Installation and Upgrade Guide

Access Manager Appliance 4.2

November 2015

Legal Notice

Contents

About this Book and the Library

The *Installation and Upgrade Guide* provides an introduction to NetIQ Access Manager Appliance 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 Appliance 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 Appliance

This part describes how to install Access Manager Appliance:

1 Planning Your Access Manager Environment

This section includes the following topics:

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.

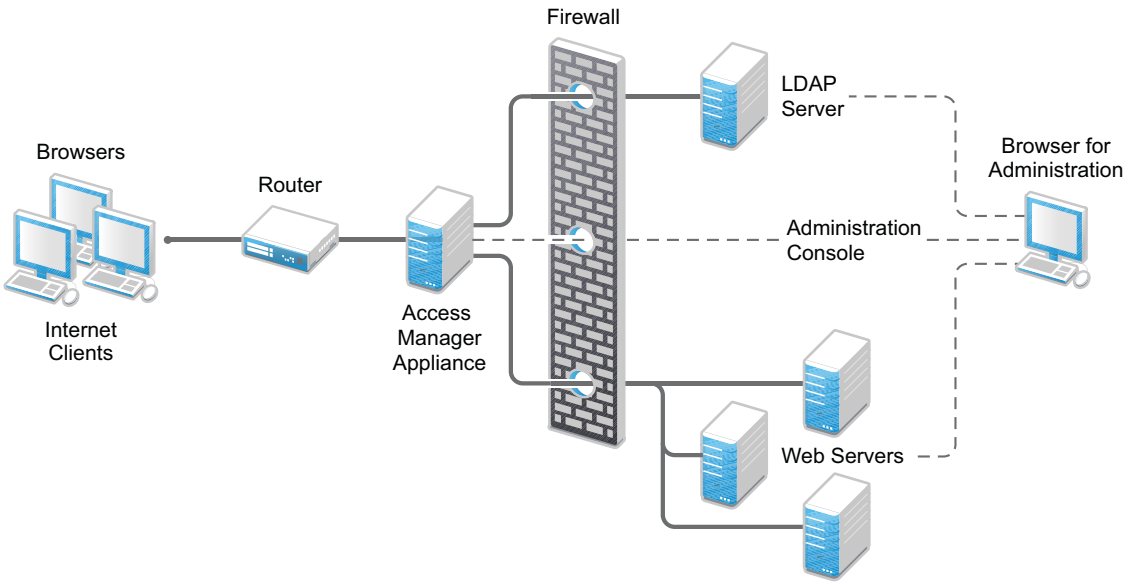
Some of the key differentiators that Access Manager Appliance offers over the Access Manager solution are:

- 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 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.

Feature	Access Manager Appliance	Access Manager
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
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.

Feature	Access Manager Appliance	Access Manager
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.
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.

Feature	Access Manager Appliance	Access Manager
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.
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.

Feature	Access Manager Appliance	Access Manager
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 1-2 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 1-3 on page 20.

Figure 1-2 *Access Manager Appliance Cluster*

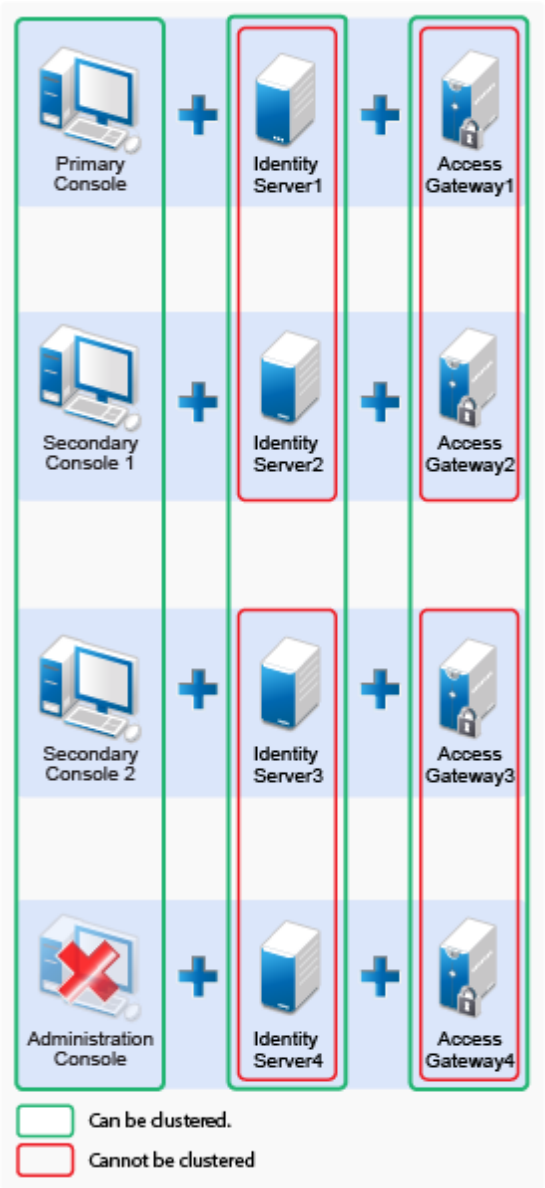
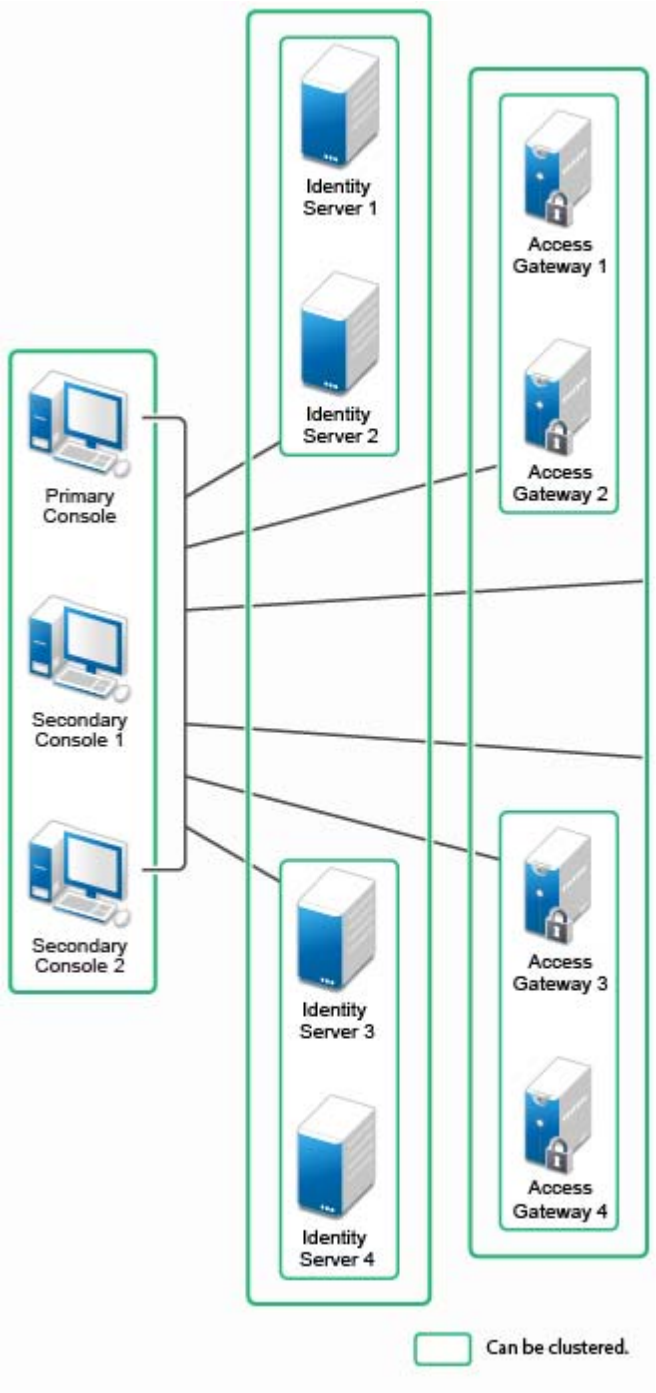


Figure 1-3 *Access Manager Cluster*



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 Appliance in the NetIQ Access Manager Appliance 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.
- Domain name server, which resolves DNS names to IP addresses and which has reverse lookups enabled.

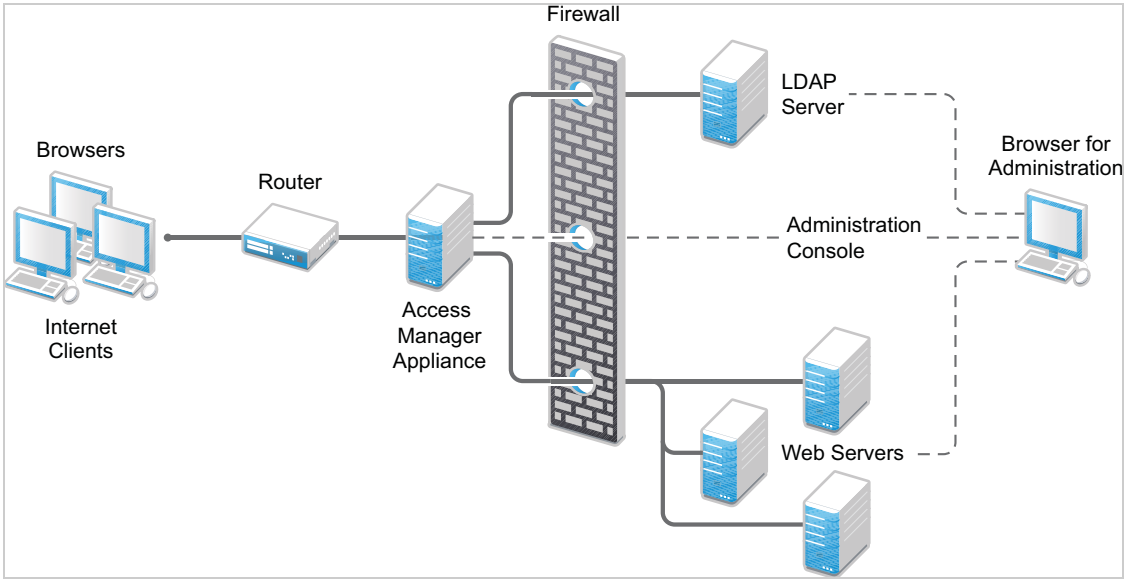
  Access Manager Appliance know each other by their IP addresses, and some requests require them to match an IP address with the device's DNS name. Without reverse lookups enabled, these requests fail. In particular, Identity Servers perform reverse lookups to their user stores. If reverse lookups are 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.

Basic Setup

Figure 1-4 illustrates the basic Access Manager Appliance installation, where Access Manager Appliance is installed outside your firewall. The figure provides an overview of the flexibility built into Access Manager Appliance. You can use it to design a deployment strategy that fits the needs of your company.

Figure 1-4 *Basic Configuration*



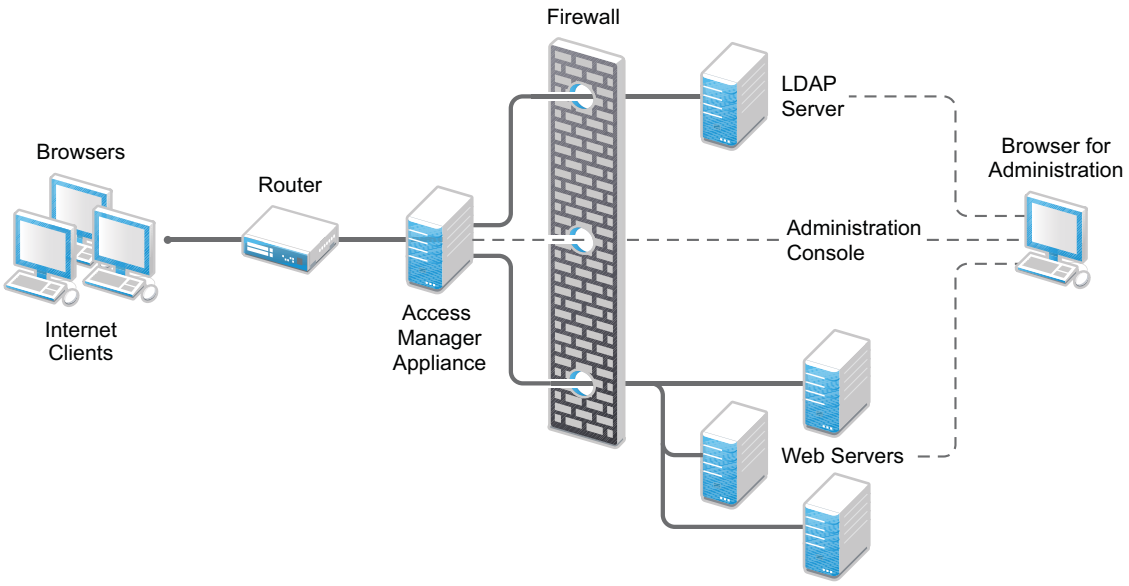
For more information, see “Installing Access Manager Appliance” on page 30.

The firewall protects the LDAP server, which contains a permanent store of sensitive data. The Web servers are also installed behind the firewall for added protection. This is a tested and recommended configuration. We have also tested this configuration with an L4 switch in place of the router so that the configuration can support clusters of Access Manager Appliance.

Setting Up Firewalls

Access Manager Appliance should be used with firewalls. Figure 1-5 illustrates a simple firewall setup for a basic Access Manager Appliance configuration.

Figure 1-5 *Access Manager Appliance and Firewall*



The first firewall separates the Access Manager Appliance from the Internet, allowing browsers to access the resources through specific ports. This is one of many possible configurations. This section describes the following:

- "Required Ports" on page 23
- "Sample Configurations" on page 25

Required Ports

The following table lists the ports that need to be opened when a firewall separates Access Manager Appliance from Internet.

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

Component	Port	Description
NTP Server	UDP 123	Access Manager components must have time synchronized else the authentication fails. We highly recommend that all components be configured to use an NTP (network time protocol) server. Depending upon where your NTP server is located in relationship to your firewalls, you might need to open UDP 123 so that the Access Manager component 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 the Access Manager component can resolve DNS names.

Component	Port	Description
Remote Linux Administration Workstation	TCP 22	If you use SSH for remote administration and want to use it for remote administration of Access Manager components, you need to open TCP 22 to allow communication from your remote administration workstation to your Access Manager components.
Access Manager Appliance	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 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 the devices to the 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.
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.
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.
	TCP 8028, 8030	To use iMonitor or DSTrace from a client to view information about the configuration store on the Administration Console.
	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 the Web servers. This is configurable.

NOTE: On SLES 11 SP4, you can edit this file or use YaST to configure UDP ports and internal networks.

Sample Configurations

Access Manager Appliance in DMZ

First Firewall

If you place a firewall between browsers and Access Manager Appliance, 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 1-5 on page 23

Table 1-2 *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.
TCP 8443	For HTTPS communication with the Identity Server.
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 1-3 *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.

You need to open ports on the second firewall according to the offered services.

2 Installing Access Manager Appliance

This chapter explains how to install Access Manager Appliance. Topics include:

Installation Requirements

This section explains requirements for installing Access Manager Appliance. For a list of current filenames and for information about installing the latest release, see the Readme of that release on the NetIQ Access Manager Documentation Web site.

The Access Manager Appliance installer installs all components on a single server, so software and hardware requirements are same for all components. *"Access Manager Versus Access Manager Appliance" on page 14* lists differences between previously shipped Access Manager versus Access Manager Appliance.

Access Manager Appliance is based on the SUSE Linux Enterprise Server (SLES) 11 SP4 64-bit operating system. The hard disk, RAM, and CPU requirements are same for all components.

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

Hardware Platform Requirements

The following are the hardware requirements:

- 8 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.

  2 to10 GB per reverse proxy that requires caching and for log files. The amount varies with the rollover options and logging level that you configure.
- The static IP address and an assigned DNS name (hostname and domain name) for your Access Manager Appliance.

Browser Support

The following browsers are supported for users to log in to Access Manager Appliance:

- Internet Explorer 11 or higher (Non Metro UI)
- Mozilla Firefox
- Chrome

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

Client Access Requirements

Clients can use any browser or operating system when accessing resources protected by the Access Gateway.

Installation Mode

You must install Access Manager Appliance by burning the Access Manager Appliance ISO on a DVD.

Virtual Machine Requirements

The virtual machine must have enough resources. The requirements for a virtual machine need to match the requirements for a physical machine. To achieve the performance similar to a physical machine, increase the memory and CPU requirements.

For the hard disk, RAM, and CPU requirements, each virtual machine should meet the following minimum requirements:

- 100 GB of disk space
- 8 GB RAM
- 2 CPUs

You can use the virtual machines that are supported on SUSE Linux Enterprise Server (SLES) 11 SP3 and SLES 12 with 64-bit operating system x86-64 hardware.

NOTE: SLES 11 SP4 64-bit Access Manager Appliance does not support XEN paravirtualization for the 4.2 release.

The following sections contain installation tips for virtual machines:

- “Keeping Time Synchronized on Access Manager Appliances” on page 28
- “Number of Virtual Machines Per Physical Machine” on page 29
- “Using a Network Adapter for VMWare ESX” on page 29

Keeping Time Synchronized on Access Manager Appliances

Even when virtual machines are configured to use a network time protocol (NTP) server, time does not stay synchronized because the machines periodically lose their connection to the NTP server. The easiest solution is to configure primary Access Manager Appliance to use an NTP server and configure other Access Manager Appliance to use a cron job to synchronize their time with primary Access Manager Appliance.

SLES 11 SP4: The `ntpdate` command is not supported by SLES 11 SP4 64-bit. You can use the `sntp` command. Add the following command to the `/etc/crontab` file of the device:

```
*/5 * * * *   root   /usr/sbin/sntp -P no -r 10.20.30.108 >/dev/null 2>&1
```

Replace 10.20.30.108 with the IP address of your NTP server.

Number of Virtual Machines Per Physical Machine

How you deploy your virtual machines can greatly influence the Access Manager Appliance performance. Deploy maximum of four Access Manager Appliance virtual machines on a single piece of hardware. When you start deploying more than four, components of Access Manager Appliance start competing with each other for same hardware resources at the same time. You can include other types of services that the machine can support if they do not use the same hardware resources that Access Manager Appliance components use.

The configured CPUs must match the hardware CPUs on the machine. Performance is drastically reduced if you allocate more virtual CPUs than actually exist on the machine.

Another potential bottleneck is IO. For best performance, each virtual machine should have its own hard disk, or you need a SAN that is capable of handling the IO traffic.

For example, if you have one 16-CPU machine, you get better performance when you configure the machine to have four Access Gateways with 4 assigned CPUs than you get when you configure the machine to have eight Access Gateways with 2 assigned CPUs. If the machines are dedicated to Access Manager Appliance components, you get better performance from two 8-CPU machines than you get from one 16-CPU machine.The setup depends on your unique environment and hardware and virtualization configuration for your cluster.

Using a Network Adapter for VMWare ESX

Use the E1000 network adapter for Access Manager Appliance installation on VMWare ESX.

Network Requirements

Your network environment must meet the following requirements:

- 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.
- Static IP addresses for each Access Manager Appliance. If the IP address of the machine changes, Access Manager Appliance components cannot start.
- Domain name server, which resolves DNS names to IP addresses and that has reverse lookups enabled.

  Access Manager Appliance components know each other by their IP addresses. 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 the reverse lookups are not available, host table entries can be used.
- Network time protocol (NTP) server 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.

Installing Access Manager Appliance

Installation time: 45 to 90 minutes, depending on the hardware.

What you need to know	◆ Root password of Access Manager Appliance. ◆ Username and password of the Administration Console administrator. ◆ Static IP address for Access Manager Appliance. ◆ 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 tree for the configuration store is named after the server on which you install Access Manager Appliance. Check the hostname and rename the machine if the name is not appropriate for a configuration tree name.

Access Manager Appliance can be installed on all supported hardware platforms for SLES 11 SP4 (64-bit).

Prerequisites

- ❒ Ensure that you have backed up all data and software on the disk to another machine. The Access Manager Appliance installation completely erases all the data on your hard disk.
- ❒ Ensure that the machine meets the minimum hardware requirements. See "Installation Requirements" on page 27.
- ❒ (Optional) If you want to try any advanced installation options such as driver installation or network installation, see the *Deployment Guide* (http://www.suse.com/documentation/sles11/book_sle_deployment/data/book_sle_deployment.html).
- ❒ (Optional) On RHEL, ensure that the SELinux configuration allows communication with local TCP port 1290.

Installing Access Manager Appliance

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

NOTE

- Do not install or import any non- 4.2 Appliance devices during installation.
- 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.

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

1. Insert the Access Manager Appliance CD into the CD drive.

   The boot screen appears.
2. By default, the **Boot From Hard Disk** option is selected in the boot screen.

   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. Click **Next**.
7. Configure the details on the Appliance Configuration page:

Field	Description
Host Name	The hostname for the Access Manager Appliance machine.
Domain Name	The domain name for your network.
Public IP	Configure the following options for the public IP: • **IP Address:** The public IP address of Access Manager Appliance. • **Subnet Mask:** The subnet mask of Access Manager Appliance. • **Default Gateway:** The IP address of the default gateway.
Private IP	Configure the following options for the private IP. This is an optional configuration. If this is configured, the Administration Console listens on this IP. • **IP Address:** Private IP address of Access Manager Appliance. • **Subnet Mask:** Subnet mask of Access Manager Appliance. • **Gateway:** IP address of the gateway.
DNS Server 1	IP address of your DNS server. You must configure at least one DNS server.
DNS Server 2	IP address of your additional DNS server. This is an optional configuration.
In the Root Password section, specify password for the `root` user and name of the NTP server.	

8. Click **Next**.

Configure the following details under the Administration Console Configuration:

Field	Description
Primary	Deselect this option to specify if this Access Manager Appliance is not primary. If you are installing it as a secondary Access Manager Appliance then ensure that the primary Access Manager Appliance is reachable.
Admin Console IP	Specify the IP address of the primary Access Manager Appliance if this is secondary.
Username	The name of the Administration Console user. **NOTE:** The Administration Console username does not accept special characters # (hash), & (ampersand), and ( ) (round brackets).
Password	Specify and confirm the password for the user. **NOTE:** The Administration Console password does not accept special characters : (colon) and " (double quotes).

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.

Do not change the software selections listed on this screen.

10 (Optional) To modify the installation settings for partitions, click **Change**.

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

This process might take 45 to 90 minutes depending on the configuration and hardware.

The machine reboots after the installation is completed. It runs an auto configure script, and then the Access Gateway and Identity Server components are configured.

12 (Optional) Verify if Access Manager Appliance is installed and configured successfully.

Log in to the Administration Console. See “Logging In to the Administration Console” on page 34), then 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.

The Access Gateway health is displayed as green. The configuration takes care of establishing a trust relationship between an embedded service provider and the Access Gateway and also the trust relationship with the Identity Server before you proceed with any other configuration.

12a In a browser, enter the Access Manager Appliance URL. The Access Manager Appliance URL is formed by using the Host Name and Domain Name provided in the Step 8. For example, if the host name is `accessapp` and the domain name is novell.com, then the URL will be `https://accessapp.novell.com`. You will be redirected to the Sample Portal Page.

12b Click the Administration Console link and log in to.

12c Click **Devices**> **Access Gateways**. The Servers tab displays AG-Cluster with one Access Gateway. The IP Address of the Access Gateway is same as the Access Manager Appliance IP Address. The health of both the AG-Cluster and Access Gateway should display green.

13 Continue with one of the following sections:

- "Removing the Landing Portal" on page 33
- Setting up User Stores for Identity Server Configuration and Configuring the Access Gateway in the NetIQ Access Manager Appliance 4.2 Administration Guide.

Removing the Landing Portal

The landing portal is enabled by default during the installation of Access Manager Appliance. The portal also has a sample application, which you can configure to learn Access Manager Appliance capabilities. The landing portal is visible to users, hence it is not recommended to use in the production setup. Use it for demonstration and trial purposes. Remove the landing portal after you verify all your configurations in a staging environment.

Perform the following steps to remove the landing portal:

1 In the Administration Console, click **Access Gateway** > **Cluster** > **Edit** > **NAM - RP.**

2 Select the **namportal** path based service.

3 Click **Delete**.

4 Click **Protected Resources**.

Delete the following protected resources:

- portal_employee
- portal_manager
- portal_public
- portal_users

5 Click **OK** > **Update**.

6 In the Administration Console, click **Devices** > **Identity Servers** > **Servers** > **Edit** > **Roles**.

7 Select the role policy check box, select the **portal_roles** role from the Roles Policy List, and click **Disable**.

8 Click **OK** > **Update**.

9 To remove the portal web application from the Access Manager Appliance filesystem, perform the following steps:

9a Log in to Access Manager Appliance by using any SSH client (for example, SSH in Linux and PuTTY in Windows).

9b Stop the Administration Console by using the `/etc/init.d/novell-ac stop` command.

9c Go to the portal directory by running the `cd /opt/novell/nam/adminconsole/webapps` command.

9d Remove the portal by running the `rm -rf portal` command.

9e Start the Administration Console by running the `/etc/init.d/novell-ac start` command.

10 The portal creates two default users Alice and Bob in the Appliance Configuration store.

You can remove the users by performing the following steps:

10a In the Administration Console, click **Roles and Tasks** > **Users** > **Delete User**.

10b In the Delete User page, specify the Object Name as bob.novell to delete Bob and alice.novell to delete Alice.

10c Click **OK**.

NOTE: Optional: You can delete Employee, Manageronly, portal_formfill, portal_id_injection, portal_roles policies on the Policies page.

Logging In to the Administration Console

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

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

You should not download and add iManager plug-ins to this customized version. If you do, you can destroy the Access Manager Appliance schema, which can prevent you from managing the Access Manager Appliance components. This can also prevent communication among the modules.

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

To log in to:

1 Enable browser pop-ups.

2 From a client machine external to your Administration Console server, launch your preferred browser and enter the URL for the Administration Console.

If the hostname of your Access Manager Appliance is www.host.com, you would enter `http://www.host.com:8080/nps`.

3 Click **OK**. You can select either the permanent or temporary session certificate option.

4 Specify the administrator name and password that you defined during installation and click **Login**. Access Manager Appliance Dashboard opens.

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

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

To understand the conventions of the Administration Console, see “Administration Console Conventions” on page 35.

Administration Console Conventions

- The required fields on a configuration page contain an asterisk by the field name.
- All actions such as delete, stop, and purge require verification before they are executed.
- Changes are not applied to a server until you update the server.
- Sessions are monitored for activity. If your session becomes inactive, you are asked to log in again and unsaved changes are lost.

Upgrading Access Manager Appliance

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

For more information, see "Back Up and Restore" in the *NetIQ Access Manager Appliance 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. For more information, see "Removing Portal Related Proxy Service And Protected Resources" on page 47
- Access Manager indicates the Access Gateway cluster health in yellow if you do not remove the proxy services and protected resources that refer to SSL VPN and the portal.
- If you are upgrading to Access Manager 4.2 from 4.0.x or earlier, the Access Manager Appliance portal is no longer available. After you upgrade to Access Manager Appliance 4.2, manually remove the proxy services and protected resources that refer to the portal. For more information, see "Removing Portal Related Proxy Service And Protected Resources" on page 47.
- 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 Appliance," on page 37.

This part describes how to upgrade Access Manager Appliance:

3 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 Appliance 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 39 or “Maintaining Customized JSP Files for Access Gateway” on page 41.
- 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 Appliance 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 Access Manager Appliance.
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 Access Manager Appliance.

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 Manager Appliance.
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.

4 Upgrading the Operating System for Access Manager Appliance

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

NOTE: After upgrading, you also need to re-register the new channel. For more information, Section 10.1, “Setting Up the 4.2 Channel,” on page 124.

Perform the following steps to upgrade the base operating system:

1. Get the Access Manager4.2 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/ 42appiso
   ```

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 42appiso
   ```

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 Manager 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 Section 10, “Upgrading the Operating System for Access GatewayManager Appliance,” on page 123.
2. Upgrade the Access Manager 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 Section 12.1, “Installing or Updating Security Patches for the Access Gateway ApplianceAccess Manager Appliance,” on page 137.
7. Use the `zypper lr` command to verify if the new channel `NAM42-APP-Updates` is added.

5 Upgrading Access Manager Appliance

5.1 Upgrading from the Evaluation Version to the Purchased Version

1. Log in as `root`.
2. Download the upgrade file from dl.netiq.com and extract the `tar.gz` file by 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.
3. Change to the directory where you extracted the file, then run the following command:

   `./sb_upgrade.sh`
4. The system displays a message regarding restoring customized files.

   For more information about how to sanitize jsp pages, see Preventing Cross-site Scripting Attacks in the NetIQ Access Manager Appliance 4.2 Administration Guide.
5. A confirmation message is displayed.

   ```
   Would you like to continue this upgrade?
   ```

   Type **Y** to continue.
6. Enter the Access Manager Administration Console user ID.
7. Enter the Access Manager Administration Console password.
8. Re-enter the password for verification.

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

   ```
   Upgrade completed successfully.
   ```

5.2 Upgrading Access Manager Appliance

Prerequisite: Before upgrading Access Manager Appliance, perform the following actions:

1. Before upgrading, you must first upgrade the base operating system of the 3.2 SP3 or higher to the latest operating system that is included in the 4.2 Access Manager Appliance ISO. For more information about how to upgrade, see Section 4, “Upgrading the Operating System for Access Manager Appliance,” on page 43.
2. If you are upgrading Access Manager to 4.2, and want to use syslog for auditing, you must first upgrade the base operating system.

3. (Optional) On RHEL, ensure that the SELinux configuration allows communication with local TCP port 1290.
4. 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.

NOTE: If you do not upgrade the base operating system before upgrading to 4.2, upgrade will display a warning message, but still allow upgrading to 4.2. If you are using versions earlier than 3.2 SP3, upgrade displays an error and terminates.

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. For more information about auditing, see Configuring Access Manager Appliance for Auditing in the NetIQ Access Manager Appliance 4.2 Administration Guide

---

Perform the following steps to upgrade Access Manager Appliance.

1 Log in as `root`.

2 Download the `tar.gz` file of Access Manager Appliance 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 file, see the Access Manager Appliance 4.2 Release Notes on theAccess Manager Documentation website.

---

3 Change to the directory where you extracted the file, then run the following command:

```
./sb_upgrade.sh
```

4 A confirmation message is displayed.

NOTE: If you have upgraded the base Operating System and want to upgrade Access Manager 4.2 to 4.2.1, then you can ignore the following message.

```
Platform Agent is no longer supported for auditing. It is recommended to use
Syslog instead. To use Syslog, ensure that you upgrade the base Operating
System followed by Access Manager/Gateway Appliance upgrade. After upgrading,
enable Syslog on the Auditing user interface of the Administration Console. Do
you want to proceed? (Y/N)
```

Type **Y** to continue.

5 The system displays a message regarding restoring customized files:

```
Before you restore your existing custom pages, ensure that you read and
understand the changes in steps from the Installation and Upgrade guide
available online.
# It is recommended that you run XSS checks for restored JSP files as
instructed in the Installation and Upgrade guide available online.
```

Type **Y** to confirm.

For more information about how to sanitize JSP pages, see Preventing Cross-site Scripting Attacks in the NetIQ Access Manager Appliance 4.2 Administration Guide.

6 Type **Y** and press Enter.

The system displays an information message to upgrade the base operating system and enable Syslog.

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

The system displays a warning message to back up the existing JSP files.

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.

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

```
Upgrade completed successfully.
```

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

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/RiskDBScripts.zip`.

MySQL: Run `netiq_risk_mysql_upgrade.sql`

Oracle: Run `netiq_risk_oracle_upgrade.sql`

NOTE: To use Syslog for auditing, you need to upgrade the base operating system. After the upgrade, install the Syslog RPMs manually. To install the RPMs, execute the following command: `zypper in -t pattern NetIQ-Access-Manager`.

5.2.1 Removing Proxy Services And Protected Resources

After upgrading Access Manager, manually remove the portal and SSL VPN related proxy service and protected resources.

Removing Portal Related Proxy Service And Protected Resources

1 In the Administration Console, click **Access Gateway > Cluster > Edit > NAM - RP**.

2 Select the `namportal` path based service. Click **Delete**.

3 Click **Protected Resources**. Delete the following Protected Resources: **portal** and **portal_public**.

4 Click **OK** until the Access Gateway Servers page appears. Click **Update**.

Removing SSLVPN Related Proxy Service And Protected Resources

1 In the Administration Console, click **Access Gateway > Cluster > Edit > NAM - RP**.

2 Select the `sslvpn` path based service. Click **Delete**.

3 Click **Protected Resources**. Delete the following Protected Resources: **sslvpn** and **sslvpn_public**.

4 Click **OK** until the Access Gateway Servers page appears. Click **Update**.

6 Getting the Latest Security Patches

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

Prerequisites

- ❒ Before upgrading the kernel, ensure that you have updated the operating system to a supported version.
- ❒ Access Manager 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 Appliance 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 Access Manager Appliance” on page 49

Installing or Updating Security Patches for Access Manager Appliance

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

- “Registering to Novell Customer Center” on page 49
- “Configuring Subscription Management Tool for Access Manager Appliance” on page 50

Registering to Novell Customer Center

To get the latest security updates for Access Manager 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 | NetIQAccessManagerAppliance-4.x.x-x | NetIQAccessManagerAppliance-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 Access Manager Appliance

Access Manager 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 Manager Appliance:

SMT Configuration

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