NetIQ®

Access Manager Appliance 4.5

Installation and Upgrade Guide

April 2019

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

You can access other information resources in the library at the following locations:

- Access Manager Developer Resources (https://www.netiq.com/documentation/access-manager-45-developer-documentation/)

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

1 Planning Your Access Manager Environment

1.1 Deployment Models

The product is available in the following two deployment models:

- **Access Manager:** To deploy individual components (Identity Server, Access Gateway, Analytics Server and Administration Console). You can install and manager each component on separate servers. Access Manager 4.4 SP1 onwards, Administration Console, Identity Server, and Access Gateway can also be deployed as services on AWS EC2 and Microsoft Azure.
- **Access Manager Appliance:** To deploy all components together as an appliance. It is a soft appliance based on SUSE Linux Enterprise Server. It bundles pre-configured Identity Server, Access Gateway, and Administration Console in one server. You can install and manage Analytics Server on a separate server. This model enables organizations to deploy and secure web and enterprise resources quickly. 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 Access Manager 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 Section 1.2, "Access Manager Versus Access Manager Appliance," on page 9.

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

Figure 1-1 *Typical Deployment of Access Manager*

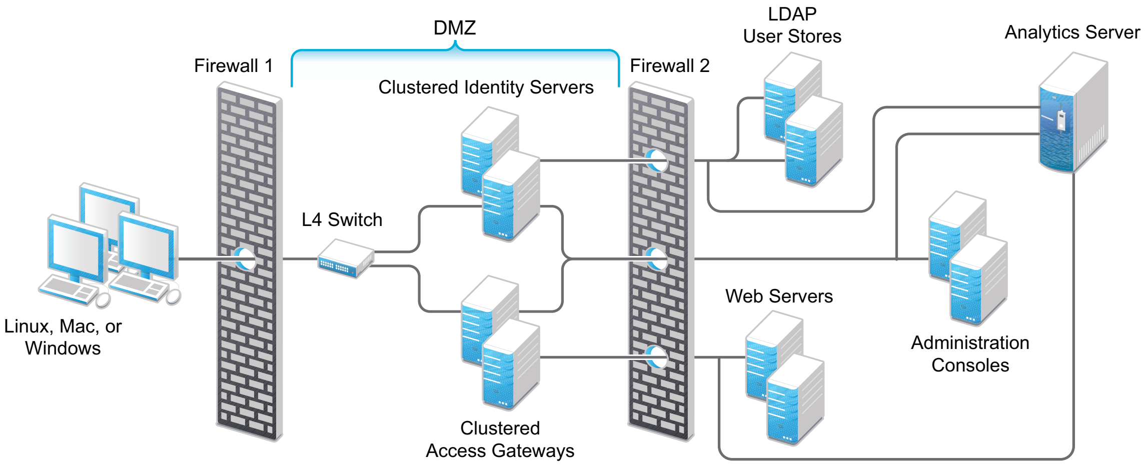
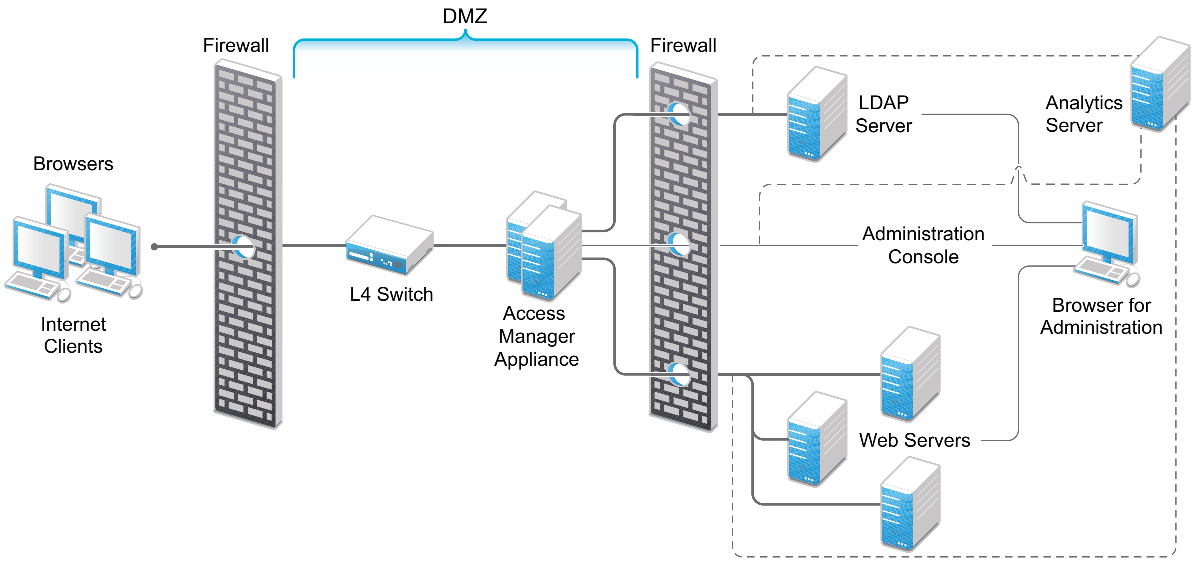


Figure 1-2 *Typical Deployment of Access Manager Appliance*



1.2 Access Manager Versus Access Manager Appliance

Both Access Manager and Access Manager Appliance deployment models use a common code base. However, a few differences exist between 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) 12 SP5 with 64-bit operating system x86-64 hardware.	Supported on the virtual servers based on SLES 12 SP3 or SLES 12 SP4 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 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 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 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. See *NetIQ Access Manager Performance and Sizing Guidelines* .	Scales both vertically and horizontally on adding nodes. See *NetIQ Access Manager Performance and Sizing Guidelines* .

Feature	Access Manager Appliance	Access Manager
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.
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 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	Administration Console and Identity Server are accelerated and protected by Access Gateways. Only HTTPS port 443 is required to access 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.
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.

Feature	Access Manager Appliance	Access Manager
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.
Associating different certificates to Identity Server	Not applicable because Identity Server is accelerated by Access Gateway.	Supported. Identity Server can be behind 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 after Access Manager Appliance installation: ◆ Importing Identity Server and Access Gateway. ◆ Cluster creation of Identity Server and Access Gateway. ◆ Configuration of Identity Server to bring it to green state. ◆ Configuration of Access Gateways and Identity Server association. ◆ Service creation to accelerate or protect 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 requires manual configuration and setup before web applications can be federation enabled, accelerated, and 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 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 Administration Console, Identity Server, and Access Gateway. Fourth installation onwards, the node does not contain Administration Console. A typical Access Manager Appliance deployment in a cluster is described in Figure 1-3.	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.

Figure 1-3 *Access Manager Appliance Cluster*

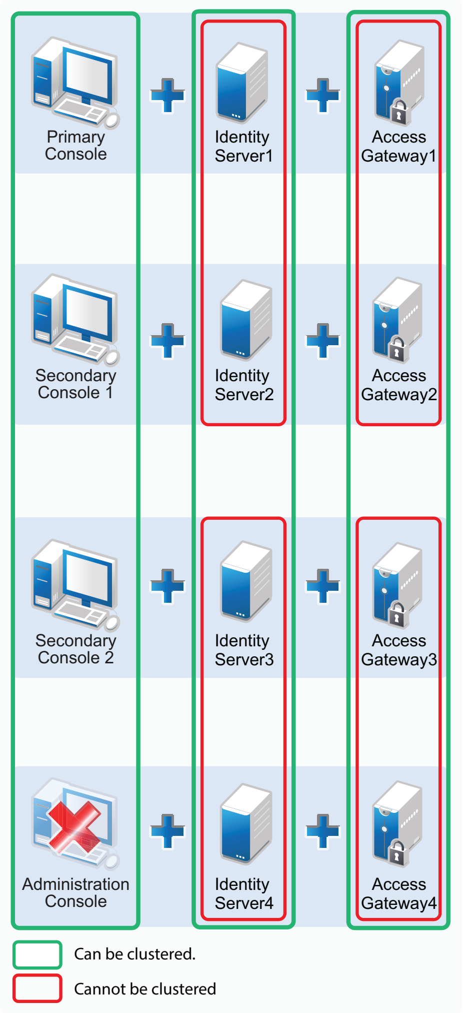
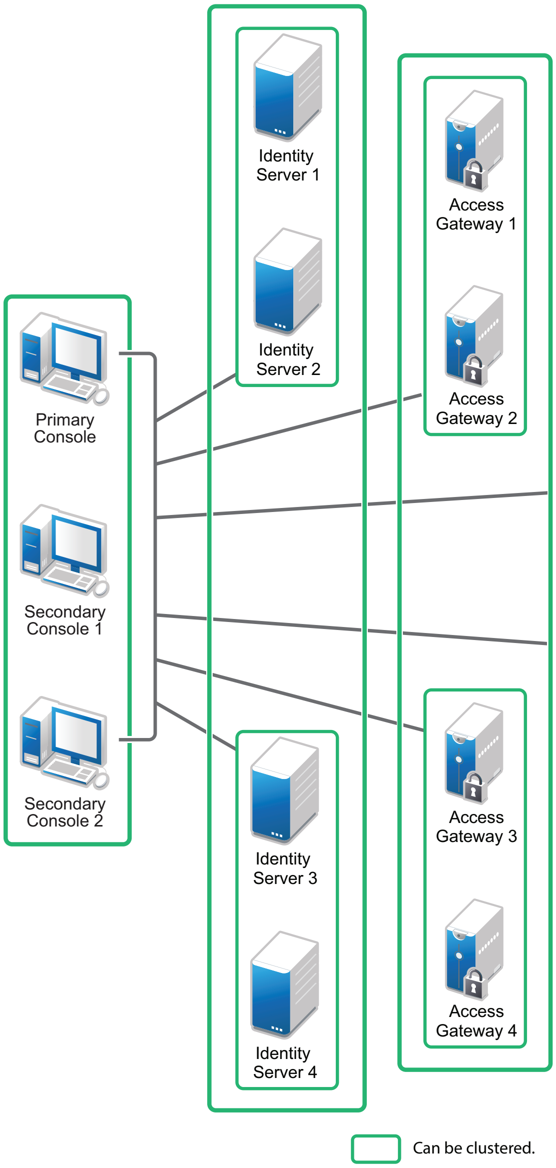


Figure 1-4 Access Manager Cluster



General Guidelines

- Adding an Access Gateway Service or Access Gateway Appliance to an Access Manager Appliance cluster is not possible.
- Deploying 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 Access Manager. This might 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 4.5 Administration Guide.
- You cannot have different certificates for signing and encryption in a federation setup.

- You cannot install any monitoring software to monitor statistics in 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.

1.3 Network Requirements

In addition to the servers on which Access Manager software is installed, your network environment must meet the following requirements:

- An LDAP directory (eDirectory, Sun ONE, Active Directory, or Azure Active Directory) that contains your system users. Identity Server uses the LDAP directory to authenticate users.

  NOTE: Azure Active Directory is supported when Access Manager is deployed on Microsoft Azure.

- Web servers with content or applications that need protection and single-sign on.
- Static IP addresses for each Access Manager Appliance. If the IP address of the machine changes, Access Manager Appliance components cannot start.
- A 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.

- Time must be synchronized to within one minute among all components of the configuration using NTP or similar solution.

  IMPORTANT: If time is not synchronized, users cannot authenticate and access resources.

- (OPTIONAL) An L4 switch or similar solution if you are planning to configure load balancing.
- Clients with an Internet browser.

1.4 System Requirements

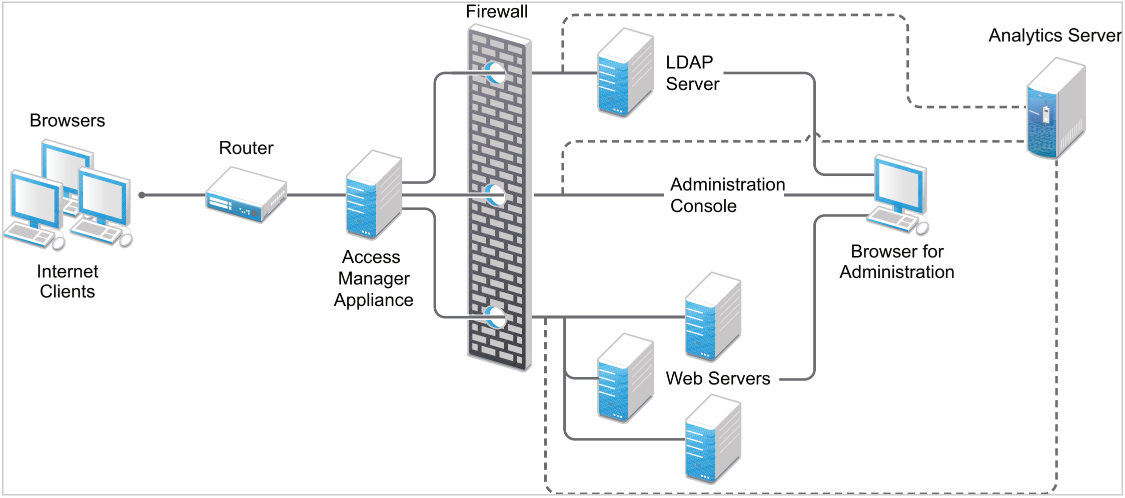
See the following sections in the *NetIQ Access Manager System Requirements* guide:

- System Requirements: Administration Console, Identity Server, Access Gateway
- System Requirements: Analytics Server
- System Requirements: Access Manager Appliance
- Browser Support

1.5 Basic Setup

Figure 1-5 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 1-5 *Basic Configuration*



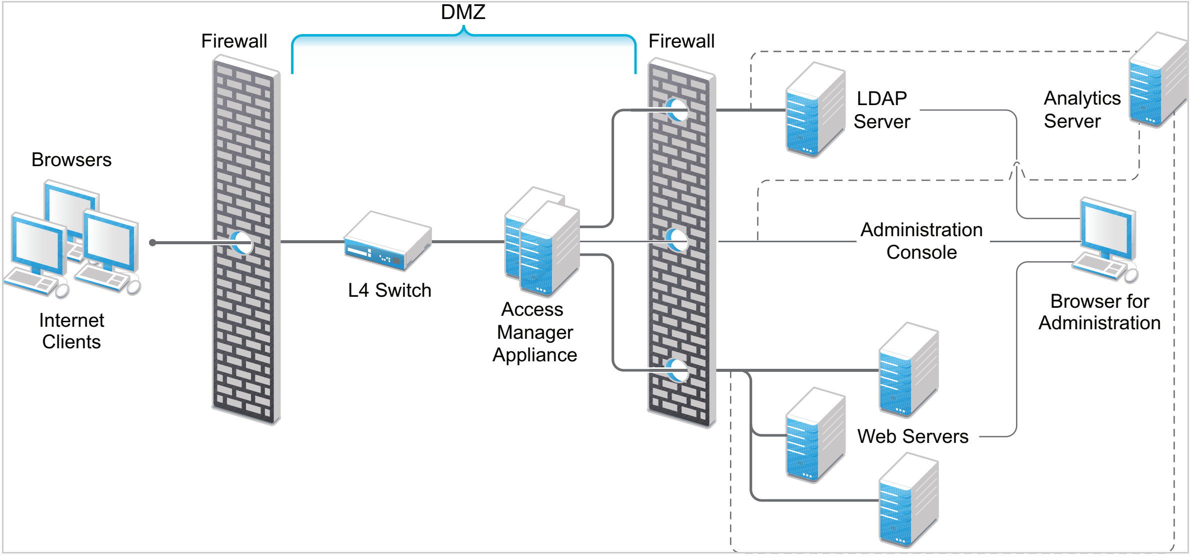
For more information, see Section 2.2.2, “Installing Access Manager Appliance,” on page 25.

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.

1.6 Setting Up Firewalls

It is recommended to use Access Manager Appliance with firewalls. Figure 1-6 illustrates a simple firewall setup for a basic Access Manager Appliance configuration. This is one of many possible configurations.

Figure 1-6 Access Manager Appliance and Firewall



The first firewall separates Access Manager Appliance from the Internet, allowing browsers to access the resources through specific ports.The second firewall separates Access Manager Appliance from web servers they are protecting.

This section describes the following topics:

- Section 1.6.1, "Required Ports," on page 16
- Section 1.6.3, "Sample Configurations," on page 19

1.6.1 Required Ports

Table 1-2 When a Firewall Separates Access Manager Appliance from Internet

Component	Port	Description
NTP Server	UDP 123	Access Manager Appliance must have time synchronized else the authentication fails. Configure Access Manager Appliance to use an NTP (network time protocol) server. Depending on where your NTP server is located in relationship to your firewalls, you might need to open UDP 123.
DNS Servers	UDP 53	Access Manager Appliance 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 Appliance can resolve DNS names.

Component	Port	Description
Remote Linux Administration Workstation	TCP 22	To use SSH for remote administration of Access Manager Appliance.
Access Manager Appliance	TCP 1443	For communication from Administration Console to devices.
	TCP 8444	For communication from devices to Administration Console.
	TCP 1290	For communication from devices to the Syslog server on Administration Console.
	TCP 524	For NCP certificate management with NPKI. The port needs to be opened so that both the device and Administration Console can use the port.
	TCP 636	For secure LDAP communication from the devices to Administration Console.
	TCP 524	Required to synchronize the configuration data store.
	TCP 636	Required for the secure LDAP communication.
	TCP 8080, 8443	Used for the Tomcat communication.
	TCP 7801	Used for back-channel communication with cluster members.
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 Administration Console. It is not used in day-to-day operations.
Browsers	TCP 8080	For HTTP communication from browsers to Administration Console.
	TCP 8443	For HTTPS communication from browsers to Administration Console.
	TCP 8028, 8030	To use iMonitor or DSTrace from a client to view information about the configuration store on Administration Console.
	TCP 80	For HTTP communication from the client to Access Gateway. This is configurable.
	TCP 443	For HTTPS communication from the client to Access Gateway. This is configurable.
Web Servers	TCP 80	For HTTP communication from Access Gateway to web servers. This is configurable.
	TCP 443	For HTTPS communication from Access Gateway to web servers. This is configurable.

NOTE: On SLES 12 SP5, you can edit this file or use YaST to configure UDP ports and internal networks.

Table 1-3 When a Firewall Separates Analytics Server from Administration Console or any Services

Component	Port	Description
Administration Console	TCP 1444	For communication between Administration Console and Analytics Server.
Browsers	TCP 8445	For HTTPS communication with Analytics Server for Analytics Dashboard.
Browsers	TCP 8443	For HTTPS communication with Analytics Server for Reports console.
Syslog	TCP 1468	For sending Syslog messages from Access Manager components to Analytics Server.
Control Center	TCP 10013	For communicating from a computer to the control center on Analytics Server.
Remote Linux Administration Workstation	TCP 22	For communication from your remote administration workstation to Analytics Server.
High availability configuration	TCP 7360	For communication between the servers in an Analytics Server cluster.

1.6.2 Restricted Ports

The following ports are reserved for internal use only and other applications should not use these:

22
111
524
1443
2443
3443
8028
8030
8080
8443
8444
9000
9001
55982
61222
61613
61616
61617
9443
9090

If required, use port redirection by using IP tables.

1.6.3 Sample Configurations

- Section 1.6.3.1, “Access Manager Appliance in DMZ,” on page 19

1.6.3.1 Access Manager Appliance in DMZ

- “First Firewall” on page 19
- “Second Firewall” on page 19

First Firewall

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

See, Figure 1-6 on page 16

***Table 1-4** 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 Identity Server.
TCP 8443	For HTTPS communication with 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 Administration Console from Identity Server and Access Gateway. You need the following ports opened in the second firewall:

***Table 1-5** 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.	

Port	Purpose
TCP 1443	For communication from Administration Console to the devices.
TCP 8444	For communication from the devices to Administration Console.
TCP 1290	For communication from the devices to the Syslog server installed on 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 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.

1.7 Using Certificates for Secure Communication

When you install Administration Console, the following test certificates are automatically generated:

test-signing
test-encryption
test-connector
test-provider
test-consumer
test-stunnel

For strong security, it is recommended that you replace these certificates, except the test-stunnel certificate, with certificates from a well-known certificate authority.

For more information, see "Strengthening Certificates " in the *NetIQ Access Manager Appliance 4.5 Security Guide*.

Installing Access Manager Appliance

This section includes the following topics:

- Chapter 2, “Installing Access Manager Appliance,” on page 23
- Chapter 3, “Installing Analytics Server,” on page 31

2 Installing Access Manager Appliance

This section includes the following topics:

- Section 2.1, “Requirements for Installing Access Manager Appliance,” on page 23
- Section 2.2, “Installing Access Manager Appliance,” on page 25

For information about differences between Access Manager and Access Manager Appliance*, see Access Manager Versus Access Manager Appliance*.

2.1 Requirements for Installing Access Manager Appliance

For a list of current filenames and for information about how to install a specific release, see the Release Notes of that release on the NetIQ Access Manager Documentation website.

For system requirements, see “System Requirements: Access Manager Appliance” in the *NetIQ Access Manager System Requirements* guide.

For network requirements, see Network Requirements.

For supported browsers, see Browser Support in the NetIQ Access Manager System Requirements guide.

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

2.1.1 Client Access Requirements

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

2.1.2 Installation Mode

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

2.1.3 Virtual Machine Requirements

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 must meet the following minimum requirements:

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

You can install Access Manager on virtual machines that support an operating system supported by your Access Manager version and component. For example, SLES 12 SP5 with 64-bit operating system x86-64 hardware.

NOTE: SLES 12 SP5 64-bit Access Manager Appliance does not support XEN paravirtualization.

The following sections contain installation tips for virtual machines:

- Section 2.1.3.1, "Keeping Time Synchronized on Access Manager Appliances," on page 24
- Section 2.1.3.2, "Number of Virtual Machines Per Physical Machine," on page 24
- Section 2.1.3.3, "Using a Network Adapter for VMWare ESX," on page 25

2.1.3.1 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.

Perform the following steps to synchronize time with the primary Administration Console:

1. Configure the NTP server in the `/etc/ntp.conf` file. For information about how to configure the NTP server, see Configuring NTP (https://support.ntp.org/bin/view/Support/ConfiguringNTP).
2. Run the following command on the primary Administration Console to start the NTP server:

   ```
   rcntp start
   ```
3. Run the `ntpdate pool.ntp.org` command on the primary Administration Console to synchronize devices.

   NOTE: The `ntpd` process must be running to keep the time in sync among devices.

2.1.3.2 Number of Virtual Machines Per Physical Machine

How you deploy your virtual machines can influence Access Manager Appliance performance. Deploy maximum of four Access Manager Appliance virtual machines on a single hardware. When you deploy 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 the best performance, each virtual machine must 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, performance is better when you configure the machine to have four Access Gateways with four assigned CPUs than the machine is configured to have eight Access Gateways with two assigned CPUs. If the machines are dedicated to Access Manager Appliance, performance is better from two 8-CPU machines than one 16-CPU machine. The setup depends on your environment, hardware, and virtualization configuration for the cluster.

2.1.3.3 Using a Network Adapter for VMWare ESX

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

2.2 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 Administration Console administrator. ◆ Static IP address for Access Manager Appliance. ◆ DNS name (host and domain name) for Access Gateway that resolves to the IP address. ◆ Subnet mask that corresponds to the IP address for 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 configuration store tree 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.

You can install Access Manager Appliance on all hardware platforms supported for SLES 12 SP5 (64-bit).

2.2.1 Prerequisites

- ☐ Ensure that you have backed up all data and software on the disk to another machine. Access Manager Appliance installation completely erases all the data on your hard disk.
- ☐ Ensure that the machine meets the minimum requirements. See Requirements for Installing Access Manager Appliance.
- ☐ (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).

2.2.2 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`.

IMPORTANT: ◆Do not install or import any non-4.5 Appliance devices during installation.

- From Access Manager 4.2 onwards Platform Agent and Novell Audit are no longer supported for auditing. It is recommended to use Syslog for auditing.

Installation Procedure:

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

2 Select **Install Appliance**.

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

3 Press Enter.

4 Review the license agreement and click **I Agree**.

5 Select the region and time zone on the Clock and Time Zone page.

6 Click **Next**.

7 Specify the following details:

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, Administration Console listens on this IP. ◆ **IP Address:** The private IP address of Access Manager Appliance. ◆ **Subnet Mask:** The subnet mask of Access Manager Appliance. ◆ **Gateway:** The IP address of the gateway. **NOTE:** You must configure this option during installation if you require the private IP address later.
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** and configure the following details under 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 Administration Console user. **NOTE:** Administration Console username does not accept special characters `#` (hash), `&` (ampersand), and `()` (round brackets).
Password	Specify and confirm the password for the user. **NOTE:** Administration Console password does not accept special characters `:` (colon) and `"` (double quotes).

9 Click **Next**.

The Installation Settings 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 Access Gateway and Identity Server components are configured.

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

Log in to Administration Console (see Logging In to Administration Console) and click **Devices** > **Access Gateways**.

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

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

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

12a In a browser, enter the Access Manager Appliance URL. The 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, the URL will be `https://accessapp.novell.com`. You will be redirected to the Sample Portal Page.

12b Click 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 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:

- Section 2.2.3, "Removing the Landing Portal," on page 28
- Editing a Cluster Configuration and Configuring Access Gateway in the NetIQ Access Manager Appliance 4.5 Administration Guide.

2.2.3 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 a 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 Administration Console, click **Access Gateway** > **Cluster** > **Edit** > **NAM - RP.**

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

3 Click **Delete**.

4 Click **Protected Resources** and delete the following protected resources:

- portal_employee
- portal_manager
- portal_public
- portal_users

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

6 Click **Devices** > **Identity Servers** > **Servers** > **Edit** > **Roles**.

7 Select the role policy check box, select **portal_roles** 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 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 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 Administration Console, click **Roles and Tasks** > **Users** > **Delete User**.

10b Specify the Object Name as bob.novell to delete Bob and alice.novell to delete Alice.

10c Click **OK**.

NOTE: If required, you can delete Employee, Manageronly, portal_formfill, portal_id_injection, portal_roles policies on the Policies page.

2.2.4 Removing Proxy Services And Protected Resources

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

2.2.4.1 Removing Portal Related Proxy Service And Protected Resources

1. In 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 Access Gateway Servers page appears. Click **Update**.

2.2.4.2 Removing SSLVPN Related Proxy Service And Protected Resources

1. In 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 Access Gateway Servers page appears. Click **Update**.

2.2.5 Logging In to Administration Console

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

Do 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 Access Manager Appliance components. This can also prevent communication among the modules.

Do not start multiple sessions of Administration Console on the same machine through the same browser. Because the browser shares session information, this can cause unpredictable results in 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 the browser and enter the URL for 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 the permanent or temporary session certificate option.

4 Specify the administrator name and password that you defined during installation and click **Login**.

For information about configuring the view of Administration Console for Access Manager Appliance, see Configuring the Default View in the NetIQ Access Manager Appliance 4.5 Administration Guide.

2.2.6 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.

3 Installing Analytics Server

You can install Analytics Server after installing Administration Console.

It is recommended to use the latest Analytics Server shipped with **Access Manager 4.5 Service Pack 3 HotFix 1**.

This section includes information about how to install the latest Analytics Dashboard. For information about installing the earlier version, see Installing Analytics Server in the NetIQ Access Manager Appliance 4.4 Installation and Upgrade Guide.

IMPORTANT: Before installing the new Analytics Server, ensure to delete Analytics Server nodes of the earlier version from Administration Console.

Installation time: 10 minutes approximately

What you need to know to install Analytics Server	◆ Username and password of the Administration Console administrator. ◆ Install Administration Console and Analytics Server on separate servers. ◆ Do not perform any configuration tasks in Administration Console during the installation.

Prerequisites for Installing Analytics Server

- ❐ Ensure that the system meets the requirements for installing Analytics Server. For information about the requirements, see System Requirements: Analytics Server.
- ❐ When installing Access Manager components on multiple machines, ensure that the time and date are synchronized on all machines.
- ❐ Ensure that Administration Console is running.
- ❐ Install Analytics Server on a separate machine and ensure that the following ports in Analytics Server are open:
    - 8445
    - 1444
    - 22 (Optional)
    - 1468
    - 9200
    - 9300
- ❐ If you have custom partitioned your hard disk as follows, ensure that the free disk space mentioned against each partition is available.

Partition	**Disk Space**
/opt	5 GB

NOTE: For data and logs ensure that you have enough space available in the `/var` partition. You can also install if the entire disk has only root and swap partition.

To Install Analytics Server

1. Open a terminal window.
2. Log in as a `root` user.
3. Access the install script.
   - **3a** Ensure that you have downloaded the software.
   - **3b** If you downloaded the `tar.gz` file, unzip the file by using the following command:

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

   ```
   ./ar_install.sh
   ```
5. Specify the IP address, user ID, and password of the primary Administration Console.
6. Re-enter the password for verification. Analytics Server installation starts.

   If the installation program rejects credentials and IP address, ensure that the required ports are open on both Administration Console and Analytics Server.
7. Verify the installation. You can check the logs in `/tmp/novell_access_manager/install_ar_`.

Analytics Server Cluster Configuration

You can configure Analytics Server cluster for high availability. For a cluster, you can install Analytics Server on three servers using the `tar.gz` file.

After you install the second node of Analytics Server, perform the following steps in Administration Console:

1. **Devices** > **Analytics Servers** > **[Name of Server]** > **Health**.
2. Click **Refresh**.

Perform the same steps after installing the third node. Update one device at a time from top to down and wait for the Elasticsearch database server’s health to turn green and then refresh other servers for the update.

If the server does not come up, click **Restart** to bring all services up and running, and then manually click **Refresh** for each service.

After all servers’ health turn green, the cluster is ready for use.

II 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 4.5 Administration Guide*.

NOTE: By default, the Access Manager configuration uses stronger TLS protocols, ciphers, and other security settings. If you want to revert these settings after upgrading, see "Restoring Previous Security Level After Upgrading Access Manager Appliance" in the *NetIQ Access Manager Appliance 4.5 Security Guide*.

Supported Upgrade Paths

To upgrade to **Access Manager Appliance 4.5**, you need to be on one of the following versions of Access Manager Appliance:

- 4.4 Service Pack 2
- 4.4 Service Pack 3
- 4.4 Service Pack 4

For information about the latest supported upgrade paths, see the specific Release Notes on the Access Manager Appliance Documentation Website (https://www.netiq.com/documentation/access-manager-45-appliance/).

This section includes the following topics:

4 Prerequisites for Upgrading Access Manager Appliance

Watch the following video for important considerations that you must know before starting the Access Manager Appliance upgrade:

🎬 http://www.youtube.com/watch?v=aph7hzyZP3Q

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

- ❒ You must upgrade the base operating system from SLES11-SP4 to SLES12-SP5. For more information on upgrading, see Section 5.2, “Upgrading the Base Operating System,” on page 40.
- ❒ Any option that is configured through the `nidpconfig.properties` file will be overwritten after upgrade. Therefore, back up the `nidpconfig.properties` file before upgrading to Access Manager 4.5. After the upgrade, replace the new `nidpconfig.properties` file with the backed up file.

  Identity Server: `/opt/novell/nids/lib/webapp/WEB-INF/classes/nidpconfig.properties`

  Access Gateway:`/opt/novell/nesp/lib/webapp/WEB-INF/classes/nidpconfig.properties`
- ❒ Back up your current Access Manager configuration using `./ambkup.sh` command. For more information, see section Back Up and Restore in the NetIQ Access Manager Appliance 4.5 Administration Guide.
- ❒ Some of the options are supported only through Administration Console. After the upgrade, configure those options through 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 4.5 Administration Guide.
- ❒ Access Manager 4.2 and later versions do not support Platform Agent and Novell Audit. If you are upgrading from an older version of Access Manager where you have configured Platform Agent, ensure to remove this configuration before upgrading to the latest version. Otherwise, auditing will fail because the Platform Agent service is not available post upgrade.
- ❒ The upgrade process overwrites all customized JSP files. If you have customized JSP files for Identity Server or Access Gateway, you must perform manual steps to maintain the customized JSP files. For more information, see Section 4.1, “Maintaining Customized JSP Files for Identity Server,” on page 36 or Section 4.2, “Maintaining Customized JSP Files for Access Gateway,” on page 38.
- ❒ If you have customized any changes to `tomcat.conf` or `server.xml`, back up the files. After the upgrade, restore the files.
- ❒ If you have installed the unlimited strength java crypto extensions before upgrade, re-install it after the upgrade because a new Java version will be used.
- ❒ If you are using Kerberos, back up the `/opt/novell/nids/lib/webapp/WEB-INF/classes/kerb.properties` file. After the upgrade, restore the files.

Similarly, if you are using any customized files, ensure to back it up and copy the customized content from the backed up file to the upgraded file after the upgrade is successful.

❐ If you have made any customization in the `/opt/novell/nam/idp/webapps/nidp/META-INF/context.xml` file, back up the file.

After the upgrade, add the customized content to the upgraded `context.xml` file and uncomment the following lines in the `context.xml` file:

```
<!-- Force use the old Cookie processor (because this new tomcat version uses RFC6265 Cookie Specification) -->

<!--  <CookieProcessor className="org.apache.tomcat.util.http.LegacyCookieProcessor" /> -->

  </Context>
```

❐ (Linux) Ensure to perform the following procedure for both SLES 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.

❐ If you have enabled history for risk-based authentication in a prior version of Access Manager, you must upgrade the database for risk-based authentication after upgrading to 4.5. 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`

Microsoft SQL Server: Run `netiq_risk_sql_server_upgrade.sql`

In addition to the these prerequisites, ensure that you also meet the hardware requirements. For more information about hardware requirements, see the component-specific requirements in Part I, “Installing Access Manager Appliance,” on page 21.

4.1 Maintaining Customized JSP Files for Identity Server

Access Manager Appliance contains a default user portal and a set of default login pages from Access Manager 4.2 onwards. 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

4.1.1 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/nids/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.

4.1.2 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/nids/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.

4.2 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.

5 Upgrading Access Manager Appliance

From Access Manager 4.5.3 patch 2 update onwards, in order to upgrade Access Manager Appliance you must complete the following actions:

1. Upgrade the base operating system using Section 5.2, “Upgrading the Base Operating System,” on page 40.
2. Running the product upgrade script using information provided in Section 5.3, “Upgrading Access Manager Appliance,” on page 42.

5.1 Upgrading from the Evaluation Version to the Purchased Version

1 Log in as the `root` user.

2 Download the upgrade file from Software Licenses and Downloads 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 Appliance Documentation website (https://www.netiq.com/documentation/access-manager-45-appliance/).

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 4.5 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 the Base Operating System

To upgrade Access Manager Appliance, the following actions are mandatory:

1. Upgrading the base operating system from SLES 11 SP4 to SLES 12 SP5.
2. Running the product upgrade script using information provided in Section 5.3, “Upgrading Access Manager Appliance,” on page 42.

NOTE: This upgrade procedure from steps 1-7 are valid for Access Manager Appliance deployed in a virtual environment only.

Prerequisite: Before upgrading the base operating system, perform the following task:

- If you have customized the `tomcat.conf` file or the `server.xml` file, back up these files before upgrading. These files will get overwritten during the upgrade process.

Perform the following steps to upgrade the base operating system SLES 11 SP4 to SLES 12 SP5:

1 Power off the virtual machine and insert the SLES 12 SP5 ISO.

2 Change the boot option to view the reboot screen in the BIOS setup utility.

3 Select **CD-ROM Drive** and click `[OS] SLE-12-SP5-Server-DVD-x86_64`.

4 On the **Options** tab, select the following:

- 5,000 milliseconds from **Power On Boot Delay**
- Select the following option:

```
The next time the virtual machine boots, force entry into the BIOS
setup screen.
```

5 Power on the virtual machine and move the **CD-ROM Drive** option to the top of the available list.

6 Click **Yes** in the **Save Configuration Changes and Exit?** dialog box to confirm.

The SUSE welcome page is displayed.

7 Select **Upgrade** from the following options:

- **Boot from Hard Disk**
- **Installation**
- **Upgrade**
- **more...**

The Linux kernel starts loading, and the upgrade process initializes.

8 On the **Language, keyboard, and License agreement** page, select the desired language, select the **I Agree to the License Terms** check box, and click **Next**.

The **Network Configuration** and **System Probing** processes begin. It is not mandatory to select the network setting in the **Network Configuration** page. You can skip this action.

9 Select **Partition or System to Update**. Click **OK** when the system displays the following warning message:

```
Some partitions in the system on /dxx/sxxx are mounted by kernel-device
name. This is not reliable for the update since kernel-device names are
unfortunately not persistent. It is strongly recommended to start the
old system and change the mount-by method to any other method for all
partitions.
```

10 The following **Previously Used Repositories** are removed from the system while upgrading:

NOTE: The messages are for reference only, they might change based on the environment.

Example 5-1 *Error Message Example*

Following sample repositories names are displayed:

- `NAM-APP-Updates`
- `NetIQAccessManagerAppliance-x.x.x.x-78`

11 Click **Next** when the system displays the following message:

```
Device is not configured. Press Edit to configure.
```

NOTE: You can ignore this message.

12 Click **No** when system displays the **Registration** screen with the following message:

```
Network is not configured, the registration server cannot be reached.
Do you want to configure the network now?
```

13 On the **Registration** page, select **Skip Registration** if you are not connected to the network. The system displays the following warning:

```
If you do not register to your system we will not be able to grant you
access to the update repositories. You can register after the
installation or visit our Customer Center for online registration.
```

14 Click **OK** > **Next**.

NOTE: If you skipped the registration process during the installation, you can register anytime using the software and the license from the Software License and Download portal.

15 On the **Installation Settings** page, click **Update**.

NOTE: Some products are marked for automatic removal, and the add-on products are listed.

If you get any errors on the **Installation Settings** page, perform the following steps:

15a Click **Packages**.

15b Search for `novell` to list all the novell RPMs.

15c Right-click the `novell-am-app-release` RPM, and select the **Protect, Do not Modify** option.

15d Select the Option 1 in **Conflict Resolution** that contains the following message:

```
remove lock to allow removal of product:Nxx_Axx-x.x.x.x86_64
```

15e Select the Option 3 in **Conflict Resolution** that contains the following message:

```
break product:Nxx_Axx-x.x-x.x86_64 by ignoring some of its
dependencies
```

16 Click **Okay - Try Again** to go back to the **Installation Settings** page.

17 **Accept** and **Continue** the installation.

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

```
You have successfully installed the required RPMs, and are ready to use
MySQL for the first time.
```

18 Click **OK** in the **Packages notifications** dialog box.

NOTE: The system automatically reboots after the operating system upgrade.

There is no change in the Access Manager Appliance upgrade process. Continue with Section 5.3, "Upgrading Access Manager Appliance," on page 42.

5.3 Upgrading Access Manager Appliance

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

1. If you are upgrading Access Manager, and want to use syslog for auditing, you must first upgrade the base operating system.
2. 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: Platform Agent and Novell Audit are no longer supported. Access Manager 4.2 onwards, the installation no longer installs Platform Agent and Novell Audit for auditing. If you upgrade from an older version of Access Manager to 4.5, Platform Agent is still available. It is recommended to use syslog for auditing. For more information about auditing, see Auditing in the NetIQ Access Manager Appliance 4.5 Administration Guide.

IMPORTANT: If you are using SQL database and you are upgrading to Access Manager 4.5, you must run a utility to re-factor the database. This is to ensure that Access Manager and its associated products use the same naming convention.

Perform the following steps to upgrade Access Manager Appliance.

1 Log in as the `root` user.

2 Download the `tar.gz` file of Access Manager Appliance from Software Licenses and Downloads and extract the `tar.gz` file using the following command:

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

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

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

```
./sb_upgrade.sh
```

4 The system displays the following confirmation message:

```
Would you like to continue this upgrade (y/n)? [y]:
```

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

5 Enter the Access Manager Administration Console user ID.

6 Enter the Access Manager Administration Console password.

7 Re-enter the password for verification.

8 The system displays the following confirmation message:

```
Do you want to back up the configuration before the upgrade (y/n)?
```

9 Type **Y** and press Enter.

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.
- If OAuth and OpenID Connect protocol is enabled, then after upgrading you must update Administration cluster to use the JSON Web Token (JWT token). For more information about JWT token, see Understanding How Access Manager Uses OAuth and OpenID Connect in the NetIQ Access Manager Appliance 4.5 Administration Guide.

NOTE: If you have enabled history for risk-based authentication in a prior version of Access Manager, you must upgrade the database for risk-based authentication after upgrading to 4.5. 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`

Microsoft SQL Server: Run `netiq_risk_sql_server_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.
```

6 Upgrading Analytics Server

It is recommended to use the latest Analytics Server shipped with Access Manager 4.5 Service Pack 3 HotFix 1. Upgrade to the latest Analytics Server is not supported from an earlier version. You must perform a fresh installation.

However, you can use the new Analytics Dashboard along with the earlier Sentinel-based Analytics Dashboard for events to be captured in both until all the data become available in the new dashboard. For this, you need to configure two target servers, one for the old and one for the new Analytics Dashboard. For more information, see "Setting Up Logging Server and Console Events" in the *NetIQ Access Manager Appliance 4.5 Administration Guide*.

You cannot launch the old Analytics Dashboard and reports from Administration Console. Instead, you can access the old data using the following direct access links:

- Dashboard: https://<Analytics IP>:8445/amdashboard/login
- Reports: https:// <Analytics IP>:8443/sentinel

IMPORTANT: Before installing the new Analytics Server, ensure to delete Analytics Server nodes of the earlier version from Administration Console.

7 Getting the Latest OpenSSL Updates for Access Manager Appliance

The OpenSSL open source project team regularly releases updates to known OpenSSL vulnerabilities. Access Manager Appliance and Analytics Server use the OpenSSL library for cryptographic functions. It is recommended that you keep Access Manager Appliance and Analytics Server 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 12 SP5. If you want to install the latest patches as they become available, you must have a user account to receive Linux updates.
- ❒ Ensure that you have obtained the activation code for Access Manager Appliance from Micro Focus Customer Center.

WARNING: Installing additional packages other than security updates and VMware tools breaks your support agreement. If you encounter a problem, Technical Support might require you to remove the additional packages and to reproduce the problem before providing any help with your problem.

7.1 Installing or Updating Security Patches for Access Manager Appliance and Analytics Server

Getting the latest security updates through Channel Update is not supported for the latest Analytics Server shipped with Access Manager 4.5 Service Pack 3 HotFix 1. The latest Analytics Server is available as a service and not as an appliance. For information about how to get the security patches for the earlier version of Analytics Server, see Getting the Latest Security Patches in the NetIQ Access Manager Appliance 4.4 Installation and Upgrade Guide.

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

7.1.1 Registering to Micro Focus Customer Center

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

1. Run the `registration_MCC.sh` script located at: `/opt/novell/channel`.
2. Enter a valid e-mail ID associated with the Micro Focus account and the activation code at the following prompt:

```
Please enter the following information to register your product. By
completing this simple registration, you will get immediate access to
online updates.
```

3 After you see the “Registration Successful” message, enter the following command to verify if the repository named `NAM453-APP-Updates` was created:

```
zypper lr
```

An output similar to the following appears:

Access Manager Appliance

```
# | Alias                                | Name
| Enabled | Refresh
--+--------------------------------------+----------------------------
-------
1 | SLES-12 SP5-12.5-0 | SLES-12 SP5-12.5-0
| Yes     | No
2 | nu_novell_com:NAM453-APP-Updates      | NAM453-APP-Updates
| Yes     | Yes
```

4 Run the `zypper up` command to install the patches.

5 After the patches are installed, restart the machine.

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

The details of new packages that will be installed are displayed.

7.1.2 Configuring Subscription Management Tool

You can register Access Manager Appliance to local Subscription Management Tool (SMT) server and download software updates from there instead of communicating directly with the Micro Focus 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.

- Section 7.1.2.1, “SMT Configuration,” on page 48
- Section 7.1.2.2, “Configuring Access Manager Appliance,” on page 49

7.1.2.1 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 12 SP5 server. For more information, see Subscription Management Tool (SMT) for SUSE Linux Enterprise 11.

2 Log in to you Micro Focus 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-12-x86_64` repository is displayed in the **Repositories** tab.

7 Select `sle-12-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.

7.1.2.2 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.

III

Troubleshooting Installation and Upgrade

This section includes the following topics:

8 Troubleshooting Installation

8.1 Checking the Installation Logs

If Access Manager Appliance installation fails, check the installation logs for warning and error messages.

The installation logs are located in the `/tmp/novell_access_manager` directory. The following is the list of useful log files:

Log File	Description
`install_main_2011-06-06_17:28:19.log`	Contains messages generated for installing and configuring Access Manager Appliance.
`iinstall_edir_2011-06-06_17:38:35.log`	Contains messages generated for installing and configuring Administration Console configuration store.
`install_audit_2011-06-06_17:38:35.log`	Contains messages generated for installing and configuring NetIQ Auditing components.
`Novell_iManager_2.7_InstallLog.log`	Contains messages generated for installing and configuring iManager.
`install_iman_2011-06-06_17:38:35.log`	Contains messages generated for installing and configuring iManager.
`install_adminconsole_2011-06-06_17:38:35.log`	Contains messages generated for installing and configuring Administration Console.
`install_jcc_2011-06-06_17:38:36.log`	Contains messages generated for installing and configuring the Communications module.
`install_mag_2011-06-06_17:38:37.log`	Contains messages generated for installing and configuring Access Gateway.
`install_idp_2011-06-06_17:38:36.log`	Contains messages generated for installing and configuring Identity Server.

Log File	Description
`configure_cluster_2011-06-06_17:28:19.log`	Contains messages generated for configuring Identity Server and Access Gateway.

8.2 Some of the New Hardware Drivers or Network Cards Are Not Detected during Installation

Access Manager Appliance installation might fail if some of the hardware drivers or network cards are not detected. If this happens, you must upgrade the hardware drivers manually as follows:

1. Start the Access Manager Appliance installation.

   See Chapter 2, “Installing Access Manager Appliance,” on page 23.
2. Select **Kernel Module (Hardware Driver)** in the main menu, then click **OK**.
3. Select **Add Driver Update**, then click **OK**.
4. Select the driver update medium.

   The driver update medium can be CD-ROM or floppy disk.
5. Click **OK** and continue with the installation.

8.3 Installation Through Terminal Mode Is Not Supported

Installation through terminal mode is supported on the GUI mode only. To resolve this issue, initiate the installation in the GUI mode. After entering the required input, switch to the terminal mode.

8.4 Access Manager Appliance Installation Fails Due to an XML Parser Error

This error may happen if the Appliance is installed by using a remotely mounted installer. Use a locally mounted installer to avoid this issue.

8.5 DN Is Added as Provider ID While Installing the NMAS SAML Method

While installing the NMAS SAML method in an external user store, DN is added as a provider ID instead of the metadata URL.

To resolve this issue, perform the following steps:

1. Log in to Administration Console which has the external user store.
2. Go to **Roles and Tasks** > **NMAS** > **NMAS Login Methods** > **SAML Assertion** > **Affiliates**.
3. Select the respective affiliate and change the provider ID to the identity provider metadata URL. For example, https://www.trunk2.com:8443/nidp/idff/metadata.

8.6 Rsyslog Fails to Start After Access Manager Installation

Scenario:

Installing the Access Manager installs the updated version of rsyslog and its dependencies. In some cases, the dependencies may not be updated to the latest version as compared to rsyslog. This results in failure to start rsyslog.

Workaround:

Update the ryslog dependency, `libfastjson` to the latest version using `zypper` or `yum` depending on RHEL or SUSE respectively.

NOTE: Updating the Operating System may also result in failure to start rsyslog.

9 Troubleshooting Upgrade

9.1 Access Gateway Throws a 403 Forbidden Page Error for a Resource Protected by a Form Fill Policy

This issue happens if a web server returns a form with a HTTP 403 error code. Access Gateway, by default, returns its own custom error pages. Hence, this prevents the Form Fill feature to work.

To workaround, perform the following steps:

1. Click **Devices** > **Access Gateways** > **Edit** > **Advanced Options**.
2. Specify `ProxyErrorOverride off`.
3. Click **OK**.

9.2 Access Gateway Displays an Error After the Base Operating System Upgrade

The error message is displayed after upgrading the base operating system from SLES 11 SP4 to SLES 12 SP5 and before upgrading Access Manager Appliance using the `sb_upgrade.sh` script. The instance of error log present in `rcnovell-apache2.out` is because of the `novell-apache2` service from the previous SLES11S4 Access Manager Appliance which tries to run on the upgraded SLES12SP5 operating system. After upgrading Access Manager Appliance if you run the `sb_upgrade.sh` script, this error no longer appears.

Check the status of the `novell-apache2` service if you see the following error in `/var/log/novell-apache2/rcnovell-apache2.out`:

```
httpd: Syntax error on line 559 of /etc/opt/novell/apache2/conf/httpd.conf:
Syntax error on line 15 of /etc/opt/novell/ag/ag_hook.conf: Cannot load /
usr/lib64/liblog4cxx.so.10 into server: libdb-4.5.so: cannot open shared
object file: No such file or directory
```

Use the `service novell-apache2 status` command to check the status.

If the status of the `novell-apache2` service is active and httpd server processes are running, ignore this error.

If the status of the `novell-apache2` service is down, check the `liblog4cxx.so` library for any missing dependency. Use the following commands:

- `~# export LD_LIBRARY_PATH="/opt/novell/ssllib:/opt/novell/openssl/lib"`
- `~# ldd /usr/lib64/liblog4cxx.so.10`

9.3 Issue in SSL Communication between Access Gateway and Web Applications

After upgrading Access Manager, applications are not accessible. This issue happens when any discrepancy exists between cipher suites configured for Access Gateway and applications protected by this Access Gateway.

To workaround this issue, see TID 7016872 (https://www.novell.com/support/kb/doc.php?id=7016872).

9.4 Customized Login Pages Are Missing After Upgrading Access Manager

After upgrading Access Manager, you cannot view the customized login JSP pages. This happens when the customized JSP files are not restored or the `legacy` filesystem directory is not created.

To resolve this issue, see Maintaining Customized JSP Files for Identity Server.

9.5 The Email OTP JSP Page Does Not Render Properly on Internet Explorer 11

This issue occurs when the Identity Server domain is added to the local Intranet or when the compatibility mode is enabled.

To workaround this issue, add the following entry to the `nidp_latest.jsp` page:

`response.setHeader("X-UA-Compatible","IE=edge");` after the first `<%`.

You can locate the `nidp_latest.jsp` file in the following path:

Linux: `/opt/novell/nids/lib/webapp/jsp`

Windows: `C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp`

Example, add `response.setHeader("X-UA-Compatible","IE=edge");` after

```
<%
    final String NIDP_JSP_CONTENT_DIV_ID = "theNidpContent";
```

For more information, see TID 7022722 (https://www.novell.com/support/kb/doc.php?id=7022722).

9.6 X509 Authentication Does Not Work and Throws HTTP 500 Error After Upgrade

This issue occurs in a dual identity server cluster configuration. After upgrading Access Manager, X509 authentication fails because the `context.xml` file gets overwritten and some configurations get deleted.

To workaround this issue, perform the following steps:

1. Before upgrading Access Manager, back up the `/opt/novell/nam/idp/webapps/nidp/META-INF/context.xml` file, if you have customized the `context.xml` file.
2. After upgrading Access Manager, add the customized content to the upgraded `context.xml` file and uncomment the following lines in the `context.xml` file:

   ```
   <!-- Force use the old Cookie processor (because this new tomcat version uses RFC6265 Cookie Specification) -->
   <!-- <CookieProcessor className="org.apache.tomcat.util.http.LegacyCookieProcessor" /> --> </Context>
   ```

9.7 Changes Required in server.xml for Apache Tomcat 8.5.51 after Upgrading to Access Manager 4.5 Service Pack 2

Access Manager 4.5 Service Pack 2 (4.5.2) adds support for Apache Tomcat 8.5.51. This version adds a secret required attribute to the Apache JServ Protocol (AJP) Connector. For fresh Access Manager installations, this string is specified in the `server.xml` file as `secret=` *"namnetiq"* by default. You do not need to make any change to `server.xml` in this regard.

However, the Tomcat service might not get loaded if you upgrade an existing Access Manager setup to 4.5.2 and Tomcat to version 8.5.51. You might see the following error in the `Tomcat catalina.log` file:

```
SEVERE [main] org.apache.catalina.core.StandardService.startInternal
Failed to start connector [Connector[AJP/1.3-8009]]
    org.apache.catalina.LifecycleException: Protocol handler start failed
          Caused by: java.lang.IllegalArgumentException: The AJP Connector
is configured with secretRequired="true" but the secret attribute is either
null or "". This combination is not valid.
'
```

To workaround this issue, after upgrading Tomcat to version 8.5.51, perform the following steps:

1. Open the `server.xml` file. This file is located in the following path:

Linux: `/opt/novell/nam/mag/conf/server.xml`

2 Add the `secret required` attribute. Set it to *true* by specifying a a non-null or non-zero length string.

NOTE: The value of this `secret required` attribute must be same in `server.xml` files of each component.

For example:

Embedded Service Provider configuration:

Linux: `/opt/novell/nam/mag/conf/server.xml`

```
/opt/novell/nam/mag/conf/server.xml <Connector port="9009"
enableLookups="false" redirectPort="8443" protocol="AJP/1.3"
address="127.0.0.1" minSpareThreads="25" maxThreads="600" backlog="0"
connectionTimeout="20000" packetSize="65536" maxPostSize="65536"
secret="namnetiq" />^M
```

Access Manager Appliance:

Linux: `/opt/novell/nam/idp/conf/server.xml`

```
/opt/novell/nam/idp/conf/server.xml -->^M <Connector port="9019"
enableLookups="false" secure="true" scheme="https"
protocol="com.novell.nam.tomcat.ajp.NAMAjpNIOProtocol"
address="127.0.0.1" minSpareThreads="25" maxThreads="600" backlog="0"
connectionTimeout="20000" packetSize="65536" maxPostSize="2097152"
secret="namnetiq" />^M
```

3 Save the file and restart the Apache Tomcat Service.

The following are examples of `Apache vhost.d/`*snippets:

Path: `/opt/novell/nam/mag/webapps/agm/WEB-INF/config/apache2/vhosts.d/NAM-Service.conf`

```
ProxyPass /AGLogout ajp://127.0.0.1:9009/nesp/app/plogout secret=namnetiq

ProxyPass /nidp/nidpsecure ajp://127.0.0.1:9019/nidp secret=namnetiq

ProxyPass /nidp ajp://127.0.0.1:9019/nidp secret=namnetiq

ProxyPass /nesp ajp://127.0.0.1:9009/nesp secret=namnetiq
```

Embedded Service Provider configuration:

Path: `/opt/novell/nam/mag/webapps/agm/WEB-INF/config/apache2/vhosts.d/soapbc.conf`

```
ProxyPass /AGLogout ajp://127.0.0.1:9009/nesp/app/plogout secret=namnetiq
ProxyPass /nesp ajp://127.0.0.1:9009/nesp secret=namnetiq
```

9.8 Rsyslog Fails to Start After Access Manager Upgrade

Scenario:

Upgrading the Access Manager upgrades rsyslog and its dependencies. In some cases, the dependencies may not be updated to the latest version as compared to rsyslog. This results in failure to start rsyslog.

Workaround:

Update the ryslog dependency, `libfastjson` to the latest version using `zypper` or `yum` depending on RHEL or SUSE respectively.

NOTE: Updating the Operating System may also result in failure to start rsyslog.

IV Appendix

This section includes the following topics:

- Appendix A, “Configuring Ports 9000 and 9001 to Listen on the Specified Address,” on page 65
- Appendix B, “Denormalizing SQL Database,” on page 67

A Configuring Ports 9000 and 9001 to Listen on the Specified Address

ports 9000 and 9001 listen on 127.0.0.1 by default. Access Manager Appliance uses these ports for scheduling jobs. If you encounter any issue because of these ports listening on 127.0.0.1, such as issue with IPv6 connectivity, you can specify a different address by using the following Java option in the `tomcat8.conf` file:

```
/opt/novell/nam/adminconsole/conf/tomcat8.conf
```

```
"com.microfocus.nam.adminconsole.localhost.ipaddress"
```

For example:

```
JAVA_OPTS="${JAVA_OPTS} -
Dcom.microfocus.nam.adminconsole.localhost.ipaddress=10.0.0.0"
```

Denormalizing SQL Database

IMPORTANT: You must perform this task only if you are upgrading to Access Manager 4.5 Service Pack 2 (SP2) or later from an older version and your database contains the Risk Based Authentication (RBA) data.

From Access Manger 4.5 SP2, a one-to-one data model is used to store the device information for RBA in SQL database. The older versions of Access Manager uses the many-to-one data model to provide the storage benefits of data normalization. The many-to-one data model can cause performance issues in some versions of SQL database when the system is under heavy load.

If you are upgrading to Access Manager SP2 with existing RBA data in database, you must denormalize the existing data. To denormalize your database, you must run a jar utility supplied along with Access Manager 4.5 SP2. If you do not run this utility, the existing user data can become irrelevant in RBA and may not be used for Risk Score calculation.

Refer the following points to know how this utility works:

- It runs outside Access Manager as a separate JAR utility.
- It runs on a configuration file and the configuration file is bundled with JAR.
- It uses hibernate and native SQL queries to modify the database entries.

Perform the following steps to denormalize your database:

IMPORTANT: ◆It is recommended to back up your database before you run the utility.

- Make sure that enough Java heap space is available before you run the utility.
- Provide appropriate hibernate connector JARs in classpath.

1 Log in to Administrator Console of Access Manager.

2 Click **Policies > Risk-based policies > User history**. Make a note of the following information provided on this page:

   1. Database Driver
   2. Database Dialect
   3. Username
   4. Password
   5. URL

3 Extract the utility JAR (`RBA_SQL_Cleanup_Util.zip`) outside Identity Server folders.

   NOTE: If you want to use c3p0 connection pool libraries to optimize the database connection usage while running the utility, you must place the c3p0 JAR files in the same location where the utility JAR is extracted. Specify the c3p0 properties in the configuration file in the following format:

   ```
   <key=value>
   ```

Download the following c3p0 connection pool libraries from Maven Repository (https://mvnrepository.com/):

- c3p0-0.9.2.1.jar (https://mvnrepository.com/artifact/com.mchange/c3p0/0.9.2.1)
- hibernate-c3p0-4.3.6.Final.jar (https://mvnrepository.com/artifact/org.hibernate/hibernate-c3p0/4.3.6.Final)
- mchange-commons-java-0.2.3.4.jar (https://mvnrepository.com/artifact/com.mchange/mchange-commons-java/0.2.3.4)

4 Open the `config.properties` file that you extracted from utility JAR.

5 Specify the details that you noted in Step 2 in `config.properties` file:

For example, see the following information to understand what information is specified in `config.properties` file:

```
hibernate.connection.url=<URL>
hibernate.connection.username=<Username>
hibernate.connection.password=<Password>
hibernate.dialect=<Database Dialect>
hibernate.connection.driver_class=<Database Driver>
```

6 Run command line or terminal as an administrator.

7 Run the following java command to run the utility:

```
java -cp '<directory path where the zip is extracted>/*'
com.novell.nam.nidp.risk.sql.cleanup.SQLApp
<directory path where the zip is extracted>/config.properties
<directory to save log files> denormalization_01
```

IMPORTANT: Make sure that you specify absolute paths in classpath and arguments to avoid platform specific issues.

8 Open the log files to check for errors, if occurred.

B