell.com** to your local SMT server.
9. When mirroring is complete, click **OK** to close the tool.

Configuring Access Gateway Appliance

1. Copy `/usr/share/doc/packages/smt/clientSetup4SMT.sh` from the SMT server to the client machine.

   You can use this script to configure a client machine to use the SMT server or to reconfigure it to use a different SMT server.
2. Specify the following command as `root` to execute the script on the client machine:

   ```
   ./clientSetup4SMT.sh --host server_hostname
   ```

   For example,

   ```
   ./clientSetup4SMT.sh --host smt.example.com.
   ```

   You can get the SMT server URL by running the SMT Configuration tool at the server. The URL is set by default.
3. Enter y to accept the CA certificate of the server.
4. Enter y to start the registration.
5. The script performs all necessary modifications on the client.
6. Execute the following command to perform registration:

   ```
   suse_register
   ```
7. Specify the following command to get online updates from the local SMT server:

   ```
   zypper up
   ```

8 Reboot the machine if prompted at the end of any patch install.

9 Confirm that all the patches are installed by running `zypper up` command again.

Updating Security Patches for Access Gateway Service

- Updating Linux Access Gateway Service with the Latest OpenSSL Patch
- Updating Windows Access Gateway Service with the Latest OpenSSL Patch

Updating Linux Access Gateway Service with the Latest OpenSSL Patch

1 Download the openssl-update.sh script.

2 Change the file permission to executable:

```
chmod +x openssl-update.sh
```

3 Run the following command:

```
openssl-update.sh username password novell-nacm-apache-extra-4.0.8-1.0.1t'
```

NOTE: This downloads the 1.0.1t version of OpenSSL. Change the version number depending on the version available on the appliance channel.

`username` and `password` are the mirror credentials for the Novell Customer Care Portal the product is registered with.

Updating Windows Access Gateway Service with the Latest OpenSSL Patch

1 Download the patch_update.ps1 file.

2 Open the powershell command line with the admin privilege.

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
```

3 Run `patch_update.ps1` with the following three arguments:

- username
- password
- rpmfilename (the RPM file name should not be suffixed with .rpm)

Here username and password are the mirror credentials for the Novell Customer Care Portal the product is registered with, and the rpmfilename is the version of OpenSSL you are upgrading to. This version includes the OpenSSL version in the string. For example,

```
patch_update.ps1 <myusername> <mypassword> <Openssl_Win_101t>
```

NOTE: This command updates to OpenSSL 1.0.1t.

The local download location for the OpenSSL update is `C:\Program Files\Novell\apache\novell_patch`.