Access Manager 4.5
Installation and Upgrade Guide

April 2019

Legal Notice

Contents

About this Book and the Library

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

Intended Audience

This book is intended for Access Manager administrators. It is assumed that you have knowledge of evolving Internet protocols, such as:

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

Other Information in the Library

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

- Access Manager Product Documentation (https://www.netiq.com/documentation/access-manager/index.html)
- 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 13.

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

Figure 1-1 *Typical Deployment of Access Manager*

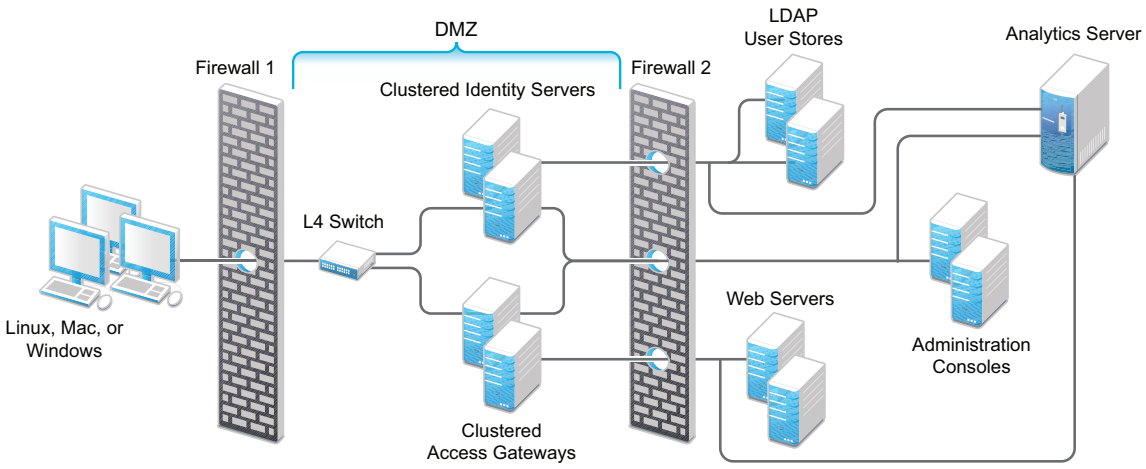
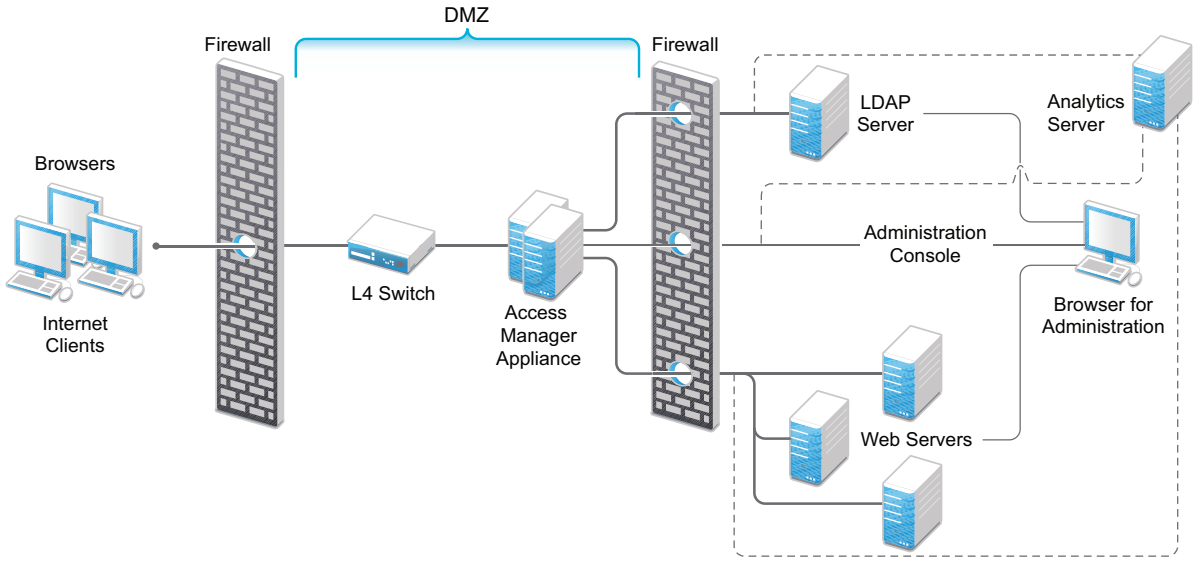


Figure 1-2 *Typical Deployment of Access Manager Appliance*



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*

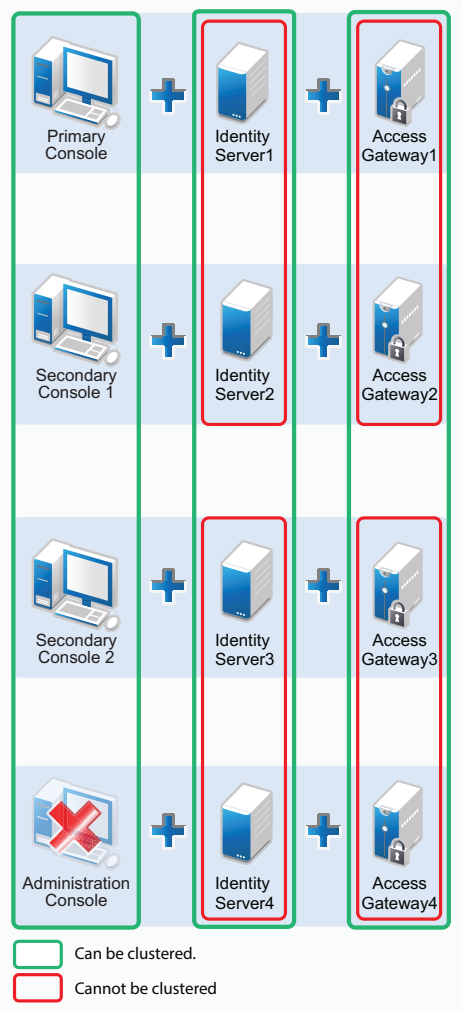
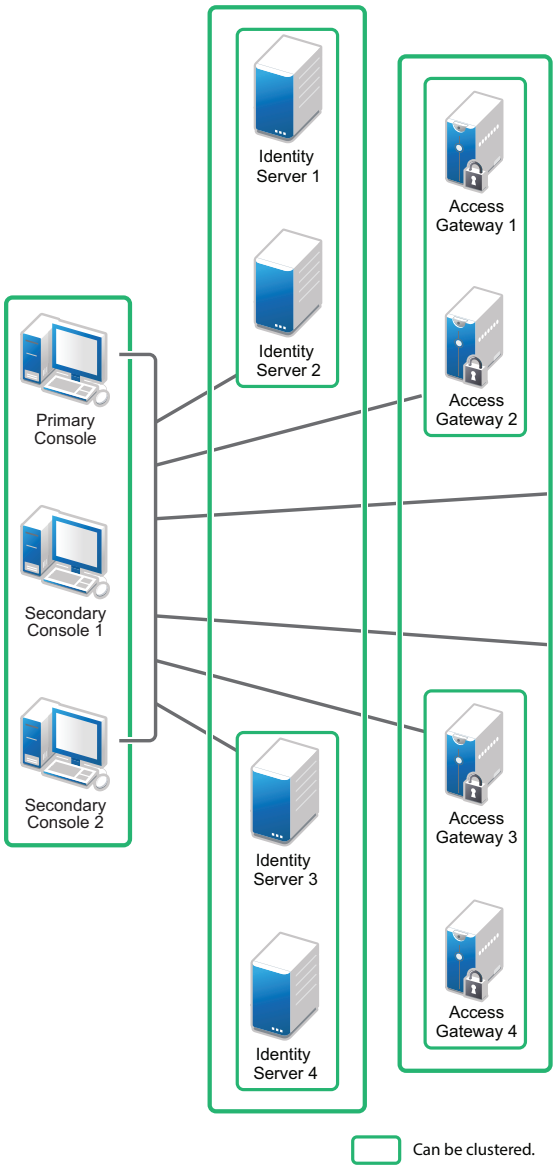


Figure 1-4 *Access Manager Cluster*



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 Devices in the Access Manager 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 machine used for Access Manager components. If the IP address of the machine changes, Access Manager components installed on that machine will not start.
- A domain name server, which resolves DNS names to IP addresses and which has reverse lookups enabled.

  Access Manager devices know each other by their IP addresses, and some requests require them to match an IP address with the device's DNS name. Without reverse lookups enabled, these requests fail. In particular, Identity Servers perform reverse lookups to their user stores. If reverse lookups are not available, host table entries can be used.
- 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 Recommended Installation Scenarios

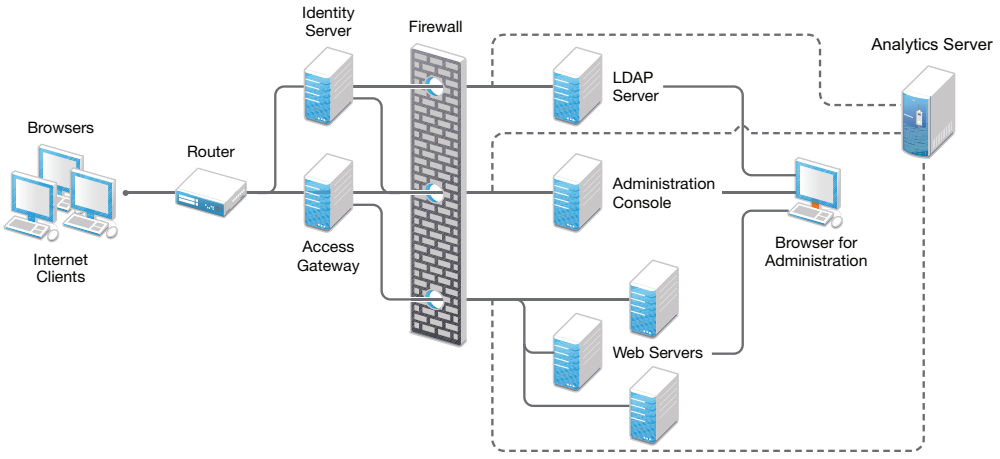
The following scenarios provide an overview of the flexibility built into Access Manager. Use them to design a deployment strategy that fits the needs of your company.

- Section 1.5.1, “Basic Setup,” on page 19
- Section 1.5.2, “High Availability Configuration with Load Balancing,” on page 20

1.5.1 Basic Setup

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

Figure 1-5 *Basic Installation Configuration*



1 Install Administration Console.

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

2 If firewall is set up, open the ports required for Identity Server and Access Gateway to communicate with Administration Console:

TCP 1443, TCP 8444, TCP 1289, TCP 1290, TCP 524, TCP 636.

For more information about these ports, see Section 1.8, “Setting Up Firewalls,” on page 28.

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

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

4 Install Access Gateway.

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

5 Install Analytics Server.

Log in to Administration Console to verify that Analytics Server is imported successfully.

6 Configure Identity Server, Analytics Server, and Access Gateway. See Configuring Access Manager in the Access Manager 4.5 Administration Guide.

In this configuration, the LDAP server is separated from Identity Server by firewall. Ensure that you open the required ports. See Section 1.8, “Setting Up Firewalls,” on page 28.

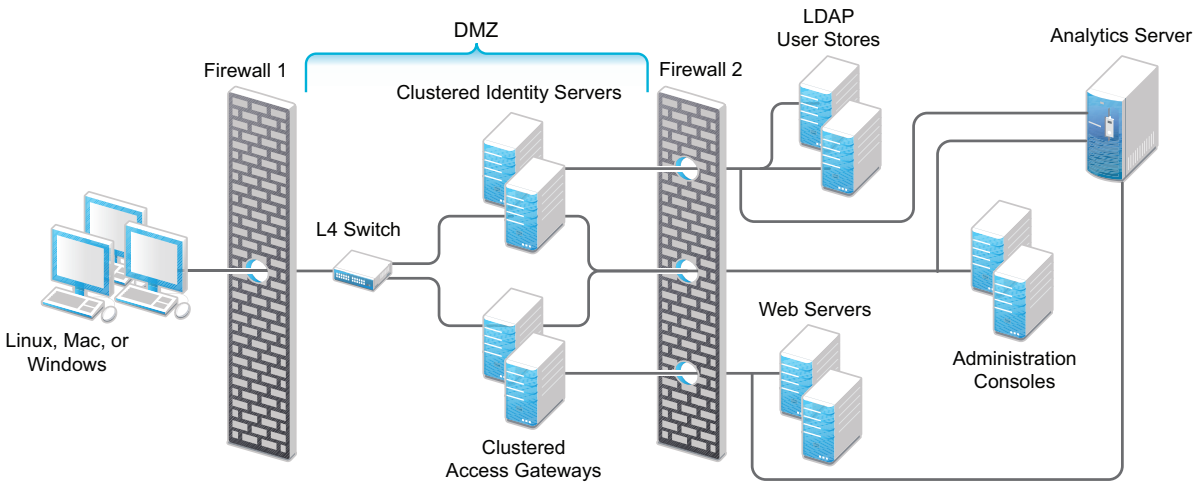
For information about setting up configurations for fault tolerance and clustering, see High Availability and Fault Tolerance in the Access Manager 4.5 Administration Guide.

Firewall protects the LDAP server and Administration Console, both of which contain a permanent store of sensitive data. Web servers are installed behind the firewall for added protection. Identity Server does not permanently store any user data. This is the recommended configuration. This configuration also supports an L4 switch in place of a router to support clusters of Identity Servers and Access Gateways.

1.5.2 High Availability Configuration with Load Balancing

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

Figure 1-6 *Clustering Configuration for High Availability*



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

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

1.6 Deploying Access Manager on Public Cloud

The following list provides the recommended configuration details for deploying Access Manager on Amazon Web Services (AWS) EC2 and Microsoft Azure:

- Install the LDAP server and Administration Console in the private subnet. Both of these contain a permanent store of sensitive data. Install web servers also in the private subnet for added protection.

  In the private subnet, servers do not have any public IP address. This prevents the servers from security vulnerabilities. However, the servers on the public subnet can have public IP addresses.
- You cannot access Administration Console directly in the private subnet. Therefore, it is recommended to configure a dedicated server called as jump server in the public subnet. You can then use the jump server to access Administration Console. You can use a Windows server as a jump server and Remote Desktop Protocol to access the jump server.

  For more information about jump servers, see Linux Bastion Host Quick Start (https://docs.aws.amazon.com/quickstart/latest/linux-bastion/architecture.html).
- The cloud-based service provider routes communications among servers on the public subnet and servers on the private subnet.
- Install Identity Server in the public subnet because it does not permanently store any sensitive user data.

This configuration has been tested with a load balancer to support clusters of Identity Servers and Access Gateways. As the number of users and demands for web resources increase, you can easily add another Identity Server or Access Gateway to handle the load. You can then add the new servers to the load balancer. When the new servers are added to the cluster, they are automatically sent the cluster configuration. See Appendix B, “Recommendations for Scaling Access Manager Components in Public Cloud,” on page 183.

The following sections provide information specific to AWS EC2 and Microsoft Azure:

- Section 1.6.1, “Deploying on AWS EC2,” on page 21
- Section 1.6.2, “Deploying on Microsoft Azure,” on page 22

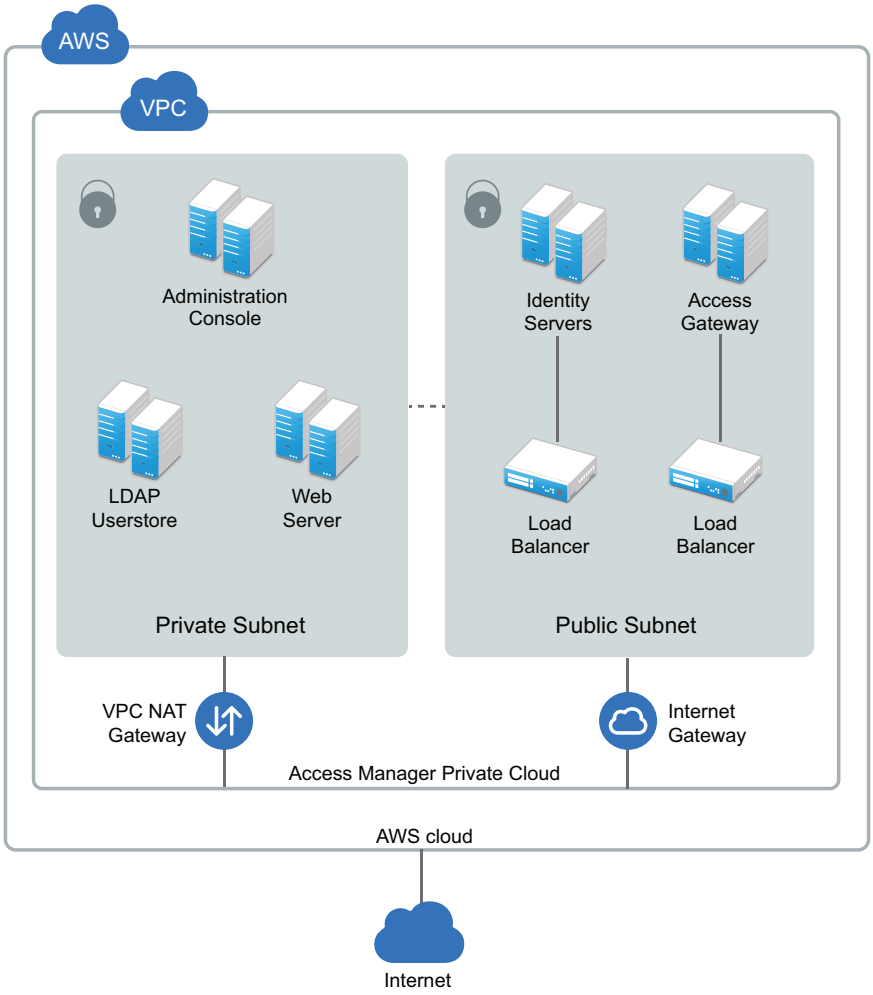
1.6.1 Deploying on AWS EC2

You need to configure a VPC NAT gateway. Servers in the private subnet use VPC NAT gateway to access the Internet. Similarly, you need to configure an Internet gateway for enabling servers in the public subnet to access Internet and vice versa. For more information, see the Amazon Virtual Private Cloud Documentation (https://aws.amazon.com/documentation/vpc/).

For more information about AWS EC2 VPC, see Amazon Virtual Private Cloud Documentation (https://aws.amazon.com/documentation/vpc/).

For information about how to deploy Access Manager on AWS EC2, see Chapter 6, “Deploying Access Manager on Amazon Web Services EC2,” on page 85.

Figure 1-7 *Access Manager Deployment on AWS EC2*



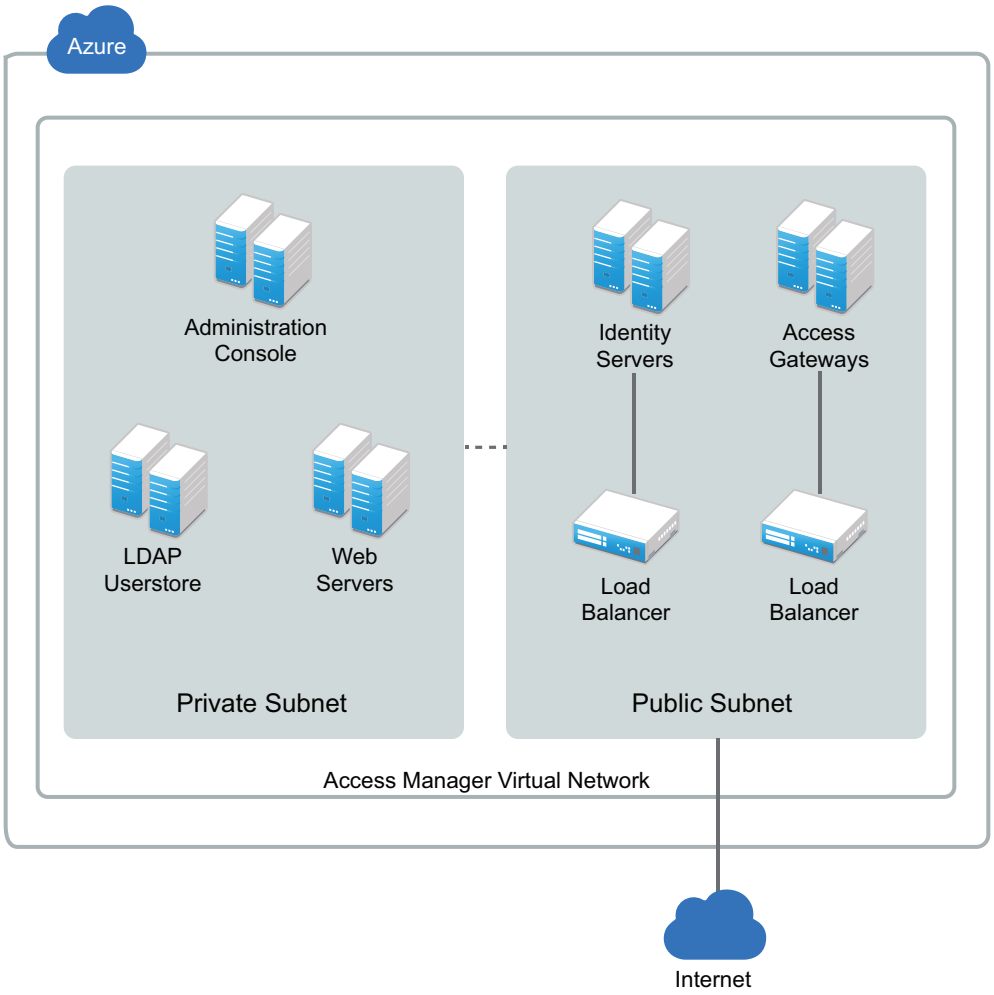
1.6.2 Deploying on Microsoft Azure

In Microsoft Azure, you do not need to configure a VPC NAT gateway and Internet gateway. Azure takes care of this configuration.

For more information about the Azure virtual network, see Virtual Network Documentation (https://docs.microsoft.com/en-in/azure/virtual-network/).

For information about how to deploy Access Manager on Azure, see “Deploying Access Manager on Microsoft Azure” on page 97.

Figure 1-8 *Access Manager deployment on Microsoft Azure*



1.7 Installing Access Manager Components in NAT Environments

You can deploy Access Manager components in a multi-tenant or service provider environment, where Network Address Translation (NAT) protocol is used as one of the network configuration.

This section includes the following topics:

- Section 1.7.1, “Network Prerequisites,” on page 24
- Section 1.7.2, “Network Setup Flow Chart,” on page 25
- Section 1.7.3, “Installing Access Manager Components in NAT Environments,” on page 25
- Section 1.7.4, “Configuring Network Address Translation,” on page 27

1.7.1 Network Prerequisites

Service Provider Network Setup

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

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

- ❒ An L4 switch if you need to configure load balancing. This can be hardware or software (for example, a Linux machine running Linux Virtual Services).
- ❒ IP connectivity is established between different Access Manager components. Because the components can be in different private networks, you can use NAT, VPNs, or combination of both to achieve connectivity.

Customer Network Setup

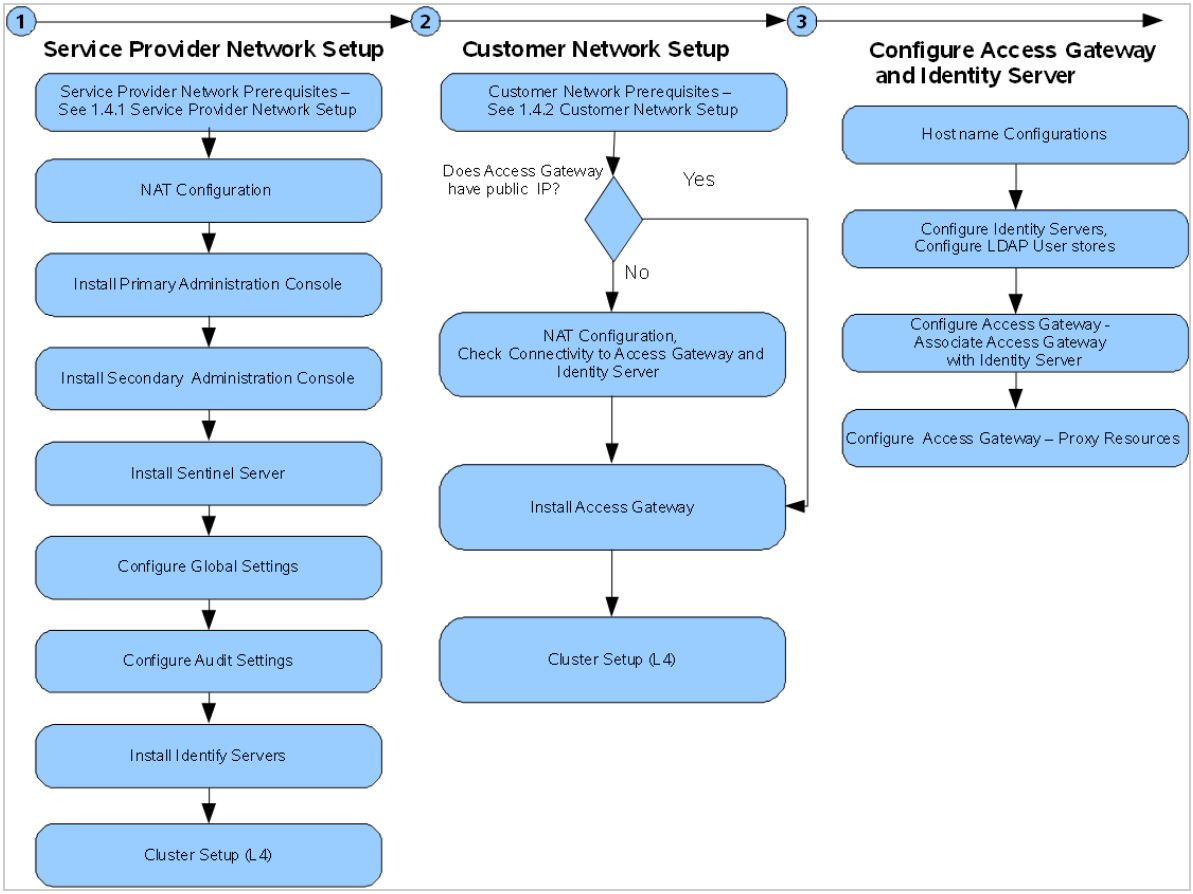
- ❒ A server configured with an LDAP directory (eDirectory 8.8.8.8 or later, Sun ONE, or Active Directory) that contains your system users. Identity Server uses the LDAP directory to authenticate users to the system.
- ❒ Domain name server, which resolves DNS names to IP addresses and which has reverse lookups enabled.

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

1.7.2 Network Setup Flow Chart

Figure 1-9 provides the setup information about installing Access Manager components and configuring NAT in a multi-tenant or service provider network.

Figure 1-9 *Network Setup Flow Chart*



1.7.3 Installing Access Manager Components in NAT Environments

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

1. “Installing Administration Console” on page 25.
2. “Configuring Global Settings” on page 26
3. “Installing Identity Server” on page 55
4. “Installing Access Gateway” on page 67

1.7.3.1 Installing Administration Console

For installation requirements, see “Installing Administration Console” on page 43.

1 Before installing Access Manager components, check the network connectivity across these machines.

2 Verify the link latency and ensure that it is less than 100 milliseconds.

If the link latency is greater than 100ms, it might lead to performance degradation.

3 Synchronize time across all Access Manager components.

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

3a 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).

3b Run the following commands on the primary Administration Console to start the NTP server:

```
systemctl start ntpd
systemctl enable ntpd
```

3c 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.

---

4 Install the primary Administration Consoles by providing the listening IP address for the primary Administration Console.

For more information about installing Administration Console, see the "Installing Administration Console on Windows" on page 49.

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

6 Continue with Section 1.7.3.2, "Configuring Global Settings," on page 26 to add both the primary and secondary Administration Consoles to the **Global Settings** configuration.

1.7.3.2 Configuring Global Settings

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

1 Log in to Administration Console.

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

3 Click **New**.

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

5 Specify the corresponding Public NAT IP address.

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

```
IP Address is not valid
```

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

1.7.3.3 Installing and Configuring Identity Server

For information about how to install Identity Server, see "Installing Identity Server" on page 55.

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

For information about how to configure Identity Server, see Configuring Identity Servers Clusters in the Access Manager 4.5 Administration Guide.

1.7.3.4 Installing and Configuring Access Gateway

For information about how to install Access Gateway, see "Installing Access Gateway" on page 67.

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

For information about configuring Access Gateway, see Configuring Access Gateway in the Access Manager 4.5 Administration Guide.

1.7.4 Configuring Network Address Translation

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

See your router documentation for more information.

1.7.4.1 Configuring Administration Console Behind NAT

1. Log in to Administration Console.
2. Go to **Access Manager** > **Global Settings**, then click **New**.
3. Select an IP address from the **Administration Console Public IP Address** list.

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

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

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

For more information about configuring NAT, see Mapping the Private IP Address to Public IP Address in the Access Manager 4.5 Administration Guide.

1.7.4.2 Configuring Identity Server and Access Gateway Behind NAT

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

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

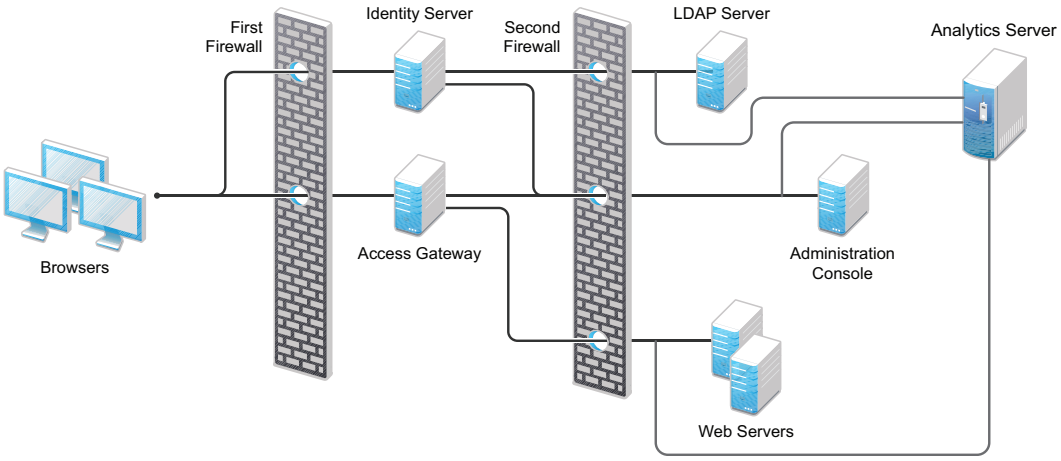
Enter `Y` and specify the NAT address. This enables Administration Console to use this NAT address when communicating to this device.

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

1.8 Setting Up Firewalls

It is recommended to use Access Manager with firewalls. Figure 1-10 illustrates a simple firewall setup for a basic Access Manager configuration of an Identity Server, an Access Gateway, and an Administration Console. This is one of many possible configurations.

Figure 1-10 *Access Manager Components between Firewalls*



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

This section describes the following topics:

- Section 1.8.1, “Required Ports,” on page 29
- Section 1.8.3, “Sample Configurations,” on page 36

1.8.1 Required Ports

List of Tables

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

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

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

Component	Port	Description
Access Gateway, Identity Server	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. Open this port so that both the device and Administration Console can use the port.
	TCP 636	For secure LDAP communication from devices to Administration Console.
	HTTP 2443 HTTP 8443	For the installer to communicate with Administration Console. You can close these port after installation is complete.
Importing an Access Gateway Appliance	ICMP	During an import, Access Gateway Appliance sends two pings through ICMP to Administration Console. When the import has finished, you can disable the ICMP echo requests and echo replies.
LDAP User Store	TCP 524	Required only if the user store is eDirectory. When configuring a new eDirectory user store, NCP is used to enable Novell SecretStore by adding a SAML authentication method and storing a public key for Administration Console. It is not used in day-to-day operations.
	TCP 636	For secure LDAP communication from Administration Console to user store.
Administration Console	TCP 524	Required to synchronize the configuration data store.
	TCP 636	Required for the secure LDAP communication.
	TCP 8080, 8443	Used for the Tomcat communication.
	TCP 705	Used by Sub Agent-Master Agent communication inside Administration Console.
	UDP 161	Used for communication by an external Network Monitoring System with Administration Console by using SNMP.
Browsers	TCP 8080	For HTTP communication from browsers to Administration Console.
	TCP 8443, 2443, 2080.	For HTTPS communication from browsers to Administration Console. **NOTE:** 2443 and 2080 are optional ports required when Administration Console and Identity Server are collocated.
	TCP 8028, 8030	To use iMonitor or DSTrace from a client to view information about the configuration store on Administration Console.

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

Component	Port	Description
Access Gateway	TCP 8080 or 8443	For authentication communication from Access Gateway to Identity Server. The default ports for Identity Server are TCP 8080 and 8443. They are configurable. You need to open the port that you configured for the base URL of Identity Server.
	TCP 80 or 443	For communication from Identity Server to Access Gateway ESP. This is the reverse proxy port that is assigned to be ESP (see the Reverse Proxy /Authentication page). This is usually port 80 or 443.
Administration Console	TCP 1443	For communication from Administration Console to devices. This is configurable.
	TCP 8444	For communication from Identity Server to Administration Console.
	TCP 1290	For communication from devices to the Syslog server on Administration Console.
	TCP 524	For NCP certificate management with NPKI from Identity Server to Administration Console.
	TCP 636	For the secure LDAP communication from Identity Server to Administration Console.
Identity Server	TCP 8443 or 443	For HTTPS communication. You can use iptables to configure this for TCP 443. See Translating Identity Server Configuration Port.
	TCP 7801	For back-channel communication with cluster members. You must enable the multicast traffic on this port. This port is configurable.
LDAP User Stores	TCP 636	For secure LDAP communication from Identity Server to the LDAP user store.
Service Providers	TCP 8445	If you have enabled identity provider introductions, open a port to allow HTTPS communication from the user's browser to the service provider.
	TCP 8446	If you have enabled identity provider introductions, open a port to allow HTTPS communication from the user's browser to the service consumer.
Browsers	TCP 8080	For HTTP communication from a browser to Identity Server. You can use iptables to configure this for TCP 80. SeeSection 3.5, "Translating Identity Server Configuration Port," on page 60.
	TCP 8443	For HTTPS communication from a browser to Identity Server. You can use iptables to configure this for TCP 443. See Section 3.5, "Translating Identity Server Configuration Port," on page 60.
CRL and OCSP Servers	Configurable	If you are using x.509 certificates that include an AIA or CRL Distribution Point attribute, you need to open the port required to talk to that server. Ports 80/443 are the most common ports, but the LDAP ports 389/636 can also be used.

Component	Port	Description
Active Directory Server with Kerberos	TCP 88, UDP 88	For communication with KDC on the Active Directory Server for Kerberos authentication.

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

Component	Port	Description
Identity Server	TCP 8080 or 8443	For authentication communication from Access Gateway to Identity Server. The default ports are TCP 8080 and 8443, which are configurable. You need to open the port of the base URL of Identity Server.
	TCP 80 or 443	For communication from Identity Server to ESP of Access Gateway. This is the reverse proxy port that is assigned to be ESP (see the Reverse Proxy / Authentication page). This is usually port 80 or 443.
Administration Console	TCP 1443	For communication from Administration Console to Access Gateway. This is configurable.
	TCP 8444	For communication from Access Gateway to Administration Console.
	TCP 1290	For communication from devices to the Syslog server on Administration Console.
	TCP 524	For NCP certificate management with NPKI from Access Gateway to Administration Console.
	TCP 636	For secure LDAP communication from Access Gateway to Administration Console.
Access Gateway	TCP 7801	For back-channel communication with cluster members. You must enable the multicast traffic option on this port. This port is configurable. It is set by Identity Server cluster configuration that Access Gateway trusts. See Configuring a Cluster with Multiple Identity Servers in the Access Manager 4.5 Administration Guide.
	TCP 80 or 443	For communication among Embedded Service Providers (ESP) of the Access Gateway cluster members. This is the reverse proxy port that is assigned to be ESP (see the Reverse Proxy /Authentication page). This is usually port 80 or 443. This port is configurable.
Access Gateway Appliance Configuration console (`https://<access_gateway_appliance-IP address>:9443`)	TCP 9090 or 9443	For using the Jetty service on the appliance Configuration console. For more information about the Configuration console, see Configuring Access Gateway Appliance.
	TCP 1099	For the Java RMI communication.

Component	Port	Description
Browsers/ Clients	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.

Table 1-6 *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.

NOTE: On SLES, you can use YaST to configure UDP ports and internal networks.

Table 1-7, Table 1-8, and Table 1-9 are intended for use in configuring the security groups in cloud deployments. The security groups, by default, do not restrict the outbound ports. Therefore, these tables include only the inbound ports.

Table 1-7 *Administration Console on Cloud*

Component	Port	Traffic Direction	Description
Access Gateway, Identity Server	TCP 1290	Inbound	For communication from devices to the Syslog server on Administration Console.
	TCP 8443	Inbound	For the installer to communicate with Administration Console.
	TCP 8444	Inbound	For communication from devices to Administration Console.
	TCP 524	Inbound	For NCP certificate management with NPKI. Open this port so that both the device and Administration Console can use the port.
	TCP 636	Inbound	For secure LDAP communication from devices to Administration Console.
Access Gateway	TCP 1289	Inbound	For importing Access Gateway into Administration Console.
SSH	TCP 22	Inbound	For accessing Administration Console using SSH.
Access Gateway	ICMP	Inbound	For importing Access Gateway.

Table 1-8 *Identity Server on Cloud*

Component	Port	Traffic Direction	Description
Administration Console	TCP 1443	Inbound	For communication from Administration Console to devices. This is configurable.
	TCP 524	Inbound	For NCP certificate management with NPKI from Identity Server to Administration Console.
Identity Server	TCP 7801	Inbound	For the back-channel communication with cluster members. You must enable the multicast traffic option on this port. This port is configurable.
SSH	TCP 22	Inbound	For accessing Identity Server using SSH.
Access Gateway, Browsers	TCP 8443	Inbound	For authentication communication from Access Gateway to Identity Server. For HTTPS communication from a browser to Identity Server's base URL when the default ports are used.

Table 1-9 *Access Gateway on Cloud*

Component	Port	Traffic Direction	Description
Service Providers	TCP 8445	Inbound	If you have enabled identity provider introductions, open a port to allow HTTPS communication from the user's browser to the service provider.
	TCP 8446	Inbound	If you have enabled identity provider introductions, open a port to allow HTTPS communication from the user's browser to the service consumer.
Access Gateway	TCP 7801	Inbound	For back-channel communication with cluster members. You must enable the multicast traffic option on this port.
Administration Console	TCP 1443	Inbound	For communication from Administration Console to Access Gateway. This is configurable.
SSH	TCP 22	Inbound	For accessing Administration Console using SSH.
Identity Server	TCP 80 or 443	Inbound	For communication from Identity Server to Access Gateway ESP. This is the reverse proxy port that is assigned to be ESP.
Browsers/Clients	TCP 443	Inbound	For HTTPS communication from workstation browsers to Access Gateway.
	TCP 80	Inbound	For HTTP communication from workstation browsers to Access Gateway.

1.8.2 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.

1.8.3 Sample Configurations

- Section 1.8.3.1, “Access Gateway and Identity Server in DMZ,” on page 36
- Section 1.8.3.2, “A Firewall Separating Access Manager Components from the LDAP Servers,” on page 37

1.8.3.1 Access Gateway and Identity Server in DMZ

First Firewall

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

See, Figure 1-10 on page 28

Table 1-10 *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. For information about redirecting Identity Server to use port 80, see Translating Identity Server Configuration Port.
TCP 8443	For HTTPS communication with Identity Server. For information about redirecting Identity Server to use port 443, see Translating Identity Server Configuration Port.
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:

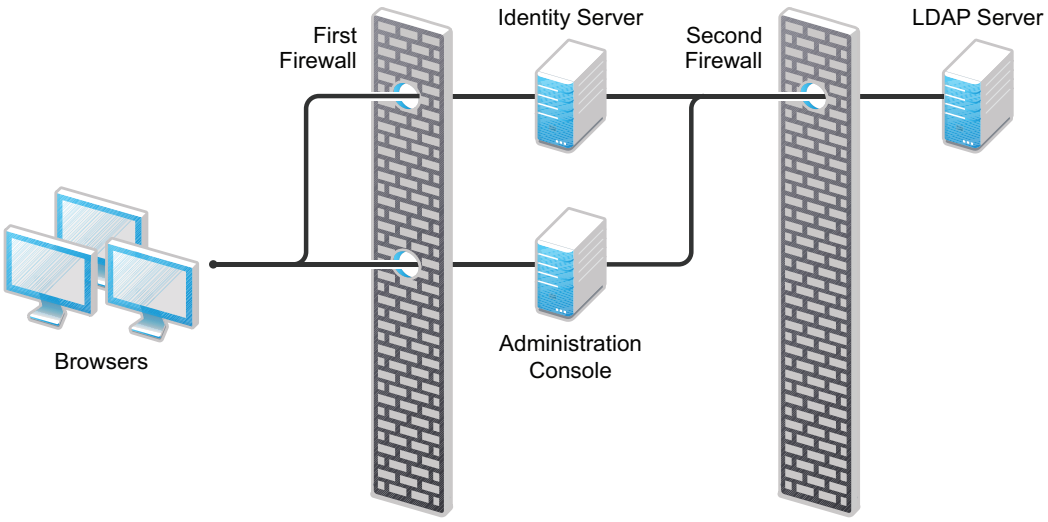
Table 1-11 *Ports to Open in the Second Firewall*

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 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.

1.8.3.2 A Firewall Separating Access Manager Components from the LDAP Servers

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

Figure 1-11 *A Firewall Separating Administration Console and the LDAP Server*



In this configuration, you need to open the following ports in the second firewall for Administration Console and Identity Server:

Table 1-12 *Ports to Open in the Second Firewall*

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

1.9 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

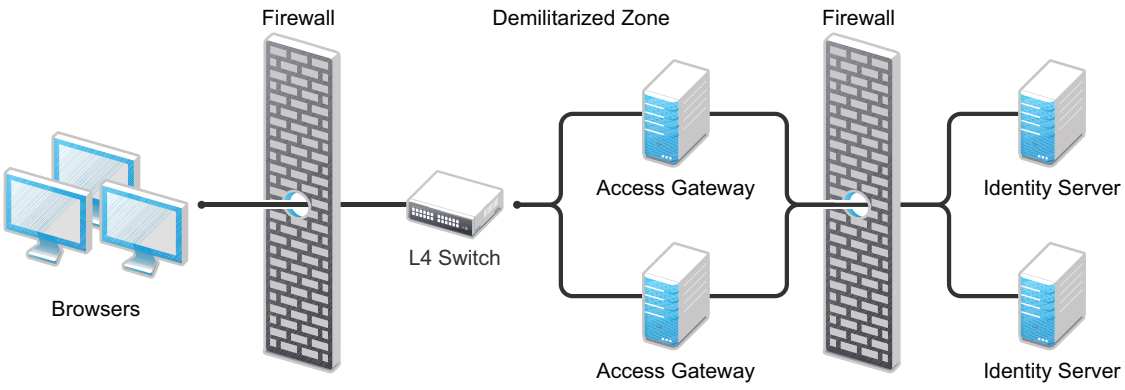
For strong security, it is recommended that you replace these certificates, except the test-stunnel certificate, with certificates from a well-known certificate authority.

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

1.10 Protecting an Identity Server Through Access Gateway

For security reasons, you might want to set up your Access Manager configuration so that Identity Server is a resource protected by an Access Gateway. This configuration reduces the number of ports you need to open between the outside world and your network. Figure 1-12 illustrates such a configuration.

Figure 1-12 *Identity Servers behind an Access Gateway*



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

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

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

For configuration details, see Configuring a Protected Identity Server Through Access Gateways in the Access Manager 4.5 Administration Guide.

Installing Access Manager

Before you start installation, evaluate how you want to implement Access Manager. You can install components on a single server (excluding Analytics Server) or on separate servers. For more information, see Chapter 1, “Planning Your Access Manager Environment,” on page 11.

The following is the sequence of installing Access Manager components:

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

This section includes the following topics:

2 Installing Administration Console

Administration Console must be installed before installing any other Access Manager devices. If iManager is installed for other products, you still need to install this version on a separate server. Administration Console is installed with an embedded version of eDirectory, which is used as the configuration store for Access Manager.

For a functioning system, you need Administration Console for configuration and management, Identity Server for authentication, and Access Gateway for protecting resources.

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

This chapter includes the following topics:

For information about installing a secondary Administration Console and fault tolerance, see Installing Secondary Administration Console in the Access Manager 4.5 Administration Guide.

2.1 Installing Administration Console on Linux

IMPORTANT: The eDirectory DIB within the Administration Console installation is not supported in a B-tree file system (BTRFS). If your Administration Console system uses BTRFS, create a separate mount point using XFS or ext4 that mounts automatically at `/var/opt/novell/eDirectory` to meet this requirement. For more information, see eDirectory documentation (https://www.netiq.com/documentation/edirectory-9/edir_install/data/a79kg0t.html).

2.1.1 Prerequisites for Installing Administration Console on Linux

❒ Ensure that the system meets the requirements for installing Administration Console.

For information about the requirements, see *NetIQ Access Manager System Requirements*.

❒ If you have custom partitioned your hard disk, ensure to allocate the minimum space for each partition as mentioned in the following table:

Partition	Minimum Disk Space
/opt/novell	1 GB
/opt/volera	5 MB
/var/opt/novell	1 GB
/var	512 MB
/usr	25 MB
/etc	1 MB
/tmp/novell_access_manager	10 MB
/tmp	10 MB
/	512 MB

NOTE: These are the minimum free disk spaces that must be available before installation or upgrade. However, it is recommended to maintain more than the specified free disk space based on the requirement of your production environment.

You can perform the disk partitioning based on your requirement.

For example, consider a scenario where an administrator is installing Access Manager with 100 GB disk space. The administrator wants to allocate enough space for the logs from the available space. Therefore, the administrator can partition the hard disk as follows:

Partition	Disk Space
/opt	5 GB
/var	30 GB
/tmp	2 GB
/	63 GB

❒ (Conditional) For SUSE Linux Enterprise Server (SLES), ensure that the following packages are installed:

Package	Description
perl-gettext, gettext-runtime	The required library and tools to create and maintain message catalogs.
python	The basic Python library.

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

- ❒ (Conditionally) For manually installing RHEL packages, see Installing Packages and Dependent RPMs on RHEL for Access Manager.

NOTE: You can select to install these RPMs automatically along with Access Manager installation. While installing Access Manager, specify `N` when you get the following prompt:

```
Enter the local mount directory if you have the OS ISO mounted locally.
This will be used as the local catalog for the additional rpms.
Do you have a locally mounted ISO (y/n)?
```

The Access Manager installer checks the online catalog and then installs the required RPMs automatically.

- ❒ Ensure that the latest `net-snmp` package from the SLES or RedHat update channel is installed.
- ❒ Zip and unzip utilities is available for the backup and restore procedure.
- ❒ Ports 389 and 636 are open.
- ❒ Static IP addresses.

  If the IP address changes after devices have been imported, these devices can no longer communicate with Administration Console.
- ❒ The tree for the configuration store is named after the server on which you install Administration Console. Check the hostname and rename the machine if the name is not appropriate for a configuration tree name.

Network Requirements

See Section 1.3, “Network Requirements,” on page 18.

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

- OpenLDAP server. If it is installed, uninstall it. If you do not want to uninstall it, ensure that it does not use the port 636 or does not bind the port 389 to localhost.
- The LDAP software such as eDirectory.

- Other version of iManager.

  In addition, you cannot add other iManager product plug-ins to this Administration Console.
- You cannot install Access Manager on a Linux User Management (LUM) machine because of library update conflicts.
- JRE. If it is installed, uninstall it.

2.1.2 Installation Procedure

Installation time: about 20 minutes.

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

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

1. If you have Red Carpet or auto update running, stop these programs before you install Administration Console.
2. Verify that the machine meets the minimum requirements. See Prerequisites for Installing Administration Console on Linux.
3. Open a terminal window.
4. Access the install script as a `root` user:
   - **4a** Ensure that you have downloaded the software.

     For software download instructions, see the release-specific Release Notes.
   - **4b** If you downloaded the `tar.gz` file, unzip it by using the following command:

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

   `./install.sh`

   Ensure that you have adequate space in the system before you proceed with installation.
6. When you are prompted to install a product, select **1. Install Administration Console** and then press Enter.

   The system displays an error message if `/var` uses BTRFS filesystem and the installation is terminated. You can change the filesystem from BTRFS to any other available filesystem, and then try installing.
7. Review and accept the License Agreement.

   Novell Base and JDK for NetIQ are installed.
8. (Optional) The installer displays a warning if the host name of the system is mapped to the IP address 127.0.0.2 in the `/etc/hosts` file:

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

Specify `Y` to proceed.

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

9 Verify that the required rpms are of the latest versions. Specify `Y` to proceed.

10 Specify the IP address of the local Administrator server.

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

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

12 Specify the administration username.

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

NOTE:
- Administration Console username does not accept special characters `#` (hash), `&` (ampersand), and `()` (round brackets).
- If you are installing secondary Administration Console, the username must be from the `o=novell` container. If the username is from any other container, the Administration Console installation fails.

---

13 Specify the administration password. Use alphanumeric characters only.

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

---

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

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

The following components are installed:

Component	Description
Syslog	Responsible for packaging and forwarding the audit log entries to the configured Syslog Server. For more information, see Auditing in the Access Manager 4.5 Administration Guide.
Tomcat for NetIQ	NetIQ packaging of the Java-based Tomcat web server used to run servlets and JavaServer Pages (JSP) associated with NetIQ Access Manager web applications.
Access Manager Configuration Store	An embedded version of eDirectory used to store user-defined server configurations, LDAP attributes, Certificate Authority keys, certificates, and other Access Manager attributes that must be securely stored.
iManager	The web-based Administration Console that provides customized and secure access to server administration utilities. It is a modified version and cannot be used to manage other eDirectory trees.
Device Manager	

Component	Description
Administration Console	A modification of iManager that enables management of all aspects of Access Manager. This component is not a standard iManager plug-in. It significantly modifies the tasks that iManager can perform.
Identity Server Administration Plug-In	Works in conjunction with Administration Console for managing Identity Server.
REST API Service (AMService)	
Patch Management Tool	

15 Record the login URL.

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

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

Use this to configure Access Manager components.

16 Continue with "Configuring the Linux Administration Console Firewall" on page 48.

2.1.2.1 Configuring the Linux Administration Console Firewall

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

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

This launches the Firewall Configuration screen.

2 Click **Allowed Services** > **Advanced**.

3 In **TCP Ports**, specify the ports to open.

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

- 8080
- 8443
- 3080
- 3443

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

- 2080
- 2443

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

- 1443
- 8444

- 1289
- 1290
- 524
- 636

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

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

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

---

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

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

6 Continue with Section 2.3, “Logging In to Administration Console,” on page 51.

2.2 Installing Administration Console on Windows

2.2.1 Prerequisites for Installing Administration Console on Windows

- Ensure that the system meets the requirements for installing Administration Console.

  For information about the requirements, see *NetIQ Access Manager System Requirements*.
- The hard disk has ample space for logging in a production environment. This disk space must be in the local server and not in the remote server.
- Static IP address
- Ports 389 and 636 are open

For information about browser support, see Browser Support in the *NetIQ Access Manager System Requirements* guide.

For information about network requirements, see Section 1.3, “Network Requirements,” on page 18.

2.2.2 Installation Procedure

IMPORTANT: Before you start the installation, ensure that Powershell is installed and enabled.

Installation time: about 20 minutes.

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

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

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

   For software download instructions and the filename, see the release-specific Release Notes.
5. Double-click the `<ZIP filename>.exe` file from the extracted folder.
6. Read the introduction, then click **Next**.
7. Accept the license agreement, then click **Next**.
8. Select **Access Manager Administration Console**, then click **Next**.

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

   The first Administration Console installed becomes the primary console.

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

    NOTE: If you are installing secondary Administration Console, the user ID must be from the `o=novell` container. If you specify a user from other container, the installer fails to install Administration Console.
11. Specify the static IP address of the machine.
12. Click **Install**.

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

    `\Program Files\Novell\log\AccessManagerServer_ InstallLog.log`
14. Restart the server.

    IMPORTANT: You must restart the server before installing any other Access Manager components.
15. Continue with "Configuring the Windows Administration Console Firewall" on page 51.

2.2.2.1 Configuring the Windows Administration Console Firewall

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

1 Click **Control Panel** > **Windows Firewall**.

2 Click **Advanced**, then for the Local Area Connection, click **Settings**.

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

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

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

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

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

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

6 Run the following commands to restart Tomcat:

```
net stop Tomcat8
net start Tomcat8
```

7 Continue with Section 2.3, “Logging In to Administration Console,” on page 51.

2.3 Logging In to Administration Console

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

Important points that you must know:

- You cannot use Administration Console to log in to other eDirectory trees and manage them.

- Do not download and add iManager plug-ins to this customized version. It may result in destroying the Access Manager schema, which can prevent you from managing Access Manager components. This can also prevent communication among the modules.
- Do not start multiple sessions of Administration Console on the same machine through the same browser. Browsers share session information and this can cause unpredictable issues in Administration Console. However, you can start different sessions with different brands of browsers.

Perform the following steps to log in to Administration Console:

1. Enable browser pop-ups.
2. On Administration Console, ensure that ports 8080 and 8443 are open.

   For information, see "Configuring the Linux Administration Console Firewall" on page 48 and "Configuring the Windows Administration Console Firewall" on page 51.
3. From a client machine external to your Administration Console server, launch a browser and specify the Administration Console URL.

   Use the IP address established when you installed Administration Console. It includes the application `/nps` and the following ports:

   - 8080 (HTTP) or 8443 (HTTPs): When only Administration Console is installed on the machine.
   - 2080 (HTTP) and 2443 (HTTPs): When Identity Server is installed on the same machine.

   For example, if the IP address of your Administration Console is 10.10.10.50, specify the following as URL:

   ```
   http://10.10.10.50:8080/nps
   ```
4. Click **OK** to accept the certificate.

   You can select either the permanent or temporary session certificate option.
5. On the Login page, specify the administrator name and password that you defined during Administration Console installation.
6. Click **Login**. Access Manager Dashboard opens.

   For more information about this view or about configuring Administration Console, see Configuring the Default View in the Access Manager 4.5 Administration Guide.

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

   ---
7. Continue with one of the following:
   - Before configuring the system, you need to install other Access Manager components. You need to install at least one Identity Server and one Access Gateway. It is recommended to next install Identity Server. See Chapter 3, "Installing Identity Server," on page 55.
   - If your Administration Console server has multiple interface cards, see "Enabling Administration Console for Multiple Network Interface Cards" on page 53.

NOTE: You can provide fault tolerance for the configuration store on Administration Console by installing secondary versions of the console. See "High Availability and Fault Tolerance" in the *Access Manager 4.5 Administration Guide*.

2.4 Enabling Administration Console for Multiple Network Interface Cards

Making Administration Console available for all network interface cards (NICs) is a security risk. However, you might want to allow this situation when, for example, Identity Server has multiple NICs and is also available on all ports.

Perform the following steps to enable Administration Console for Multiple NICs:

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

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

   Windows Server 2016 R2: `\Program Files\Novell\Tomcat\conf`
2. Locate the connector with the `NIDP_Name="connector"` set.
3. Delete the `address` attribute and save the file.

3 Installing Identity Server

Identity Server is the second component you install.

3.1 Prerequisites for Installing Identity Server

- Ensure that the system meets the requirements for installing Identity Server.

  For information about the requirements, see *NetIQ Access Manager System Requirements*.
- If you are installing Access Manager components on multiple machines, ensure that the time and date are synchronized on all machines.
- Ensure that the hard disk has ample space for logging in a production environment. This disk space must be local and not remote.
- Ensure that Administration Console is running. See Installing Administration Console.
- Do not perform any configuration tasks in Administration Console during an Identity Server installation.
- If you installed Administration Console on a separate machine, ensure that the DNS names resolve between Identity Server and Administration Console.
- When you are installing Identity Server on a separate machine (recommended for production environments), ensure that the following ports are open on both Administration Console and Identity Server:

  8444
  1443
  1289
  1290
  524
  636

  For information about how to open ports, see Configuring the Linux Administration Console Firewall and Configuring the Windows Administration Console Firewall.

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

- You must establish a static IP address for your Identity Server to reliably connect with other Access Manager components. If the IP address changes, Identity Server can no longer communicate with Administration Console.

3.2 Installing Identity Server on Linux

3.2.1 Points to Consider for Installing Identity Server on Linux

- Ensure that you have read and implemented prerequisites specified in Prerequisites for Installing Identity Server.
- 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/novell	1 GB
/opt/volera	5 MB
/var/opt/novell	1 GB
/var	512 MB
/usr	25 MB
/etc	1 MB
/tmp/novell_access_manager	10 MB
/tmp	10 MB
/	512 MB

NOTE: These are the minimum free disk spaces that must be available before installation or upgrade. However, it is recommended to maintain more than the specified free disk space based on the requirement of your production environment.

- (Conditional) For SUSE Linux Enterprise Server (SLES), ensure that the following packages are installed
  - rsyslog-module-gtls
  - rsyslog

- binutils
- glibc-32bit

- (Conditional) For installing the RHEL packages manually, see *Installing Packages and Dependent RPMs on RHEL for Access Manager*.

  NOTE: You can select to install these RPMs automatically along with Access Manager installation. While installing Access Manager, specify `N` when you get the following prompt:

  ```
  Enter the local mount directory if you have the OS ISO mounted locally.
  This will be used as the local catalog for the additional rpms.
  Do you have a locally mounted ISO (y/n)?
  ```

  The Access Manager installer checks the online catalog and then installs the required RPMs automatically.

- gettext
- python (interpreter)

IMPORTANT:

- No LDAP software, such as eDirectory or OpenLDAP, can be installed. (A default installation of SLES installs and enables OpenLDAP).
- If the OpenLDAP server is installed, uninstall it. If you do not want to uninstall it, ensure that it does not use the port 636 or does not bind the port 389 to localhost.
- Because of library update conflicts, you cannot install Access Manager on a Linux User Management (LUM) machine.

For information about browser support, see Browser Support in the NetIQ Access Manager System Requirements guide.

For information about network requirements, see Section 1.3, “Network Requirements,” on page 18.

3.2.2 Installation Procedure

Installation time: about 10 minutes.

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

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.

     For software download instructions, see the release-specific Readme.
   - **3b** If you downloaded the `tar.gz` file, unzip the file by using the following command:

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

3c Change to the `novell-access-manager` directory.

4 At the command prompt, run the following install script:

```
./install.sh
```

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

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

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

The following warning is displayed:

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

For information about configuring NAT, see Configuring Administration Console Behind NAT.

6 Specify `Y` to proceed.

7 Review and accept the License Agreement.

8 Verify that the required rpms are of the latest versions. Specify `Y` to proceed.

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

10 Specify the IP address of the Novell Access Manager Server Communications Local Listener. Specify the local NAT IP address if local NAT is available for Identity Server.

If the installation program rejects the credentials and IP address, ensure that the correct ports are open on both Administration Console and Identity Server, as described in Section 3.1, “Prerequisites for Installing Identity Server,” on page 55.

11 The following components are installed:

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

12 Continue with one of the following actions:

- Verify the installation. See "Verifying Identity Server Installation" on page 60
- Install Access Gateway. See Section 4.2.2, "Installing Access Gateway Appliance," on page 69 or Section 4.3, "Installing Access Gateway Service," on page 75.
- Configure Identity Server. See Setting Up a Basic Access Manager Configuration in the Access Manager 4.5 Administration Guide.

NOTE: After installing Identity Server, you must create a cluster configuration. See Configuring Identity Servers Clusters in the Access Manager 4.5 Administration Guide.

3.3 Installing Identity Server on Windows

3.3.1 Points to Consider for Installing Identity Server on Windows

- Ensure that you have read and implemented prerequisites specified in Prerequisites for Installing Identity Server.
- Ensure that the hard disk has ample space for logging in a production environment. This disk space must be local and not remote.
- Ensure that the operating system is in either Standard or Enterprise Edition with the latest patches applied.

IMPORTANT: No LDAP software, such as eDirectory or OpenLDAP, can be installed.

For information about browser support, see Browser Support in the NetIQ Access Manager System Requirements guide.

For information about network requirements, see Section 1.3, "Network Requirements," on page 18.

3.3.2 Installation Procedure

Installation time: about 10 minutes.

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

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

2 Download the ZIP file and extract it.

For software download instructions and the filename, see the release-specific Release Notes.

3 Double-click the `<ZIP filename>.exe` file from the extracted folder.

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

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

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

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

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

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

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

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

11 Continue with one of the following actions:

- Verify the installation. See "Verifying Identity Server Installation" on page 60
- Install Access Gateway. See Section 4.2.2, "Installing Access Gateway Appliance," on page 69 or Section 4.3, "Installing Access Gateway Service," on page 75.
- Configure Identity Server. See Configuring Identity Servers Clusters in the Access Manager 4.5 Administration Guide.

NOTE: After installing Identity Server, you must create a cluster configuration. See Configuring Identity Servers Clusters in the Access Manager 4.5 Administration Guide.

3.4 Verifying Identity Server Installation

1 Log in to Administration Console.

See Section 2.3, "Logging In to Administration Console," on page 51.

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

3.5 Translating Identity Server Configuration Port

To enable Identity Server to communicate through a firewall, you can perform one of the following actions:

- Open TCP ports 8080 or 8443. These are default ports used respectively for non-secure and secure communication with Identity Server.
- Configure the Identity Server service to use the TCP port 80 or 443.

This section includes the following topics:

- "Changing the Port on Windows Identity Server" on page 61
- "Changing the Port on Linux Identity Server" on page 61

3.5.1 Changing the Port on Windows Identity Server

Perform the following steps:

1. Click **Devices** > **Identity Server > Edit**, and configure **Base URL** with the HTTPS protocol and TCP port 443.
2. Click **OK**.
3. Update Identity Server.
4. In a terminal window, open the `\Program Files\Novell\Tomcat\conf\server.xml` file.
5. Change the ports from 8080 and 8443 to 80 and 443.
6. Restart the Tomcat service by running the following command:

   ```
   net stop Tomcat8
   net start Tomcat8
   ```

3.5.2 Changing the Port on Linux Identity Server

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

The following are two solutions out of many possibilities:

- If you have disabled the SLES firewall and do not have any other Access Manager components installed on the same server along with Identity Server, use a simple iptables script to translate the ports. See Configuring a Simple Redirect Script.
- If you have configured the SLES firewall or have installed other Access Manager components on the same server along with Identity Server, use a custom rule script that allows for multiple port translations. See Configuring iptables for Multiple Components.

For more information about iptables, see "Iptable Tutorial 1.2.2" (https://www.frozentux.net/iptables-tutorial/iptables-tutorial.html) and "NAM Filters for iptables Commands" (http://www.novell.com/communities/node/4029/nam-filters-iptables-commands).

Port Forwarding

For both of these configurations (Configuring a Simple Redirect Script and Configuring iptables for Multiple Components) to work, you must enable port forwarding. To verify whether port forwarding is enabled, run the following command:

```
- cat /proc/sys/net/ipv4/ip_forward
```

If the value is 0, then port forwarding is not enabled.

To enable port forwarding, perform the following steps:

1. Run the following command:

   ```
   echo 1 > /proc/sys/net/ipv4/ip_forward
   ```

2. Verify the status.

For more information, see How To Forward Ports through a Linux Gateway with Iptables (https://www.digitalocean.com/community/tutorials/how-to-forward-ports-through-a-linux-gateway-with-iptables).

3.5.2.1 Configuring a Simple Redirect Script

This simple solution works only if you are not using iptables to translate ports of other applications or other Access Manager components. For a solution that works with multiple components, see "Configuring iptables for Multiple Components" on page 65.

Ensure that you have enabled port forwarding. See "Port Forwarding" on page 61.

Perform the following steps to configure a simple redirect script:

On SLES 12 SP4 or RHEL server

1. Click **Devices** > **Identity Server > Edit**, and configure **Base URL** with HTTPS protocol and Port 443.
2. Click **OK**.
3. Update Identity Server.
4. At a terminal window, log in as the `root` user.
5. Create a unit configuration file to hold the iptables rule and place it in any directory. For example, `/usr/bin/redirect-idp`.

   Ensure that it has execute rights. You can use CHMOD as appropriate.

NOTE: Do not create the file in the `/etc/init.d` directory because it may cause some issues. For information about the issues, see 13.3.3 System V Compatibility (https://www.suse.com/documentation/sles-12/book_sle_admin/data/sec_boot_systemd_boot.html).

---

6 Copy the following example script and paste it in the file that you created in Step 5 on page 62.

The following is an example of a redirect startup file:

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

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

. /etc/rc.status



# First reset status of this service
rc_reset

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

```
        rc_status -v
        ;;
    restart)
        $0 stop
        $0 start
        rc_status
        ;;
    *)
        echo "Usage: $0 {start|stop|restart}"
        exit 1
        ;;
esac
rc_exit
```

For more information about init scripts for SLES 12, see "Managing Services in a Running System" (https://www.suse.com/documentation/sles-12/book_sle_admin/data/sec_boot_systemd_basics.html) in the *SLES 12 Administration Guide*.

7 Create a systemd service unit at `/etc/systemd/system/<unit-name>.service`. In this example unit-name is redirect-idp therefore, the service unit is `/etc/systemd/system/redirect-idp.service`.

8 Copy the following code and paste it in the service unit:

```
[Unit]
Description=Novell AM-IDP-Redirection

After=local-fs.target network.target

[Service]
Type=oneshot
ExecStart=/usr/bin/redirect-idp start
ExecStop=/usr/bin/redirect-idp stop
RemainAfterExit=yes

[Install]
WantedBy=multi-user.target
```

9 Modify the service unit content as per requirement but ensure that `ExecStart` and `ExecStop` script points to the script that you created in the unit configuration file.

In this example, the scripts must include `/usr/bin/redirect-idp`.

10 Execute the following commands:

1. `systemctl daemon-reload`
2. `systemctl enable <unit-name>.service`

   For example, `systemctl enable redirect-idp.service`

11 Reboot the Identity Server machine.

12 Verify that port 443 is being routed to Identity Server by running the following command:

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

The following is a sample entry:

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

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

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

3.5.2.2 Configuring iptables for Multiple Components

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

Identity Server requires pre-routing commands.

NOTE: Port forwarding must be enabled for this configuration to work. See Port Forwarding.

Adding Identity Server Commands

1 In Administration Console, click **Devices** > **Identity Server > Edit**, and configure **Base URL** with the HTTPS protocol and the TCP port 443.

2 Click **OK**.

3 Update Identity Server.

4 On Identity Server, edit the `/etc/sysconfig/SuSEfirewall2` file.

4a Change the FW_CUSTOMRULES="" line to the following:

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

4b Save the changes and exit.

5 Open the `/etc/sysconfig/scripts/SuSEfirewall2-custom` file in an editor.

This is the custom rules file you specified in Step 4.

6 Add the following lines under the `fw_custom_before_port_handling()` section:

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

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

The second command rewrites the health checks.

7 Save the file.

8 At the system console, restart the firewall by running the following command:

```
/etc/init.d/SuSEfirewall2_setup restart
```

9 Verify that port 443 is being routed to Identity Server by running the following command:

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

The following is a sample entry:

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

This entry states that eth0 is routing TCP port 443 to IP address 10.10.0.1:8443.

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

4 Installing Access Gateway

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

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

This section includes the following topics:

4.1 Feature Comparison of Different Types of Access Gateways

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

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

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

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

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

Feature	Access Gateway Appliance	Access Gateway Service
Platform support	SLES 12 SP3	◆ SLES 12 SP4 ◆ Red Hat Enterprise Linux 6.10 ◆ Red Hat Enterprise Linux 7.6 ◆ Windows Server 2016
Network configuration ◆ DNS servers ◆ Gateways ◆ Network interface cards ◆ Host names	Configurable from Administration Console. After the installation, by default only one network interface card is displayed in Administration Console. To detect other network interface card, perform the following steps: 1. Configure a primary IP Address in YaST for the remaining interfaces. 2. Click **Devices > Access Gateways > Select the device > New IP > click OK**.	Configurable with standard operating system utilities.
Date and time	Configurable from Administration Console.	Configurable with standard operating system utilities.
Cache directory	Uses Apache-caching. The cached files are stored in clear text. The operating system must be configured to protect this directory. For more information about the Apache model, see "Caching Guide".	Uses filesystem provided by the Apache mod_cache module. For more information about the Apache model, see "Caching Guide".

4.2 Installing Access Gateway Appliance

Access Gateway Appliance is a virtual appliance that is packaged in an OVF format. This makes the deployment of Access Gateway easy and fast.

The OVF is preconfigured with the following hardware:

- 4 GB RAM
- Dual CPU or Core
- A static IP address for your Access Gateway server and an assigned DNS name (host name and domain name).
- 100 GB hard disk

  8 GB is reserved for swap.

  You can modify the RAM and CPU based on your requirement.

Linux allows four primary partitions per hard disk. Access Gateway Appliance uses the following partitions:

Table 4-2 *Access Gateway Appliance Partitions*

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

NOTE: If the production environment requires more space for logging the data, you must provide additional disk space before configuring Access Gateway Appliance. You cannot add the hard disk space after configuring Access Gateway Appliance. For information about using the additional hard disk, see "Using Additional Hard Disk" on page 75.

4.2.1 Prerequisites for Installing Access Gateway Appliance

- Ensure that the server meets the minimum hardware requirements. See *NetIQ Access Manager System Requirements*.
- If you want to try any advanced installation options such as driver installation or network installation, see the SUSE Linux Enterprise Server 12 Installation Guide (https://www.suse.com/documentation/sles-12/book_sle_deployment/data/book_sle_deployment.html).

For information about network requirements, see Section 1.3, "Network Requirements," on page 18.

4.2.2 Installing Access Gateway Appliance

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

What you need to know	◆ Username and password of the administrator ◆ IP address of Administration Console ◆ Static IP address for Access Gateway ◆ 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

IMPORTANT: After Access Gateway Appliance installation, upgrade the Linux kernel to the latest security patch to avoid any security vulnerabilities. For more information, see Installing or Updating Security Patches for Access Gateway Appliance.

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

4.2.2.1 Prerequisites

- Ensure that the server meets the minimum hardware requirements. See Section 4.2.1, "Prerequisites for Installing Access Gateway Appliance," on page 69.
- If you want to try any advanced installation options such as driver installation or network installation, see the SUSE Linux Enterprise Server 12 Installation Guide (https://www.suse.com/documentation/sles-12/book_sle_deployment/data/book_sle_deployment.html).

4.2.2.2 Installing Access Gateway Appliance

1. Deploy the Access Gateway Appliance OVF template to your enterprise virtual environment.

   For more information, see Deploy an OVF Template (https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.vm_admin.doc/GUID-17BEDA21-43F6-41F4-8FB2-E01D275FE9B4.html) in the *vSphere Virtual Machine Administration Documentation*.
2. Select the desired language, review the license agreement, then click **Accept**.
3. Specify the following details on the Appliance Passwords and Time Zone page:

Field	Description
root Password	Specify the password for `root`.
NTP Server	Specify the name of the primary and secondary NTP server.
Region and Time Zone	Select a region and time zone.

4. Specify the hostname for the Access Gateway Appliance server and click **Next**.
5. Specify the following network setting details:

Field	Description
IP Address	The IP address of Access Gateway.
Network Mask	The subnet mask of Access Gateway Appliance network.
Gateway	The IP address of the default gateway.
DNS Server	The IP address of your DNS server. You must configure at least one DNS server. Specify the IP address of your additional DNS server, if you have configured. This is an optional configuration.
Domain Search	Specify the domain name.

6 Click **Next**.

7 Continue with Configuring Access Gateway Appliance.

To add a new hard disk to the virtual machine, see Add a New Hard Disk to a Virtual Machine (https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.vm_admin.doc/GUID-F4917C61-3D24-4DB9-B347-B5722A84368C.html) in the *vSphere Virtual Machine Administration Documentation*.

4.2.3 Configuring Access Gateway Appliance

Access Gateway Appliance is bundled with Configuration console (`https://<access_gateway_appliance-IP address>:9443`), Common Appliance Framework (CAF). You can use this console for modifying the Access Gateway Appliance configuration.

After installing Access Gateway Appliance, you must configure Access Gateway Appliance using the Configuration console to make it available in Administration Console.

Perform the following steps to configure Access Gateway Appliance:

NOTE: If you are using an existing IP address of Access Gateway Appliance and it uses a multiple NIC card in your cluster set up, ensure to configure the primary IP addresses for all the interfaces before configuring Access Gateway Appliance.

Also, ensure that you provide the IP address in the same order to the interfaces as it is in the existing Access Gateway Appliance.

---

1 Access the `https://<access_gateway_appliance-IP address>:9443` URL to launch the Configuration console.

2 Log in as a `root` user.

3 Click **Access Gateway Configuration** under **Access Gateway Tools**.

4 Specify the Administration Console URL, username, and password.

5 Click **Save**.

You can use the following configuration options in the console based on your requirement:

- Section 4.2.3.1, “Managing Digital Certificates,” on page 71
- Section 4.2.3.2, “Setting Administrative Passwords,” on page 74
- Section 4.2.3.3, “Performing an Online Update,” on page 75
- Section 4.2.3.4, “Using Additional Hard Disk,” on page 75
- Section 4.2.3.5, “Performing a Product Upgrade,” on page 75
- Section 4.2.3.6, “Rebooting or Shutting Down the Appliance,” on page 75

4.2.3.1 Managing Digital Certificates

You can perform the following actions using the Digital Certificates tab:

- Add and activate certificates for Access Gateway Appliance.

- Create your own certificate and then get it signed by a CA.
- Use an existing certificate and key pair.

IMPORTANT: You can manage the certificates only for the Access Gateway Appliance (port 9443).

Access Gateway Appliance is shipped with a self-signed digital certificate. Instead of this self-signed certificate, it is recommended to use a trusted server certificate signed by a trusted CA, such as Digicert or Equifax.

To use and activate the digital certificate, perform the following tasks:

- "Using the Digital Certificate Tool" on page 72
- "Using an Existing Certificate and Key Pair" on page 73
- "Activating the Certificate" on page 74

Using the Digital Certificate Tool

- "Creating a New Self-Signed Certificate" on page 72
- "Getting Your Certificate Officially Signed" on page 73

Creating a New Self-Signed Certificate

1 Log in to the Configuration console (`https://<access_gateway_appliance-IP address>:9443`) as the `root` user.

2 Click **Digital Certificates**.

3 In the **Key Store** list, select **Web Application Certificates**.

4 Click **File** > **New Certificate (Key Pair)** and specify the following information:

4a **General**

Alias: Specify a name that you want to use to identify and manage this certificate.

Validity (days): Specify for how long you want the certificate to remain valid.

4b **Algorithm Details**

Key Algorithm: Select either **RSA** or **DSA**.

Key Size: Select the preferred key size.

Signature Algorithm: Select the preferred signature algorithm.

4c **Owner Information**

Common Name (CN): Specify the name that exactly matches the server name in the URL for browsers to accept the certificate for SSL communication.

Organization (O): (Optional) Specify the organization. For example, My Company.

Organizational Unit (OU): (Optional) Specify the organizational unit as mentioned in the directory, such as a department or division. For example, Purchasing.

Two-letter Country Code (C): (Optional) Specify the two-letter country code. For example, US.

State or Province (ST): (Optional) Specify the state or the province name. For example, Utah.

City or Locality (L): (Optional) Specify the city name. For example, Provo.

5 Click **OK**.

After the certificate is created, it is self-signed.

6 Make the certificate official. See "Getting Your Certificate Officially Signed" on page 73.

Getting Your Certificate Officially Signed

1 On the Digital Certificates page, select the certificate that you just created.

2 Click **File** > **Certificate Requests** > **Generate CSR**.

3 Complete the process of emailing your digital certificate to a certificate authority (CA), such as Digicert.

The CA takes your Certificate Signing Request (CSR) and generates an official certificate based on the information in the CSR. The CA then emails the new certificate and certificate chain to you.

4 After you have received the official certificate and certificate chain from the CA, perform the following actions:

4a Revisit the Digital Certificates page.

4b Click **File** > **Import** > **Trusted Certificate**.

4c Click **Browse** and select the trusted certificate chain that you received from the CA.

4d Click **OK**.

4e Select the self-signed certificate.

4f Click **File** > **Certification Request** > **Import CA Reply**.

4g Click **Browse** and select the official certificate to be used to update the certificate information.

On the **Digital Certificates** page, the name in the **Issuer** column for your certificate changes to the name of the CA that stamped your certificate.

5 Continue with activating the certificate, as described in "Activating the Certificate" on page 74.

Using an Existing Certificate and Key Pair

When you use an existing certificate and key pair, use the `.P12` key pair format.

1 Log in to the Configuration console (`https://<access_gateway_appliance-IP address>:9443`) as the `root` user.

2 Click **Digital Certificates**.

3 In the **Key Store** menu, select **JVM Certificates**.

4 Click **File** > **Import** > **Trusted Certificate**.

5 Click **Browse** and select your existing certificate.

6 Click **OK**.

7 Click **File** > **Import** > **Trusted Certificate**.

8 Click **Browse** and select your existing certificate chain for the certificate that you selected in Step 4.

9 Click **OK**.

10 Click **File** > **Import** > **Key Pair**.

11 Click **Browse** and select your `.P12` key pair file and specify your password if required.

12 Click **OK**.

13 Continue with "Activating the Certificate" on page 74.

Activating the Certificate

1 On the **Digital Certificates** page, in the **Key Store** list, select **Web Application Certificates**.

2 Select the certificate that you want to make active and click **Set as Active**, then click **Yes**.

3 Select the certificate and click **View Info** to verify that the certificate and certificate chains are created appropriately.

4 Click **Close**, when you have activated the certificate successfully.

5 Restart the Jetty service by using the `systemctl restart vabase-jetty.service` command.

4.2.3.2 Setting Administrative Passwords

You can modify passwords and SSH access permissions for an Access Gateway Appliance `root` administrator in the **Administrative Passwords** tab. Depending on your password policy requirements, modify passwords periodically or reassign responsibility of the Access Gateway Appliance administration to another person.

NOTE: `vaadmin` helps in managing virtual-machine-level settings and service configurations that affect an entire service and its interactions with other services.

On the **Administrative Passwords** page, the `vaadmin` user can change the vaadmin user password and `root` user can change the `root` password. Perform the following steps to change the password:

Managing the administrative access as the `vaadmin` user:

1 Log in to the Configuration console (`https://<access_gateway_appliance-IP address>:9443`) as the `vaadmin` user.

2 Click **Administrative Passwords**.

3 Specify a new password for the `vaadmin` administrator. You must also specify the current `vaadmin` password.

4 Click **OK**.

Managing the administrative access as the `root` user:

1 Log in to the Configuration console (`https://<access_gateway_appliance-IP address>:9443`) as the `root` user.

2 Click **Administrative Passwords**.

3 Specify a new password for the `root` administrator. You must also specify the current `root` password.

4 (Optional) Select or deselect **Allow root access to SSH**.

5 Click **OK**.

4.2.3.3 Performing an Online Update

See Installing or Updating Security Patches for Access Gateway Appliance.

4.2.3.4 Using Additional Hard Disk

By default, the var directory is in the boot partition. If the logs fill the space of the var directory, Access Gateway Appliance can stop working. Therefore, you can add hard disk for the var directory.

You can use the additional hard disk that you added before configuring Access Gateway. To use additional hard disk, perform the following steps:

1. Log in to Configuration console (`https://<access_gateway_appliance-IP address>:9443`). then click **/var Mount Configuration**.
2. Select the appropriate hard disk and the file system type.
3. Click **Save**.
4. Reboot the Access Gateway Appliance.

4.2.3.5 Performing a Product Upgrade

In this release, you need to migrate Access Gateway Appliance to the latest version.

For information about how to migrate to Access Gateway Appliance 4.5, see “Upgrading Access Gateway Appliance” on page 141.

4.2.3.6 Rebooting or Shutting Down the Appliance

You might require to shutdown or to restart Access Gateway Appliance for maintenance. It is recommended to use the console options instead of using Power Off/On option in the hypervisor's VM management tool.

1. Log in to the Configuration console (`https://<access_gateway_appliance-IP address>:9443`) as the `root` user.
2. In the upper right corner of the Appliance Configuration pane, click **Reboot** or click **Shutdown**.

4.3 Installing Access Gateway Service

4.3.1 Installing Access Gateway Service on Linux

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

4.3.1.1 Prerequisites for Installing Access Gateway on Linux

- ❒ Ensure that the system meets the requirements for installing Access Gateway. For information about the requirements, see NetIQ Access Manager System Requirements.
- ❒ An Administration Console is installed. See Installing Administration Console.
- ❒ An Identity Server is installed and configured. See Installing Identity Server
- ❒ Verify that the time on the machine is synchronized with the time on Administration Console. If the times differ, Access Gateway Service does not import into Administration Console.
- ❒ If a firewall separates the machine and Administration Console, ensure that the required ports are opened. See Table 1-3 on page 30.
- ❒ Because Access Gateway Service runs as a service, the default ports (80 and 443) that Access Gateway Service uses might conflict with the ports of other services running on the machine. If there is a conflict, you need to decide which ports each service can use.
- ❒ (Windows Server 2012) If the web server (IIS) has been installed by default during the Windows Server 2012 install, the Access Gateway Service installation program detects its presence from the registry and issues a shutdown command. Even if you have never activated the web server and if even it is not running, the shutdown command is issued. Because Access Gateway Service cannot be installed while the IIS server is running, the installation program needs to ensure that it is not running.
- ❒ (Conditional) For SUSE Linux Enterprise Server (SLES). Ensure that the following rpms or higher versions are installed:
  - rsyslog-module-gtls-5.10.1-0.7.49
  - rsyslog-5.10.1-0.7.49
  - binutils 2.23.1-0.17.18
  - glibc-32bit

  IMPORTANT: ◆SLES installation libraries may be distributed across multiple CDs or DVDs. In **YaST > Software > Software Repositories** select the required CD or DVD to install the rpm files. If the rpm files are not available on the SLES server, the Access Manager installation process takes care of installing these rpm files from the SLES repository.

  - To search if an rpm is installed, use `rpm -qa | grep` *<rpm name>*. For example, `rpm - qa | grep libapr-util`.
- ❒ (Conditional) For installing the RHEL packages manually, see Appendix 8, “Installing Packages and Dependent RPMs on RHEL for Access Manager,” on page 111.

  NOTE: You can select to install these RPMs automatically along with Access Manager installation. While installing Access Manager, specify `N` when you get the following prompt:

  ```
  Enter the local mount directory if you have the OS ISO mounted locally.
  This will be used as the local catalog for the additional rpms.
  Do you have a locally mounted ISO (y/n)?
  ```

  The Access Manager installer checks the online catalog and then installs the required RPMs automatically.
- ❒ 2 to10 GB hard disk space per reverse proxy that requires caching and for log files. The amount varies with rollover options and logging level that you configure.

❒ 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/novell	1 GB
/opt/volera	5 MB
/var/opt/novell	1 GB
/var	512 MB
/usr	25 MB
/etc	1 MB
/tmp/novell_access_manager	10 MB
/tmp	10 MB
/	512 MB

NOTE: These are the minimum free disk spaces that must be available before installation or upgrade. However, it is recommended to maintain more than the specified free disk space based on the requirement of your production environment.

❒ A static IP address and a DNS name. The ActiveMQ module of Access Gateway Service must be able to resolve the machine's IP address to a DNS name. If the module can't resolve the IP address, the module does not start.

❒ Other Access Manager components should not be installed on the same machine.

For information about network requirements, see Section 1.3, "Network Requirements," on page 18.

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

4.3.1.2 Installation Procedure

You must install Access Gateway Service on a separate machine.

Installation time: about 10 minutes.

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

1 Log in to the NetIQ Customer Center and follow the link that allows you to download software. For an evaluation version, download the media kit from NetIQ Downloads.

2 Copy the file to your machine.

For the filename, see the release-specific Release Notes.

3 Prepare your machine for installation:

Make your operating system installation media available.

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

4. Start installation by running the following script:

   `./ag_install.sh`

5. Review and accept the License Agreement.
6. (Optional) Specify the local NAT IP address if the local NAT is available for Access Gateway.
7. Specify the IP address, user ID, and password of the primary Administration Console.
8. Specify the IP address of Access Gateway.
9. Continue with one of the following sections:
   - Verify the installation. See "Verifying Access Gateway Installation" on page 80
   - Configure Access Gateway. See Configuring Access Gateway in the Access Manager 4.5 Administration Guide.

IMPORTANT: (Applicable for RHEL) When you configure more than 60 proxy services, Apache fails to start. RHEL has 128 semaphore arrays by default which is inadequate for more than 60 proxy services. Apache 2.4 requires a semaphore array for each proxy service.

You must increase the number of semaphore arrays depending on the number of proxy services you are going to use. Perform the following steps to increase the number of semaphore arrays to the recommended value:

1. Open `/etc/sysctl.conf`
2. Add `kernel.sem = 250 256000 100 1024`

   This creates the following:

   Maximum number of arrays = 1024 (number of proxy services x 2)

   Maximum semaphores per array = 250

   Maximum semaphores system wide = 256000 (Maximum number of arrays x Maximum semaphores per array)

   Maximum ops per semop call = 100
3. Use command `sysctl -p` to update the changes.
4. Start Apache.

4.3.2 Installing Access Gateway Service on Windows

4.3.2.1 Prerequisites for Installing Access Gateway on Windows

- Ensure that the system meets the requirements for installing Access Gateway. For information about the requirements, see NetIQ Access Manager System Requirements.
- Ensure that the operating system (physical or virtual) is in either Standard or Enterprise Edition, with the latest patches applied.

- 2 to10 GB per reverse proxy that requires caching and for log files. The amount varies with rollover options and logging level that you configure
- A static IP address and a DNS name. The ActiveMQ module of Access Gateway Service must be able to resolve the machine's IP address to a DNS name. If the module cant resolve the IP address, the module does not start.

  You can verify this by using the `nslookup` command. Enter this command with hostname in the command prompt and it should return the IP address of the host
- Windows packages KB2919442 and KB2919355 must be installed before installing Access Gateway Service. These packages must be installed in the same sequence. You can verify if these packages are installed by using the following commands:
  - `dism /online /get-packages | findstr KB2919442`
  - `dism /online /get-packages | findstr KB2919355`

  If these packages are installed, you will get a confirmation message. If the packages are not installed, you will not receive any response.
- Other Access Manager components should not be installed on the same machine

For information about network requirements, see Section 1.3, "Network Requirements," on page 18.

For prerequisites, see "Prerequisites" on page 70.

4.3.2.2 Installation Procedure

You must install Access Gateway Service on a separate server.

Installation time: about 10 minutes.

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

1. Log in to the NetIQ Customer Center (https://www.netiq.com/customercenter) and follow the link that allows you to download software. For an evaluation version, download the media kit from NetIQ Downloads (https://dl.netiq.com/index.jsp).
2. Download the ZIP file and extract it.

   For the filename, see the release-specific Access Manager Release Notes.
3. Disable any virus scanning programs.
4. To use a remote desktop for installation, use one of the following:
   - Current version of VNC viewer
   - Microsoft Remote Desktop with the `/console` switch for Windows XP SP2
   - Microsoft Remote Desktop with the `/admin` switch for Windows XP SP3
5. Double-click the executable file in the <*ZIP filename*> folder.

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

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

7 Review and accept the License Agreement, then click **Next**.

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

9 (Conditional) Specify the local IP address, if your machine has more than one IP address, which Access Gateway Service will use for communication with Administration Console.

10 (Optional) Specify Access Gateway Local NAT IP address, if the device is behind NAT.

11 Click **Next**.

12 Configure disk cache. This holds the caching objects of Access Gateway.

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

---

13 Click **Next**, then review the installation summary.

14 Click **Install**.

15 Review the log information at the following location:

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

16 Click **Next** > **Done**.

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

At this point, Access Gateway Service is not configured.

18 Continue with one of the following:

- "Verifying Access Gateway Installation" on page 80
- Configure Access Gateway. See Configuring Access Gateway in the Access Manager 4.5 Administration Guide.
- Install another Access Manager component.

4.4 Verifying Access Gateway Installation

1 Log in to Administration Console.

See Section 2.3, "Logging In to Administration Console," on page 51.

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

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

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

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

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

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

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

5 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 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.

6 Deploying Access Manager on Amazon Web Services EC2

You can deploy the following Access Manager components as services on Amazon Web Services (AWS) EC2:

- Administration Console
- Identity Server
- Access Gateway

NOTE: Deployment of Access Gateway Appliance and Analytics Server is not supported on AWS EC2.

Access Manager supports the following operating systems on AWS EC2:

- SUSE Linux Enterprise Server
- Red Hat Enterprise Linux

This section includes the following topics:

6.1 Prerequisites for Deploying Access Manager on AWS

In addition to the system requirements of Access Manager components, ensure that you meet the following prerequisites:

- ❒ An administrative account on AWS EC2.
- ❒ The Access Manager installer (tarball) has been downloaded, extracted, and available for copying to the instances.
- ❒ An SSH client to connect to the AWS EC2 instances from your local client machine.

  By default, Linux and Mac provide access to OpenSSH through the terminal. On Windows, use PuTTY or install the Windows Subsystem for Linux feature (Windows 10 only) to install a Linux distribution environment.

6.2 Deployment Procedure

The deployment procedure consists of the following steps:

1. Creating AWS EC2 Services

2. Creating and Deploying Instances
3. Installing Access Manager
4. (Optional) Creating an AWS EC2 Load Balancer

Figure 1-7 in Section 1.6, “Deploying Access Manager on Public Cloud,” on page 21 illustrates the recommended way for deploying Access Manager on AWS EC2.

IMPORTANT: The LDAP server and web services must be deployed in the public clouds along with Identity Server and Access Gateway.

A VPN connection from Identity Server and Access Gateway in the public cloud to the LDAP user store and web servers in the on-premises deployments is not supported.

6.2.1 Creating AWS EC2 Services

This section outlines steps for creating AWS EC2 services to use with Access Manager. For more information, see the Amazon Elastic Compute Cloud Documentation (https://aws.amazon.com/documentation/ec2/).

Perform the following steps to create AWS EC2 services:

1 Log in to AWS Management Console (https://signin.aws.amazon.com/).

2 Click **Services** and create the following services:

Service	Steps
VPC	1. Click **Services** > **VPC** under Networking & Content Delivery. 2. Click **Start VPC Wizard**. 3. Select a VPC configuration type and click **Select**. 4. Specify the details in the form, and then click **Create VPC**. This creates a private network of the specified size. VPC and subnet creation use the CIDR notation for address ranges. The largest VPC size is a /16 network. For more information, see the Amazon Virtual Private Cloud Documentation (https://aws.amazon.com/documentation/vpc/).
IMPORTANT: Creating a VPC using **Start VPC Wizard** creates Subnets, Internet gateways, and Route table for the VPC. You can view or edit these items as follows:	
Subnets	1. In the left menu, click **Subnets**. 2. Locate the subnet associated with this VPC. 3. Select the subnet, verify the details, and edit if required.
Internet gateways	1. In the left menu, click **Internet Gateways**. 2. Locate the Internet gateways associated with this VPC. 3. Select the Internet gateways, verify the details, and edit if required.

Service	Steps
Route table	1. In the left menu, click **Route Tables**. 2. Select the route table that was automatically created for this VPC. 3. In the **Routes** tab, click **Edit**. 4. Click **Add another route**. 5. In **Destination**, specify `0.0.0.0/0`. 6. In **Target**, select the IGW table that has been created in **Internet gateways**. 7. Click **Save**.

3 Continue with "Creating and Deploying Instances" on page 87.

6.2.2 Creating and Deploying Instances

This section outlines steps to create and deploy instances for a basic setup of Access Manager, which includes an Administration Console, an Identity Server, an Access Gateway, and a user store.

Perform the following steps to create four instances: One for Administration Console, one for Identity Server, one for Access Gateway, and one for the Active Directory user store.

1 Click **Services** > **EC2**.

2 Click **Launch Instance**.

3 Select the `SLES 12 SP4` or `RHEL 7.9` image if you are creating this instance for an Access Manager component (Administration Console, Identity Server, or Access Gateway).

When creating an instance for the Active Directory user store, select a Windows 2012 R2 image instead of SLES or RHEL.

All instances that you create for deploying Access Manager components (Administration Console, Identity Server, or Access Gateway) must have the same operating system type (either SLES or RHEL).

4 Select the instance type that meets requirements of the base operating system and deployment of Access Manager components. See NetIQ Access Manager System Requirements.

Each type has its own instance configuration settings, optimizations, and associated costs.

5 Click **Next: Configure Instance Details**.

Ensure that the instance is using the correct VPC and subnet.

Field	Action
Auto-assign Public IP	Set to `Enable`.
Network Interfaces	Specify a static IP address in **Primary IP**.

6 Click **Next: Add Storage**.

The default storage size is 10 GB. Change it as per your requirement.

7 Click **Next: Add Tags**.

Add tags as desired. Tags enable you to organize instances. For example, you can add the following two tags to each instance:

- A tag indicating what the instance is being used for
- A tag indicating who is the owner of this machine

8 Click **Next: Configure Security Group**.

Security groups are virtual firewall rules for groups of instances. It is recommended to create a separate security group for each group of instances with the same firewall requirements.

For example, you can configure a security group for all nodes of Administration Console, one security group for all nodes of Identity Server, and one security group for all nodes of Access Gateway. By default, a new security group only allows incoming traffic on port 22, so that you can only connect to the instance by using SSH.

For more information, see Amazon EC2 Security Groups for Linux Instances (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html).

9 Create a new security group; specify a name and description for it.

Add additional port rules before installing the Access Manager components. For information about required ports, see Table 1-7, Table 1-8, and Table 1-9.

10 Click **Review and Launch**.

11 After reviewing the details, click **Launch**.

12 Select an existing key pair or create a new one.

This key pair is used for SSH access to the instance. You can use the same key pair with multiple machines.

13 Click **Download Key Pair**.

IMPORTANT: You can connect to and manage your instances only using the private key. Therefore, do not lose the private key after downloading it.

---

14 Repeat Step 1 to Step 13 and create other instances.

15 Continue with "Installing Access Manager" on page 88.

6.2.3 Installing Access Manager

Prerequisites

- ❒ Ensure that you meet the requirements listed in Section 1.3, "Network Requirements," on page 18.
- ❒ Edit the `/etc/hosts` files on each instance and add an entry to resolve its hostname to its private IP address.
- ❒ Create port rules in the various security groups.

  See Step 8 and Step 9 in Section 6.2.2, "Creating and Deploying Instances," on page 87. For the list of ports, see Table 1-7 on page 34, Table 1-8 on page 34, and Table 1-9 on page 35.
- ❒ Before starting Access Manager installation, ensure that the additional packages listed in the prerequisites sections of each Access Manager component are added.
- ❒ Verify the SSH connectivity to the instances. The following is a sample syntax for verifying the connectivity:

"ssh -i <key_name> ec2-user@<instance_public_ip>

To view the public IP address of an instance, click **Instances** > *[instance]* > **Description**.

IMPORTANT: Re-importing Identity Server and Access Gateway is not supported.

Installation Procedure

Perform the following steps to install Access Manager components on the respective instances:

In the following steps, run the Access Manager installation scripts as a `root` user using `sudo`. For example, `sudo sh <script-name>`.

1. Copy the `novell-access-manager-<version>.tar.gz` file using Secure Copy (scp) to the instances on which you will install Administration Console and Identity Server.

   The following is a sample scp command that shows how to copy the installer using the SSH key and username specified while creating the instance:

   ```
   scp -i <keyname> <path&name_of_file_to_copy> ec2-user@<instance_ip>:/<directory>
   ```

2. Copy the `novell-access-gateway-<version>.tar.gz` file to the instance on which you will install Access Gateway.

3. Install Administration Console, Identity Server, and Access Gateway on the respective instances.

   For information about how to install these components, see Installing Administration Console on Linux, Installing Identity Server on Linux, and Installing Access Gateway Service on Linux.

   IMPORTANT: While installing Identity Server and Access Gateway, specify the internal IP address of the Administration Console machine. This ensures that communications among machines happen inside the firewall.

4. Configure Identity Server and Access Gateway.

   For information about how to configure, see "Setting Up a Basic Access Manager Configuration" in the *Access Manager 4.5 Administration Guide*.

6.2.4 (Optional) Creating an AWS EC2 Load Balancer

If multiple Access Gateway and Identity Server instances have been created and configured for clustering, you can configure an AWS EC2 load balancer for each cluster to balance the load of incoming requests across the clustered instances. A separate load balancer is used for an Identity Server cluster and an Access Gateway cluster.

The following procedures provide differences in the configuration details for Identity Server load balancer and Access Gateway load balancer wherever required.

Repeat the steps in Section 6.2.4.1, “Creating Target Groups,” on page 90, Section 6.2.4.2, “Creating an Elastic IP Address,” on page 92, and Section 6.2.4.3, “Creating a Load Balancer,” on page 92, and create separate target groups, elastic IP addresses, and load balancers for Identity Server and Access Gateway clusters.

- Section 6.2.4.1, “Creating Target Groups,” on page 90
- Section 6.2.4.2, “Creating an Elastic IP Address,” on page 92
- Section 6.2.4.3, “Creating a Load Balancer,” on page 92

6.2.4.1 Creating Target Groups

A target group provides a way to associate the load balancer to the IP addresses of instances (targets) among which the load will be distributed.

IMPORTANT: For each load balancer, you need to create two target groups: one for HTTP and one for HTTPS.

For more information about target groups, see `Target group` (http://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-target-groups.html).

Perform the following steps to create a target group:

1. In the EC2 Dashboard, click **Target Groups** under **LOAD BALANCING**.
2. Click **Create target group**.
3. Specify the following details:

Field	Description
Target group name	Specify a name for the target group.
Protocol	Select **TCP**.
Port	Specify the port on which the server is configured for listening. **IMPORTANT:** You need to create two separate target groups for each load balancer, one for HTTP and one for HTTPS. **For Access Gateway** Specify the following values: ◆ If you are creating the target group for the HTTPS traffic, specify `443`. ◆ If you are creating the target group for the HTTP traffic, specify `80`. **For an Identity Server listening on the default ports of 8080/8443** Specify the following values: ◆ If you are creating the target group for the HTTPS traffic, specify `8443`. ◆ If you are creating the target group for the HTTP traffic, specify `8080`. You can use iptables to configure the listeners on Identity Server to use other ports. See Section 3.5, “Translating Identity Server Configuration Port,” on page 60.

Field	Description
Target type	Select ip.
VPC	Select the same VPC that you have selected for the instances of Access Manager components.
Health Check Settings	
Protocol	When creating a target group for the HTTPS protocol, select HTTPS. When creating a target group for the HTTP protocol, select HTTP. The load balancer uses this protocol while performing health checks.
Path	Specify the destination path for health checks. **For Identity Server**, specify `/nidp/app/heartbeat`. **For Access Gateway**, specify `/nesp/app/heartbeat`.
Advanced health check settings	Keep the default values.

4 Click Create.

5 Enable session stickiness.

5a Select the target group you have created.

5b In the Description tab, click Edit attributes.

5c Select Enable for Stickiness.

6 Add the IP addresses of instances (targets) among which load will be distributed.

6a In the edit mode, select the Targets tab, and then click Edit.

6b Click the + (Register targets) icon.

6c Specify the following details:

Field	Description
Network	Populated with the VPC that you have selected under VPC in Step 3.
IP	Specify the private IP address of Identity Server or Access Gateway instances (targets) to register as targets that you want to add in the load balancer.
Port	Populated with the port value that you have specified for Port in Step 3.

6d Click Add to list.

6e Click Register.

6f Repeat Step 6b to Step 6e and add other instances of the same component type that you want to add in the load balancer.

6.2.4.2 Creating an Elastic IP Address

An elastic IP address is a public IPv4 address, which is reachable from the Internet. Elastic IP addresses are used as the listeners for the load balancers.

1. Click **Services** > **EC2**.
2. Click **Elastic IPs**.
3. Click **Allocate new address**.
4. Click **Allocate**.

   A static IPv4 address is allocated that is not used by any other resource.
5. Click **Close**.

6.2.4.3 Creating a Load Balancer

Perform the following steps to create a load balancer:

1. In the left menu, click **Load Balancers**.
2. Click **Create Load Balancers**.
3. Click **Create** under **Network Load Balancer**.
4. Specify the following details:

Field	Description
Name	Specify a name for the load balancer.
Scheme	Select **internet-facing**.
Listeners	Specify the listener ports as follows: **For Identity Server:** ◆ **Load Balancer Protocol**: `TCP` ◆ **Load Balancer Port**: `8080` Click **Add listener** and specify the following: ◆ **Load Balancer Protocol**: `TCP` ◆ **Load Balancer Port**: `8443` **For Access Gateway:** ◆ **Load Balancer Protocol**: `TCP` ◆ **Load Balancer Port**: `80` Click **Add listener** and specify the following: ◆ **Load Balancer Protocol**: `TCP` ◆ **Load Balancer Port**: `443`

Field	Description
Availability Zones	1. Select the same VPC that you have created earlier for Access Manager components. 2. Select the Availability Zone in which Access Manager instances are available. The load balancer routes traffic to the targets in the specified Availability Zones only. 3. Select the Subnet where the Access Manager component, for which you are configuring this load balancer, is available. 4. In Elastic IP, select the elastic IP address you created for this load balancer in "Creating an Elastic IP Address" on page 92.
Tags	Do not make any change.

5 Click Next: Configure Routing.

6 Under Target group, specify the following details:

Field	Description
Target group	Select Existing target group.
Name	Select a target group from the list. You can select only one target group. For example, select the target group that you have created for the HTTP protocol. After creating the load balancer, you need to modify the listener port 8443 to use the target group that is configured for the HTTPS protocol. See Step 12 of this section.
Protocol	Populated with the value that you have configured in the specified target group. Review to ensure that the value is listed correctly.
Port	Populated with the value that you have configured in the specified target group. Review to ensure that the value is listed correctly.
Target type	Populated with the value that you have configured in the specified target group. Review to ensure that the correct value is listed.

7 Under Health Checks, review the following details:

Field	Description
Protocol	Populated with HTTPS or HTTP based on the configuration of the target group you selected in Step 6. See "Creating Target Groups" on page 90.
Path	Populated with the health URL that you configured in the target group selected in Step 6. See "Creating Target Groups" on page 90.
Advanced health check settings	Keep the default values.

8 Click Next: Register Targets.

The list of all targets registered with the target group that you selected is displayed. You can modify this list only after creating the load balancer.

9 Click **Next: Review**.

10 Verify that the load balancer details are correct.

11 Click **Create** and then click **Close**.

12 Update the listener ports to use the appropriate target groups.

12a Select the load balancer you have created.

12b Select the **Listeners** tab.

By default, both listeners (HTTP and HTTPS) are configured to forward to the same target group that you have created in Step 6 > **Name**.

12c Select the HTTPS listener (8443 for Identity Server or 443 for Access Gateway).

12d Click **Actions** > **Edit** to change the target group of the HTTPS listener.

12e In **Default target group**, select the HTTPS target group for that component type (Identity Server or Access Gateway).

12f Click **Save**.

NOTE: For scaling recommendations, see Recommendations for Scaling Access Manager Components in Public Cloud.

6.3 Auto Scaling Access Manager on AWS

AWS EC2 Auto Scaling helps you maintain the application availability and allows you to automatically add or remove EC2 instances according to the conditions you define.

Benefits

- Detects a non-responding instance, terminates it, and replaces it with a new one.
- Adds instances only when needed and scales across purchase options to optimize performance and cost.
- Ensures that the application always has the appropriate amount of compute and provisions it with predictive scaling.

  For more information, see Amazon EC2 Auto Scaling (https://aws.amazon.com/ec2/autoscaling/).

For more information about deploying Access Manager auto scaling on AWS, see Sample Auto Scaling Deployment of Access Manager on AWS (https://www.netiq.com/documentation/access-manager-45-developer-documentation/aws-autoscaling/data/aws-autoscaling.html).

Watch the following video to understand how the auto scaling of Access Manager works in AWS:

http://www.youtube.com/watch?v=IJYx3qbA1gQ

Watch the following video to understand the configuration of Access Manager auto scaling in AWS:

http://www.youtube.com/watch?v=X7OwBHuQFmU

6.4 Monitoring Access Manager in AWS Using CloudWatch

Amazon CloudWatch provides real-time monitoring of the AWS resources.

It tracks various metrics and allows you to create alarms or send notifications when a metric reaches the threshold value. You can configure CloudWatch with CloudWatch Agent to collect system-level metrics and logs from the Access Manager instances and AWS resources. It includes AWS servers as well as on-premises servers.

For example, you can use CloudWatch to monitor the CPU usage and then determine whether you should create or delete instances to meet the dynamic load.

For more information about CloudWatch, see What Is Amazon CloudWatch? (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html)

For more information about CloudWatch Agent, see Collecting Metrics and Logs from Amazon EC2 Instances and On-Premises Servers with the CloudWatch Agent (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Install-CloudWatch-Agent.html).

Perform the following tasks to configure CloudWatch with on-premises servers.

1. Install AWS Command Line Interface (CLI) on the on-premises servers. Access Manager uses AWS CLI to access CloudWatch. The primary distribution method for AWS CLI is `Python pip`. Open a terminal window on the on-premises server run the following commands:

   1a Run the `curl -O https://bootstrap.pypa.io/get-pip.py` command to download the `get-pip.py` installer package.

   1b Run the `pip install --upgrade awscli` command to install AWS CLI.

   For more information about installing AWS CLI, see Installing the AWS CLI (https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-install.html).

2. Create IAM Users for CloudWatch Agent. IAM Users are required to access the AWS resources. For more information about creating IAM Users, see Create IAM Roles and Users for Use with the CloudWatch Agent (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/create-iam-roles-for-cloudwatch-agent.html#create-iam-roles-for-cloudwatch-agent-users).

3. Install the CloudWatch Agent package on the Access Manager servers. For more information about installing the CloudWatch Agent package on servers see, Installing and Running the CloudWatch Agent on Your Servers (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/install-CloudWatch-Agent-commandline-fleet.html).

4. Specify the AWS IAM credentials and AWS Region using the `aws configure` command. When you run this command, AWS CLI prompts you to specify access key, secret access key, AWS Region, and output format.

   For more information about using the `aws configure` command, see Quickly Configuring the AWS CLI (https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-configure.html#cli-quick-configuration).

5. Create the CloudWatch Agent configuration file with configuration file wizard. The wizard prompts you to specify various details, for example monitoring metrics and log files location. Specify these details based on your requirements.

   For example, to monitor the Identity Server node logs, you must specify the following log file location in the configuration file.

   ```
   /opt/novell/nam/idp/logs/catalina.out
   ```

For more information about creating the configuration file using wizard, see Create the CloudWatch Agent Configuration File with the Wizard (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/create-cloudwatch-agent-configuration-file-wizard.html).

6 Start CloudWatch Agent using the CloudWatch Agent configuration file that you created in the previous step. For example, if the configuration file is saved in the Systems Manager Parameter Store, run the following command:

```
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m onPremise -c ssm:configuration-parameter-store-name -s
```

In the above example command, `-a fetch-config` loads the latest version of the CloudWatch Agent configuration file and -s starts the CloudWatch Agent.

For information about installing the CloudWatch Agent on servers and creating the configuration file, see Installing the CloudWatch Agent on On-Premises Servers (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/install-CloudWatch-Agent-on-premise.html).

7 Log in to AWS Console.

8 Click **Services** and search for the CloudWatch service.

9 In the CloudWatch dashboard, you can find log files under **Logs** and monitoring parameters like CPU and RAM under **Metrics**.

You can install CloudWatch Agent for EC2 instances. For more information, see Installing the CloudWatch Agent on EC2 Instances Using Your Agent Configuration (https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/install-CloudWatch-Agent-on-EC2-Instance-fleet.html).

7 Deploying Access Manager on Microsoft Azure

You can deploy the following Access Manager components as services on Azure:

- Administration Console
- Identity Server
- Access Gateway

NOTE: Deployment of Access Gateway Appliance and Analytics Server is not supported on Azure.

Access Manager supports the following operating systems on Azure:

- SUSE Linux Enterprise Server
- Red Hat Enterprise Linux

This section includes the following topics:

7.1 Prerequisites for Deploying Access Manager on Microsoft Azure

In addition to system requirements of Access Manager components, ensure that you meet the following prerequisites:

- ❒ An administrative account on Azure.
- ❒ A resource group exists in Azure for the administrator.
- ❒ The Access Manager installer (tarball) has been downloaded, extracted, and available for copying to the virtual machines.
- ❒ An SSH key pair.

  This key pair is used for administrative access to the virtual machines over SSH. You can create the key pair by using ssh-keygen or a similar utility.

  For example, `ssh-keygen -t <type> -b <keysize>`

  Supported types include `RSA`, `DSA`, `ECDSA`, and `Ed25519`.The default algorithm is `RSA`. However, the `ECDSA` algorithm is recommended.

  When using `ECDSA`, supported key sizes are 256, 384, and 521.

By default, the resulting files are named as `id_<type>` and `id_<type>.pub`. These files are available in your user accounts' home folder. For example, `/home/devuser/.ssh/`

Remember to check the appropriate permissions on the certificate file by using chmod. For example, `chmod 400 <filename>`.

7.2 Deployment Procedure

The deployment procedure consists of the following steps:

1. Creating Azure Services
2. Creating and Deploying Virtual Machines
3. Configuring Network Security Groups
4. Changing the Private IP Address from Dynamic to Static
5. Installing Access Manager
6. (Optional) Azure Load Balancer

Figure 1-8 in Section 1.6, "Deploying Access Manager on Public Cloud," on page 21 illustrates the recommended way for deploying Access Manager on Azure.

7.2.1 Creating Azure Services

This section outlines general steps for creating Azure services for use with Access Manager.

For more information, see the Azure documentation.

IMPORTANT: While creating services, (such as availability set, virtual network, security groups, instances, and load balancers), ensure to specify the same value for **Location**.

Perform the following steps to create Azure services:

1 Log in to Azure (https://portal.azure.com/).

2 Create or determine an existing **Resource group** for use with Access Manager.

2a In the Azure portal, click **Create a resource**.

2b Search for `resource group` and select **Resource group**.

2c Click **Create**.

For more information about resource groups, see Azure Resource Manager Overview > Terminology > resource group (https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-overview).

NOTE: All administrators may not have rights to create a new resource group.

---

3 Create or determine an existing **Availability Set** for use with Access Manager.

NOTE: If you plan to configure load balancing for Identity Server and Access Gateway, create a separate availability set for each cluster type.

3a In the Azure portal, click **Create a resource**.

3b Search for `availability set` and select **Availability Set**.

3c Click **Create**.

3d Specify values for **Name**, **Subscription**, **Resource group**, and **Location**.

3e Set **Fault domains** and **Update domains** to `2`.

NOTE: Keep the default values as is in other fields.

3f Click **Create**.

4 Create or determine a **Virtual Network** for use with Access Manager.

For this example configuration, all Access Manager components use the same virtual network.

4a In the Azure portal, click **New**.

4b Search for `virtual network` and select **Virtual Network**.

4c Click **Create**.

4d Configure the required network settings, such as Name, Subscription, Resource group, Location, Address Space, Subnet name, and Subnet address range.

The following is an example configuration:

Name: NAM-subnet1
Address space: 10.10.10.0/24
Subnet name: default
Subnet address range: 10.10.10.0/24

4e Click **Create**.

5 Continue with Section 7.2.2, “Creating and Deploying Virtual Machines,” on page 99.

7.2.2 Creating and Deploying Virtual Machines

This section outlines steps to create and deploy virtual machines for a basic setup of Access Manager, which includes an Administration Console, an Identity Server, an Access Gateway, and a user store.

Perform the following steps to create four virtual machines: one for Administration Console, one for Identity Server, one for Access Gateway, and one for the user store.

NOTE: If you are using Azure Active Directory as the user store, deploy virtual machines only for Access Manager components. Azure hosts and manages Azure Active Directory as a service on the cloud.

Perform the following steps to create and deploy a virtual machine:

1 Log in to Azure (https://portal.azure.com/).

2 Click **New** in the upper left pane of the dashboard.

3 In the search bar, search for SLES 12 SP4 or Red Hat Enterprise Linux 7.6 based on the operating system you want to use.

When creating a virtual machine for Active Directory, select a Windows 2016 R2 image instead of SLES or RHEL. For more information about creating a Windows virtual machine, see Quickstart: Create a Windows virtual machine in the Azure portal (https://docs.microsoft.com/en-us/azure/virtual-machines/windows/quick-create-portal).

Each of these operating systems has their own licensing and costs associated with them. With the exception of the BYOS (Bring Your Own Subscription) option, each option includes a valid support license for the operating system.

NOTE: SLES 12 SP4 has been selected here as an example configuration.

4 Select **SLES 12 SP4**.

5 Click **Create**.

6 Configure the following settings in step **1 Basics**:

Field	Description
Name	Specify a name for the virtual machine.
VM disk type	Select **SSD** or **HDD** based on your requirements. This selection affects the list of templates displayed for selection in Step 8.
User name	Specify the name of the account that you want to use for administering the virtual machine. This username is used for ssh access to the virtual machine after deployment.
Authentication type	Select **SSH public key**.
SSH public key	Copy the content of your `id_rsa.pub` file that you have generated earlier, and paste it.
Subscription	Select the Azure subscription that should be used for the virtual machine.
Resource group	Select the resource group that you have created or determined in Step 2.
Location	Select from the list of the supported Azure location where you want to create the virtual machine.

7 Click **OK**.

8 In **2 Size**, click **View all** to see all available templates.

You can filter this list based on disk type, vCPU, and memory.

Each template has its own intended use cases, optimizations, and costs per hour of usage.

Click a template that matches your requirements and the requirements of the Access Manager component that will later be installed on this virtual machine.

NOTE: You must select a virtual machine size of the **Standard** type if you require to configure an Azure load balancer later.

9 Click **Select**.

10 In **3 Settings,** review networking, high availability, storage, and monitoring options by clicking the **>** icon.

Section	Action
High Availability	While deploying a virtual machine for identity Server or Access Gateway, select the appropriate availability set that was created for each type in Step 3. For clustering and load balancing, place Identity Server virtual machines in one availability set and Access Gateway virtual machines in a different availability set.
Storage	keep the default value `Yes` for **Use managed disks**.
Network > **Virtual network**	Click **Virtual network** and select the virtual network that you created in Step 4.
Network > **Public IP Address** (Optional)	Configure the **Public IP Address** for this virtual machine or you can keep the default selection (dynamic addressing). If you do not specify a static address (adds an additional cost), the external IP address used to reach each virtual machine changes with each reboot.
Network > **Network Security Group (firewall)**	Accept the default network security group to allow incoming SSH access requests to the virtual machine used for Access Manager. The instructions to further configure these security groups are in a later section of the guide. In an advanced setup where you install multiple Administration Consoles, Identity Servers, and Access Gateways, these virtual machines should use the security group created for the first virtual machine running that component type.
Extension	Keep the default value.
Auto-shutdown	By default, this is set to `Off`. It is recommended to not set this option to on in a production environment. Enabling this option might result in a corrupted Access Manager setup. If it is necessary to enable **Auto Shutdown**, the system admin must set up a cron job to run several minutes prior to the shutdown time specified on the affected virtual machines. The cron script must be placed in the root user's crontab and it must execute the following commands: 1. `/etc/init.d/novell-idp stop` (on the virtual machine containing Identity Server) 2. `/etc/init.d/novell-ac stop` (on the virtual machine containing Administration Console) This script shuts down Access Manager safely prior to the Azure Auto-Shutdown happens. **IMPORTANT:** Before you manually shut down an Azure virtual machine containing an Access Manager installation, first run the `/etc/init.d/novell-[ac|idp] stop` command. This ensure that the Access Manager instance is in a safe state.

Section	Action
Monitoring	Disable **Boot diagnostics** and **Guest OS diagnostics** if you do not want to monitor for those options. You can change these settings later if you need these functionalities.

11 Click **OK**.

12 In **4 Summary**, review the summary of settings, terms of use, privacy policies, and cost of use.

13 Click **Create**.

Azure begins provisioning the virtual machine as you have configured it. This process may take a few minutes.

14 Verify SSH access to the virtual machine after deployment completes by running the following command:

```
ssh -i <keyfile> <username>@<publicIP>
```

Where,
<keyfile>: The name of the certificate file created with ssh-keygen.
<username>: The **User name** specified in Step 6 on page 100 while deploying the virtual machine.
<publicIP>: The public IP address assigned to the virtual machine. You can view this in the dashboard by clicking the virtual machine.

15 Repeat Step 1 to Step 14 to create additional virtual machines.

16 Continue with Section 7.2.3, “Configuring Network Security Groups,” on page 102.

7.2.3 Configuring Network Security Groups

In the previous section Creating and Deploying Virtual Machines, a separate network security group is created for each virtual machine. You must modify these security groups to open the required incoming ports, depending on the Access Manager component type that will be installed on the virtual machine.

Edit the network security groups for Administration Console, Identity Server, and Access Gateway to configure the ports based on requirements of that component.

For information about the required ports, see Table 1-7, “Administration Console on Cloud,” on page 34, Table 1-8, “Identity Server on Cloud,” on page 34, and Table 1-9, “Access Gateway on Cloud,” on page 35.

1 In the Azure portal, click **All resources**.

You can filter the list can using the fields at the top of the page.

2 Find and click the desired network security group created in Step 10 on page 101.

3 Click **Inbound security rules** > **Add**.

4 Specify details in fields.

The following is an example configuration:

Field	Value
Source	Any

Field	Value
Source port range	*
Destination	Any
Destination port range	8443
Protocol	TCP
Action	Allow
Priority	100
Name	Administration Console HTTPS
Description	HTTPS port for Access Manager Administration Console.

5 Repeat Step 3 and Step 4 for each inbound port rule to be added as listed in Table 1-7, “Administration Console on Cloud,” on page 34, Table 1-8, “Identity Server on Cloud,” on page 34, and Table 1-9, “Access Gateway on Cloud,” on page 35, depending on the component type that will use this network security group.

6 Continue with Section 7.2.4, “Changing the Private IP Address from Dynamic to Static,” on page 103.

7.2.4 Changing the Private IP Address from Dynamic to Static

The private IP addresses of Access Manager virtual machines must be static for proper communications between these devices.

Perform the following steps for each virtual machine:

1 In the Azure portal, click **Virtual machines** > name of the virtual machine.

2 Under **Settings**, click **Networking**.

3 Click the **Network Interface**.

4 In the left menu, click **IP configurations** under **Settings**.

5 Click the IP configuration line.

6 Under **Assignment**, click **Static**.

7 In **IP address**, specify the desired IP address.

8 Click **Save**.

7.2.5 Installing Access Manager

Prerequisites

- ❒ Ensure that you meet the network requirements listed in Network Requirements.
- ❒ Edit the `/etc/hosts` files on each virtual machine and add an entry to resolve its hostname to its private IP address.
- ❒ Ensure that the virtual machines do not have a default firewall configuration that could prevent proper installation and use of the Access Manager components.

❒ Ensure that the required port rules in the network security groups have been created.

See Section 7.2.3, “Configuring Network Security Groups,” on page 102.

Important Points to Consider before Installation

You must know the following points before you start the installation:

- Re-importing Identity Server and Access Gateway is not supported.
- Auto scaling of nodes is not supported. You can add or remove nodes manually. See “Recommendations for Scaling Access Manager Components in Public Cloud” on page 183.

Installation Procedure

Perform the following steps to install Access Manager components on virtual machines:

IMPORTANT: In the following steps, run the Access Manager installation scripts as a `root` user using `sudo`. For example, `sudo sh <script-name>`.

---

1. Copy the `novell-access-manager-<version>.tar.gz` file using Secure Copy (scp) to the virtual machines on which you will install Administration Console and Identity Server.

   The following is a sample scp command that shows how to copy the installer using the SSH key and username specified while creating the virtual machine:

   ```
   scp -i <key> <path/filename_of_tarball> <username>@<vm_ip>:/<path>
   ```

2. Copy the `novell-access-gateway-<version>.tar.gz` file to the virtual machine on which you will install Access Gateway.
3. Install Administration Console, Identity Server, and Access Gateway on respective virtual machines.

   For information about how to install these components, see Section 2.1, “Installing Administration Console on Linux,” on page 43, Section 3.2, “Installing Identity Server on Linux,” on page 56, and Section 4.3.1, “Installing Access Gateway Service on Linux,” on page 75.

   IMPORTANT: While installing Identity Server and Access Gateway, specify the internal IP address of the Administration Console machine. This ensures that communications among machines happen inside the firewall.

   ---

4. Configure Identity Server and Access Gateway.

   For information about how to configure, see “Setting Up a Basic Access Manager Configuration” in the *Access Manager 4.5 Administration Guide*.

7.3 (Optional) Azure Load Balancer

If multiple Access Gateway and Identity Server virtual machines have been created and configured for clustering, you can configure an Azure load balancer for each cluster to balance the load of incoming requests across the clustered machines. A separate load balancer is used for an Identity Server cluster and an Access Gateway cluster.

The following procedures provide the differences in configuration details for Identity Server and Access Gateway load balancer wherever required. Repeat the steps and create separate load balancers for Identity Server and Access Gateway clusters.

Important points to consider before configuring an Azure load balancer for Access Manager:

- ❒ All nodes of a cluster must be deployed in the same availability set. For example, all Identity Server nodes in a cluster are deployed in the same availability set, and all Access Gateway nodes in a cluster are deployed in a different availability set.
- ❒ Separate load balancers are required for Identity Server and Access Gateway.
- ❒ The Configuring a Load Balancer section includes examples assuming that the default ports are used (8080/8443 for Identity Server and 80/443 for Access Gateway). You can use iptables to configure the listeners on Identity Server to use other ports. See Translating Identity Server Configuration Port.
- ❒ Azure load balancer supports HTTP and TCP health check probe. It does not support the HTTPS probe.

  As such, using the Access Gateway heartbeat URL requires additional steps that are covered in the section "To Create a Reverse Proxy for Health Probe" on page 109.

NOTE: For scaling recommendations, see Appendix B, "Recommendations for Scaling Access Manager Components in Public Cloud," on page 183.

7.3.1 Creating a Load Balancer

You must create separate load balancers and configure separate settings, such as IP configuration, backend pool, probes, and rules settings for an Identity Server cluster and for an Access Gateway cluster.

IMPORTANT: Before creating a load balancer for an Access Gateway cluster, complete the steps available in To Create a Reverse Proxy for Health Probe.

Perform the following steps to create a load balancer:

1. In the Azure portal, click **Load balancers**.
2. Click **Add**.
3. Specify the following details:

Field	Description
Name	Specify a name for the load balancer.
Type	Select `Public`.

Field	Description
Public IP address	Create a new public IP address for this load balancer. 1. Click >. 2. Click Create new. 3. Specify a name. 4. Select Static. 5. Click OK.
Subscription	Select the same Azure subscription that you have selected for virtual machines on which Access Manager is installed.
Resource group	Select the same resource group that you have selected for virtual machines on which Access Manager is installed.
Location	Select the same location that you have used for virtual machines.

4 Click **Create**.

5 Continue with "Configuring a Load Balancer" on page 106.

7.3.2 Configuring a Load Balancer

1 In the Azure portal, click **Load balancers**.

2 Click the load balancer that you created in the previous procedure.

3 Configure the following settings:

- Frontend IP configuration
- Backend pools
- Health Probes
- Load balancing rules

Frontend IP configuration

By default, this setting takes the IP address you have configured in **Public IP address** while creating the load balancer.

You can create and select another IP address if you need to change this frontend IP address.

Backend pools

This setting provides a way to associate the load balancer to the IP addresses of virtual machines among which you want to distribute the load.

Perform the following steps to configure backend pools:

1 Click **Backend pools**.

2 Click **Add**.

3 Specify a name.

4 In **Associated to**, select **Availability set**.

5 Select the availability set for which you want to use this load balancer.

   This enables the load balancer to distribute the load among virtual machines available in the selected availability set.

6 Under **Target network IP configuration**, click **Add a target network IP configuration**.

7 In **Target virtual machine**, select the virtual machine that you want to add in the load balancer.

   You can select virtual machines available only in the specified availability set.

8 In **Network IP configuration**, select the related virtual machine.

9 Click **Add a target network IP configuration** to select other virtual machines from the same availability set to be added to the pool.

10 Click **OK**.

Health Probes

The load balancer uses probes to keep track of the health of virtual machines. If a probe fails, the related virtual machine is excluded from the load balancing automatically.

Perform the following steps to configure a health probe:

1 Click **Health probes**.

2 Click **Add**.

3 Specify a name.

4 Specify the following details:

Field	Description
Protocol	Select HTTP.
Port	◆ For **Identity Server** listening on the default ports of 8080/8443, specify `8080`. ◆ For **Access Gateway**, specify the port that you have configured in the reverse proxy for health probe. See "To Create a Reverse Proxy for Health Probe" on page 109. **IMPORTANT:** You must configure these ports in network security groups associated with the respective Access Manager component's cluster.
Path	◆ For **Identity Server**, specify `/nidp/app/heartbeat`. ◆ For **Access Gateway**, specify `/nesp/app/heartbeat`. **IMPORTANT:** An external communication to Access Gateway is typically configured to use HTTPS. Azure load balancer does not support the HTTPS probe. Therefore, when creating a health probe for an Access Gateway cluster, first create a reverse proxy that opens a non-SSL port for the probe URL. See "To Create a Reverse Proxy for Health Probe" on page 109.
Interval	Specify the time after which the load balancer verifies the health of the virtual machine.
Unhealthy threshold	Specify the number. If the health probe fails for the specified number consecutively for a virtual machine, then the load balancer removes it automatically from the load distribution.

5 Click OK.

Load balancing rules

This setting maps the frontend IP address and port combination to the backend IP addresses and port combination associated with virtual machines. You can configure multiple load balancing rules for a load balancer.

Perform the following steps to configure a load balancing rule:

1 Click Load balancing rules.

2 Click Add.

3 Specify the following details:

Field	Description
Name	Specify a name for the rule.
IP Version	Select IPv4.
Frontend IP address	Select the frontend IP address for this rule.
Protocol	Select TCP.
IMPORTANT: If you want the load balancer to handle both HTTP and HTTPS traffic, create a separate rule for both by specifying appropriate ports in Port and Backend port. The port configured in Port and Backend port must match the listening port configured in Identity Server or Access Gateway.	
Port	For Access Gateway, specify the following values: ◆ For HTTPS traffic, specify `443`. ◆ For HTTP traffic, specify `80`. For an Identity Server listening on the default ports of 8080/8443, specify the following values: ◆ For HTTPS traffic, specify `8443`. ◆ For HTTP traffic, specify `8080`.
Backend port	For Access Gateway, specify the following values: ◆ For HTTPS traffic, specify `443`. ◆ For HTTP traffic, specify `80`. For an Identity Server listening on the default ports of 8080/8443, specify the following values: ◆ For HTTPS traffic, specify `8443`. ◆ For HTTP traffic, specify `8080`.
Backend pool	Select the backend pool for this rule.
Health probe	Select the health probe for this rule.
Session persistence	Keep the default value.
Idle timeout	Keep the default value.
Floating IP (direct server return)	Keep the default value.

4 Click OK.

To Create a Reverse Proxy for Health Probe

The port 80 on Access Gateway is reserved for redirects to the SSL port. Configure this reverse proxy to use any other free port.

Perform the following steps to create a reverse proxy for the health probe:

1. Click **Devices** > **Access Gateways** > **Edit** > **Reverse Proxy / Authentication**.
2. Under **Reverse Proxy List**, click **New**, and then specify a name.
3. Change the **Non-Secure Port** to a port that is not already in use by another reverse proxy.
4. Click **New** to create the proxy service.
5. Specify the following details:

Field	Description
Proxy Service Name	Specify a name that identifies the purpose of this proxy service.
Published DNS Name	Specify a value, such as HealthProbe. A value is required, however it is not used for connection purposes.
Web Server IP Address	Specify `127.0.0.1`.
Host Header	Select **Forward Received Host Name**.

6. Click **OK**.
7. On the Reverse Proxy page, click the new proxy service under **Proxy Service List**, and then click **Web Servers**.
8. Change the **Connect Port** value to 9009.

   The service provider (ESP) in Access Gateway that provides the heartbeat service listens on 127.0.0.1:9009.
9. Click **Protected Resources**.
10. Click **New**, specify a name and click **OK**.
11. In **URL Path List**, click /*, and modify the path to contain the following value:

    ```
    /nesp/app/heartbeat
    ```

    This is the path to the heartbeat application.
12. Click **OK** > **OK**.
13. Click **OK** and apply the changes to the configuration.

8 Installing Packages and Dependent RPMs on RHEL for Access Manager

IMPORTANT: You do not need to manually install the RPMs listed in Table 8-1 if the RHEL subscription is available. The install script takes care of installing required RPMs from the RHEL subscription.

Important Points to Consider before Installing RHEL Packages and Dependent RPMs

If you require to manually install the RPMs before the installation, you must consider the following points:

- You must install the RHEL Enterprise Server-with-GUI. Run the `sudo yum groupinstall "Server with GUI"` command to obtain the required RPMs.
- To avoid RPM dependency issues, NetIQ Corporation recommends installing the package along with its respective dependent RPMs. You can also install all packages together in the same sequence as these appear in Table 8-1.
- The version of RPMs varies based on the base operating system version of RHEL. Table 8-1 lists RPMs for RHEL 7.6.
- You must install these RPMs in the same sequence as they appear in Table 8-1.

Table 8-1 *RHEL Packages and Dependent RPMs*

Package	Dependent RPM
iManager	
glibc-2.17-260.el7.i686.rpm	◆ nss-softokn-freebl-3.36.0-5.el7_5.i686 This must be installed along with glibc-2.17-260.el7.i686.rpm. To install these rpm files together, run the following: `rpm -ivh glibc-2.17-260.el7.i686.rpm nss-softokn-freebl-3.36.0-5.el7_5.i686.rpm`
libstdc++-4.8.5-36.el7.i686.rpm These RPMs are required for Administration Console also.	◆ glibc-2.17-260.el7.i686.rpm ◆ libgcc-4.8.5-36.el7.i686.rpm
libstdc++-4.8.5-36.el7.x86_64.rpm (Part of the RHEL base installation)	◆ glibc-2.17-260.el7.x86_64.rpm ◆ libgcc-4.8.5-36.el7.x86_64.rpm
libstdc++-4.8.5-36.el7.i686	◆ glibc-2.17-260.el7.i686 ◆ libgcc-4.8.5-36.el7.i686

Package	Dependent RPM
libstdc++-4.8.5-36.el7.x86_64	◆ libgcc-4.8.5-36.el7.x86_64
libXau-1.0.8-2.1.el7.x86_64.rpm	◆ glibc-2.17-260.el7.i686.rpm
libxcb-1.13-1.el7.x86_64.rpm	◆ glibc-2.17-260.el7.i686.rpm ◆ libXau-1.0.8-2.1.el7.x86_64.rpm
libX11-1.6.5-2.el7.x86_64.rpm	◆ glibc-2.17-260.el7.i686.rpm ◆ libXau-1.0.8-2.1.el7.x86_64.rpm
libXext-1.3.3-3.el7.x86_64.rpm	◆ libX11-1.6.5-2.el7.x86_64.rpm ◆ glibc-2.17-260.el7.i686.rpm
libXi-1.7.9-1.el7.x86_64.rpm	◆ libX11-1.6.5-2.el7.x86_64.rpm ◆ libXext-1.3.3-3.el7.x86_64.rpm ◆ glibc-2.17-260.el7.i686.rpm
libXtst-1.2.3-1.el7.x86_64.rpm	◆ libX11-1.6.5-2.el7.x86_64.rpm ◆ libXext-1.3.3-3.el7.x86_64.rpm ◆ libXi-1.7.9-1.el7.x86_64.rpm ◆ glibc-2.17-260.el7.i686.rpm
libxcb-1.13-1.el7.x86_64.rpm	◆ libXau-1.0.8-2.1.el7.x86_64.rpm
libX11-1.6.5-2.el7.x86_64.rpm	◆ libxcb-1.13-1.el7.x86_64.rpm
libXtst-1.2.3-1.el7.x86_64.rpm	◆ libX11-1.6.5-2.el7.x86_64.rpm ◆ libXi-1.7.9-1.el7.x86_64.rpm ◆ libXext-1.3.3-3.el7.x86_64.rpm
libXrender-0.9.10-1.el7.x86_64.rpm	◆ No dependency
Administration Console	
gettext-0.19.8.1-2.el7.x86_64	◆ No dependency
glibc-2.17-260.el7.i686.rpm	◆ nss-softokn-3.36.0-5.el7_5.x86_64.rpm
libstdc++-4.8.5-36.el7.i686.rpm	◆ glibc-2.17-260.el7.i686.rpm ◆ libgcc-4.8.5-36.el7.i686.rpm
ncurses-libs-5.9-14.20130511.el7_4.i686.rpm	◆ glibc-2.17-260.el7.i686.rpm
libgcc-4.8.5-36.el7.i686.rpm	◆ No dependency
rsyslog-8.24.0-34.el7.x86_64	◆ No dependency
rsyslog-gnutls-8.24.0-34.el7.x86_64	◆ No dependency
binutils-2.27-34.base.el7.x86_64	◆ No dependency
gperftools-libs-2.4-8.el7.x86_64	◆ No dependency
ntp-4.2.6p5-28.el7.x86_64	◆ No dependency

Package	Dependent RPM
Identity Server	
glibc-2.17-260.el7.i686.rpm	◆ nss-softokn-3.36.0-5.el7_5.x86_64
libstdc++-4.8.5-36.el7.i686	◆ glibc-2.17-260.el7.i686.rpm ◆ libgcc-4.8.5-36.el7.i686.rpm
ncurses-libs-5.9-14.20130511.el7_4.i686.rpm	◆ glibc-2.17-260.el7.i686.rpm
libgcc-4.8.5-36.el7.i686.rpm	◆ No dependency
rsyslog-8.24.0-34.el7.x86_64	◆ No dependency
rsyslog-gnutls-8.24.0-34.el7.x86_64	◆ No dependency
binutils-2.27-34.base.el7.x86_64	◆ No dependency
ntp-4.2.6p5-28.el7.x86_64	◆ No dependency
Access Gateway	
glibc-2.17-260.el7.i686.rpm	◆ nss-softokn-freebl-3.16.2.3-14.4.el7.i686
apr-1.4.8-3.el7_4.1.x86_64.rpm	◆ glibc-2.17-260.el7.i686.x86_64.rpm
apr-util-1.5.2-6.el7.x86_64.rpm	◆ apr-1.4.8-3.el7_4.1.x86_64.rpm ◆ glibc-2.17-260.el7.x86_64.rpm
libtool-ltdl-2.4.2-22.el7_3.x86_64.rpm	◆ glibc-2.17-260.el7.x86_64.rpm
unixODBC-2.3.1-11.el7.x86_64.rpm	◆ libtool-ltdl-2.4.2-22.el7_3.x86_64.rpm ◆ glibc-2.17-260.el7.x86_64.rpm
libesmtp-1.0.6-7.el7.x86_64.rpm	◆ glibc-2.17-260.el7.x86_64.rpm
rsyslog-8.24.0-34.el7.x86_64	◆ No dependency
rsyslog-gnutls-8.24.0-34.el7.x86_64	◆ No dependency
binutils-2.27-34.base.el7.x86_64	◆ No dependency
patch-2.7.1-10.el7_5.x86_64.rpm	◆ No dependency
ntp-4.2.6p5-28.el7.x86_64	◆ No dependency

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

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

Use the following command to install a RPM:

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

Use the following command to install all RPMs together:

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

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

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

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

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

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

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

Install RPMs for SNMP after installing RPMs for Administration Console. See "RHEL Packages and Their Dependent RPMs for SNMP" on page 114.

RHEL Packages and Their Dependent RPMs for SNMP

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

- net-snmp-libs-5.7.2-37.el7.x86_64.rpm
- net-snmp-5.7.2-37.el7.x86_64.rpm

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

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

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

2 Run the following commands:

yum install --nogpgcheck net-snmp-libs-5.7.2-37.el7.x86_64.rpm

```
yum install --nogpgcheck net-snmp-5.7.2-37.el7.x86_64
```

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

9 Uninstalling Components

This section provides the required uninstallation steps:

9.1 Uninstalling Identity Server

Uninstalling Identity Server is a two-step process:

1. Removing Identity Server from Administration Console. See Section 9.1.1, “Deleting Identity Server References,” on page 115.
2. Removing the Identity Server software from the Linux or Windows machine. See Section 9.1.2, “Uninstalling the Linux Identity Server,” on page 115 or Section 9.1.3, “Uninstalling the Windows Identity Server,” on page 116.

9.1.1 Deleting Identity Server References

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

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

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

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

4 Update the cluster configuration.

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

6 Continue with Section 9.1.2, “Uninstalling the Linux Identity Server,” on page 115 or Section 9.1.3, “Uninstalling the Windows Identity Server,” on page 116.

9.1.2 Uninstalling the Linux Identity Server

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

1 Unzip the `tar.gz` file by using the following command:

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

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

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

4 Select 2 to uninstall Identity Server.

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

Uninstall removes Identity Server. A log file is created at `/tmp/novell_access_manager/uninstall.log`.

9.1.3 Uninstalling the Windows Identity Server

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

1 Exit any applications and disable any virus scanning programs.

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

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

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

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

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

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

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

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

If the uninstall fails because the primary Administration Console is not available to validate the credentials, see "Uninstalling the Windows Identity Server" on page 116.

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

9.2 Reinstalling an Identity Server to a New Hard Drive

If your Identity Server hard drive fails, you must reinstall Identity Server (see Chapter 3, "Installing Identity Server," on page 55) and leave Identity Server configuration intact in Administration Console. To preserve the existing keystores, perform the following steps before installing Identity Server on the new hard drive.

1 Stop the server.

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

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

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

4 Reinstall Identity Server. (See Chapter 3, "Installing Identity Server," on page 55.)

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

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

7 Click **OK**.

9.3 Uninstalling Access Gateway

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

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

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

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

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

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

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

See Updating Identity Server Configuration in the Access Manager 4.5 Administration Guide.

5 Complete one of the following:

- If you are uninstalling the Windows Access Gateway Service, continue with Section 9.3.1, "Uninstalling Windows Access Gateway Service," on page 117.
- If you are uninstalling the Linux Access Gateway Service, continue with Section 9.3.2, "Uninstalling Linux Access Gateway Service," on page 117.

9.3.1 Uninstalling Windows Access Gateway Service

1 Exit any applications and disable any virus scanning programs.

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

3 Click **Next**.

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

9.3.2 Uninstalling Linux Access Gateway Service

1 Unzip the `tar.gz` file by using the following command:

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

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

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

4 Enter the name of the admin user.

5 Enter the password of the admin user.

Uninstall removes Access Gateway Service. A log file is created at `/tmp/novell_access_manager/uninstall.log`.

9.4 Uninstalling Administration Console

Only the primary version of Administration Console contains the certificate authority. If you uninstall this version, you can no longer use Access Manager for certificate management. You need to promote a secondary console to be the primary console. See Installing Secondary Administration Console in the Access Manager 4.5 Administration Guide.

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

Select the process that corresponds to your platform:

- Section 9.4.1, "Uninstalling Linux Administration Console," on page 118
- Section 9.4.2, "Uninstalling Windows Administration Console," on page 119

9.4.1 Uninstalling Linux Administration Console

1. Unzip the `tar.gz` file by using the following command:

   `tar -xzvf <filename>`
2. Log in as the `root` user or equivalent.
3. At the command prompt of the Access Manager directory, enter the following:

   `./uninstall.sh`

   IMPORTANT: If SLES 12 SP4 has the latest patches from SUSE update channel, run the `systemctl enable ndsd.service` command and then choose option 6.

   ---
4. Specify option 6 to uninstall all products or specify Q to quit without uninstalling.

   You must use option 6 instead of option 1.
5. After running the `./uninstall.sh` script, go to **Auditing** > **Troubleshooting** > **Other Known Device Manager Servers**, then remove the entry for this secondary Administration Console from the servers list.

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

9.4.1.1 Removing Administration Console Replicas

Remove any traces of the Administration Console replicas from the configuration datastore:

1. In Administration Console Dashboard, click *<user name>* at the top right of the page and then click **Configure Console**.
2. Click **Objects**.
3. In the tree view, click **novell**.

4 Delete all objects that reference the failed primary Administration Console. You should find the following types of objects:

- SAS Service object with the hostname of the failed primary console
- An object that starts with the last octet of the IP address of the failed primary console
- DNS AG object with the hostname of the failed primary console
- DNS IP object with the hostname of the failed primary console
- SSL CertificateDNS with the hostname of the failed primary console
- SSL CertificateIP with the hostname of the failed primary console
- NCP server object

5 Run the `/opt/novell/eDirectory/bin/ndsstat -r` command to view the list of available replicas.

6 If you can still see the replica that you deleted from **Other Known Device Manager Servers**, then perform the following steps:

6a Log in to Administration Console as a root user.

6b Change to the `/opt/novell/eDirectory/bin` directory.

6c Run the `ndsrepair -P -Ad` command.

6d Select the replica and click **View replica ring**.

Select the name of the replica that is visible and click **Remove this server from replica ring**.

6e Specify the DN of the admin user in leading dot notation. For example, `.admin.novell`.

6f Specify the password and select **I Agree**.

9.4.2 Uninstalling Windows Administration Console

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

1 Exit any applications and stop any virus scanning programs.

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

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

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

5 Click **Complete Uninstall**, then click **Next**.

6 Restart the machine.

NOTE: Some services are not completely removed. To remove it completely, you must remove few registry settings after restarting the server. For information about removing required registry settings, see "Deleting Services from Registry" on page 120.

9.4.2.1 Deleting Services from Registry

When you uninstall Administration Console by using the steps mentioned in Section 9.4.2, “Uninstalling Windows Administration Console,” on page 119, some service are not deleted. To delete the required services to uninstall Administration Console completely from the machine, perform the following steps:

1. Stop SLP service
2. Back up the registry settings
3. Remove `HKLM>SOFTWARE>Wow6432Node>Apache Software Foundation`
4. Remove `HKLM>SOFTWARE>Novell`
5. Remove `HKLM>SOFTWARE>Wow6432Node>Microsoft>Windows>CurrentVersion\Uninstall>NetIQ iManager`
6. Remove `HKLM>SOFTWARE>Microsoft>Windows>CurrentVersion>App Paths>java.exe`
7. Remove `HKLM>SOFTWARE>Microsoft>Windows>CurrentVersion>Uninstall>NDSonNT`
8. Remove `HKLM>SOFTWARE>Wow6432Node>JavaSoft`
9. Remove `HKLM>SYSTEM>ControlSet001>Services>EventLog>Application>NDS Server`
10. Remove `HKLM>SYSTEM>ControlSet001>Services>NDS Server`
11. Remove `HKLM>SYSTEM>ControlSet001>Services>slpd`
12. Remove `HKLM>SYSTEM>ControlSet001>Services>SNMP>Parameters>ExtensionAgents>Novell.eDir-Snmp.1`
13. Remove `HKLM>SYSTEM>ControlSet001>Services>Tomcat8`
14. Remove `HKLM>SYSTEM>ControlSet002>Services>EventLog>Application>NDS Server`
15. Remove `HKLM>SYSTEM>ControlSet002>Services>NDS Server`
16. Remove `HKLM>SYSTEM>ControlSet002>Services>slpd`
17. Remove `HKLM>SYSTEM>ControlSet002>Services>SNMP>Parameters>ExtensionAgents>Novell.eDir-Snmp.1`
18. Remove `HKLM>SYSTEM>ControlSet002>Services>Tomcat8`
19. Remove all files from the following location:
    - `C:\Program Files (x86)\Novell`
    - `C:\Program Files\Common Files\Novell`
    - `C:\Novell\NDS`
20. Restart the machine.

II Upgrading Access Manager

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

For more information, see "Back Up and Restore" in the *Access Manager 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" in the *NetIQ Access Manager 4.5 Security Guide* .

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

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

1. Administration Console
2. Identity Server
3. Access Gateway
4. (Optional) Analytics Server

Supported Upgrade Paths

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

- 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 Documentation Website (https://www.netiq.com/documentation/access-manager-45/).

Important Points to Consider

- If you have installed additional nodes of Administration Console on other servers for fault tolerance, ensure to first upgrade the primary Administration Console. Else, the directory schema does not get updated.
- Upgrade all nodes of a cluster before you start upgrading another type of device.
- When nodes in a cluster are running on different release versions, you must not change any configuration through Administration Console.

This section includes the following topics:

10 Prerequisites for Upgrading Access Manager

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

 http://www.youtube.com/watch?v=u6l2815jhDM

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. 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:

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

  Windows: `C:\Program Files\Novell\Tomcat\webapps\nidp\WEB-INF\classes\nidpconfig.properties`

  Access Gateway:

  Linux: `/opt/novell/nesp/lib/webapp/WEB-INF/classes/nidpconfig.properties`

  Windows: `C:\Program Files\Novell\Tomcat\webapps\nesp\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 Access Manager 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 Access Manager 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 10.1, “Maintaining Customized JSP Files for Identity Server,” on page 124 or Section 10.2, “Maintaining Customized JSP Files for Access Gateway,” on page 126.
- 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,” on page 41.

10.1 Maintaining Customized JSP Files for Identity Server

Access Manager 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

10.1.1 Using Customized JSP Pages from Access Manager 4.1 or Prior

1. Before upgrade, create a copy of all JSP files inside the `jsp` directory and place the copy somewhere else.

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

   Windows: `\Program Files\Novell\Tomcat\webapps\nidp\jsp`

   WARNING: The upgrade overwrites all existing JSP files.

2. Upgrade Identity Server.
3. Create an empty folder `legacy` in Identity Server

   Linux: `/opt/novell/nids/lib/webapp/WEB-INF/legacy`

   Windows: `\Program Files\Novell\Tomcat\webapps\nidp\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 `jsp` directory.

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

   Windows: `\Program Files\Novell\Tomcat\webapps\nidp\jsp`

5. Refresh the browser to see the changes.

10.1.2 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 `jsp` directory and place the copy somewhere else.

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

   Windows: `\Program Files\Novell\Tomcat\webapps\nidp\jsp`

   WARNING: The upgrade overwrites all existing JSP files.

2. Upgrade Identity Server.
3. Create an empty folder `legacy` in Identity Server

   Linux: `/opt/novell/nids/lib/webapp/WEB-INF/legacy`

   Windows: `\Program Files\Novell\Tomcat\webapps\nidp\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 `jsp` directory.

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

   Windows: `\Program Files\Novell\Tomcat\webapps\nidp\jsp`

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.

10.2 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 `jsp` directory and place the copy somewhere else.

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

Windows: `\Program Files\Novell\Tomcat\webapps\nesp\jsp`

WARNING: The upgrade overwrites all existing JSP files.

---

2 Upgrade Access Gateway.

3 Create an empty folder `legacy` in Access Gateway:

Linux: `/opt/novell/nesp/lib/webapp/WEB-INF/legacy`

Windows: `\Program Files\Novell\Tomcat\webapps\nesp\WEBINF\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 `jsp` directory.

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

Windows: `\Program Files\Novell\Tomcat\webapps\nesp\jsp`

5 Refresh the browser to see the changes.

11 Upgrading Administration Console

11.1 Upgrading Administration Console on Linux

IMPORTANT: If the base operating system is RHEL 7.6, you must first upgrade to Access Manager 4.5, then upgrade to RHEL 7.9.

11.1.1 Upgrading the Evaluation Version to the Purchased Version

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

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

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

Perform the following steps to upgrade the evaluation version to the purchased version:

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

   NOTE: For information about the name of the upgrade file, see the specific Release Notes on the Access Manager Documentation Website (https://www.netiq.com/documentation/access-manager-45/).
4. Change to the directory where you unpacked the file, then enter the following command in a terminal window:

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

```
The following components were installed on this machine

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

6 Type **Y** and press Enter.

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

8 Enter the Access Manager Administration Console user ID.

9 Enter the Access Manager Administration Console password.

10 Re-enter the password for verification.

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

```
Upgrade completed successfully.
```

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

If you encounter an error, see "Troubleshooting Linux Administration Console Upgrade" on page 172.

11.1.2 Upgrading Administration Console

Access Manager by default supports Tomcat 8.5.32 and OpenSSL 1.0.2r. Due to this, Identity Server and Access Gateway disable requests from clients that are on versions lower than TLS1. However, Access Gateway can continue communication with web servers that are on versions lower than TLS1.

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

Perform the following steps to upgrade Administration Console:

NOTE: To prevent security vulnerability, Access Manager uses the jQuery version that is higher than the version used in the earlier release of Access Manager. The higher version of jQuery is not compatible with the Skype for Business 2016 application. Hence, after the upgrade, you cannot log in to Skype for Business 2016 using the Identity Server login page.

If you want to continue using an old version of jQuery, which is less secure, see "Single Sign-on Fails in Skype for Business 2016" in the *Access Manager 4.5 Administration Guide*.

---

1 Back up any customized JSP pages and related files.

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

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

2 Open a terminal window.

3 Log in as the `root` user.

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

NOTE: For information about the name of the upgrade file, see the specific Release Notes on the Access Manager Documentation website (https://www.netiq.com/documentation/access-manager-45/).

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

```
./upgrade.sh
```

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

```
The following components were installed on this machine

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

7 Type **Y** and press Enter.

The system displays a warning message because the latest version of Access Manager uses stronger TLS protocols, ciphers, and other security settings.

If you are using a BTRFS filesystem, the system displays a warning message that the BTRFS filesystem might cause performance issues with the eDirectory database. It is recommended to change the filesystem from BTRFS to any other available filesystem.

For information about moving the existing database from BTRFS filesystem to any other available filesystem, see TID 7022755 (https://www.novell.com/support/kb/doc.php?id=7022755).

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

If you do not want to include the security configurations, then type n. This stops the upgrade.

9 Enter the Access Manager Administration Console user ID.

10 Enter the Access Manager Administration Console password.

11 Re-enter the password for verification.

12 The system displays the following confirmation message:

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

13 Type **Y** and press Enter.

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

```
Upgrade completed successfully.
```

NOTE: If the configuration backup fails, the system displays the following message:

```
The configuration backup failed. Do you want to continue the upgrade
without a backup (y/n)?
```

You can complete the upgrade by typing **Y**. However, the configuration will not have a backup.

15 (Optional) To view the upgrade files:

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

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

If you encounter an error, see Section 17.3, “Troubleshooting Linux Administration Console Upgrade,” on page 172.

11.2 Upgrading Administration Console on Windows

11.2.1 Upgrading the Evaluation Version to the Purchased Version

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

After you have purchased the product, log in to the NetIQ Customer Center (https://www.netiq.com/customercenter) and follow the link that allows you to download the product. Then follow the instructions in Section 11.2.2, “Upgrading Administration Console,” on page 132.

11.2.2 Upgrading Administration Console

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

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: `C:\Program Files\Novell\Tomcat\webapps\nidp\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`

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

Perform the following steps to upgrade Administration Console on Windows:

NOTE: To prevent security vulnerability, Access Manager uses the jQuery version that is higher than the version used in the earlier release of Access Manager. The higher version of jQuery is not compatible with the Skype for Business 2016 application. Hence, after the upgrade, you cannot log in to Skype for Business 2016 using the Identity Server login page.

If you want to continue using an old version of jQuery, which is less secure, see "Single Sign-on Fails in Skype for Business 2016" in the *Access Manager 4.5 Administration Guide*.

---

1. Manually back up your current Access Manager configuration using `ambkup.bat` file. For instructions, see Back Up and Restore in the Access Manager 4.5 Administration Guide.
2. If Administration is installed on the same server, manually back up the JSP pages and related files in the `C:\Program Files\Novell\Tomcat\webapps\nidp\jsp` directory.
3. If you have customized the `tomcat.conf` file or the `server.xml` file, back up these files before upgrading. These files are overwritten during the upgrade process.

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

   ---
4. Run the installation program. When the installation program detects an installed version of Administration Console, it automatically prompts you to upgrade.
5. Read the Introduction, then click **Next**.
6. Accept the License Agreement, then click **Next.**
7. Select the component to upgrade that is currently installed, then click **Next**.
8. Type **Y** and press Enter.

   The system displays an information message to enable Syslog on the Auditing user interface of Administration Console after the upgrade.
9. Type **Y** to continue with the upgrade, then press Enter.
10. At the upgrade prompt, click **Continue.**
11. Specify the following information for the administrator account on Administration Console:

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

    Password and Re-enter Password: Specify and re-enter the password for the administration user account.
12. Decide whether you want the upgrade program to create a backup of your current configuration:
    - If you have a recent backup, click **Continue**. If you choose to not create a backup when you do not have a recent backup and you then encounter a problem during the upgrade, you may be forced to re-create your configuration.
    - If you do not have a recent backup, click **Run Config Backup**. The program creates a backup and stores it in the root of the operating system drive in the `nambkup` directory.
13. Review the summary, then click **Install.**

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

15 When you are prompted, reboot the server.

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

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

17 If Identity Server is installed on the same server, copy any custom login pages to the `C:\Program Files\Novell\Tomcat\webapps\nidp\jsp` directory.

18 Restore any customized files from the backup taken earlier.

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

server.xml

If you have customized the `server.xml` file from the backup taken in 4.4.x, ensure that you apply the same to the new `server.xml` located at `C:\Program Files\Novell\Tomcat\conf\` directory.

An example below shows that the IP address is removed and ciphers added.

```
<Connector NIDP_Name="connector" port="8443" address=""
ciphers="SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA, ...   ../>
```

Tomcat properties:

Go to `C:\Program Files\Novell\Tomcat\bin`. Click the `tomcat8w` file, and make a note of any elements or attributes customized in 4.4.x.

On the 4.5 server, go to `C:\Program Files\Tomcat\bin\tomcat8w`. Change the values and attributes as required.

12 Upgrading Identity Server

12.1 Upgrading Identity Server on Linux

IMPORTANT: If the base operating system is RHEL 7.6, you must first upgrade to Access Manager 4.5, then upgrade to RHEL 7.9.

12.1.1 Upgrading the Evaluation Version to the Purchased Version

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

After you have purchased the product, log in to the NetIQ Customer Center and follow the link that allows you to download the product.

Use the following procedure to upgrade stand-alone Identity Server. If you have installed both Identity Server and Administration Console on the same machine, see “Upgrading the Evaluation Version to the Purchased Version” on page 129.

NOTE: If you have modified the JSP file to customize the login page, logout page, and error messages, you can restore the JSP file after installation. You should sanitize the restored JSP file to prevent XSS attacks. For more information, see Preventing Cross-site Scripting Attacks in the Access Manager 4.5 Administration Guide.

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

   NOTE: For information about the name of the upgrade file, see the specific Release Notes on the Access Manager Documentation website (https://www.netiq.com/documentation/access-manager-45/).
4. Change to the directory where you unpacked the file, then enter the following command in a terminal window:

   ```
   ./upgrade.sh
   ```

5 The system displays the following confirmation message:

```
The following components were installed on this machine

1. Identity Server

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

6 Type **Y** and press Enter.

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

8 Enter the Access Manager Administration Console user ID.

9 Enter the Access Manager Administration Console password.

10 Re-enter the password for verification.

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

```
Upgrade completed successfully.
```

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

NOTE: If OAuth and OpenID Connect protocol is enabled, then after upgrading all members of Identity Server cluster, 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 Access Manager 4.5 Administration Guide.

12.1.2 Upgrading Identity Server

Use the following procedure to upgrade stand-alone Identity Server. If you have installed both Identity Server and Administration Console on the same machine, see "Upgrading Administration Console" on page 130.

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

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

NOTE: To prevent security vulnerability, Access Manager uses the jQuery version that is higher than the version used in the earlier release of Access Manager. The higher version of jQuery is not compatible with the Skype for Business 2016 application. Hence, after the upgrade, you cannot log in to Skype for Business 2016 using the Identity Server login page.

If you want to continue using an old version of jQuery, which is less secure, see "Single Sign-on Fails in Skype for Business 2016" in the *Access Manager 4.5 Administration Guide*.

---

1 Back up any customized JSP pages and related files.

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

2 Open a terminal window.

3 Log in as the `root` user.

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

NOTE: For information about the name of the upgrade file, see the specific Release Notes on the Access Manager Documentation website (https://www.netiq.com/documentation/access-manager-45/).

---

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

```
./upgrade.sh
```

6 The system displays the following confirmation message:

```
The following components were installed on this machine

1. Identity Server

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

7 Type **Y** and press Enter.

The system displays two warning messages. The first message is for backing up all JSPs before proceeding with the upgrade, and the next is for including security settings.

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

If you do not want to include the security configurations, then type n. This stops the upgrade.

9 Enter the Access Manager Administration Console user ID.

10 Enter the Access Manager Administration Console password.

11 Re-enter the password for verification.

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

```
Upgrade completed successfully.
```

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

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

- `/opt/novell/nam/idp/conf/server.xml`

  Also, add the following line to the server.xml file:

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

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

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

Important Notes:

- If you are using Kerberos and you have renamed `nidpkey.keytab` and `bcsLogin.conf` with any other name, ensure that you modify the `upgrade_utility_functions.sh` script located in the `novell-access-manager-x.x.x.x-xxx/scripts` folder with these names before upgrading Access Manager.
- If you have customized the Java settings in the `/opt/novell/nam/idp/conf/tomcat.conf` file, then after the upgrade, you must copy the customized setting to the new file.
- If you have modified the JSP file to customize the login page, logout page, and error messages, you can restore the JSP file after installation. You should sanitize the restored JSP file to prevent XSS attacks. For more information, see Preventing Cross-site Scripting Attacks in the Access Manager 4.5 Administration Guide.

12.2 Upgrading Identity Server on Windows

12.2.1 Upgrading the Evaluation Version to the Purchased Version

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

After you have purchased the product, log in to the NetIQ Customer Center (https://www.netiq.com/customercenter) and follow the link that allows you to download the product. Then follow the instructions in Section 11.2.2, “Upgrading Administration Console,” on page 132.

12.2.2 Upgrading Identity Server

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

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

NOTE: To prevent security vulnerability, Access Manager uses the jQuery version that is higher than the version used in the earlier release of Access Manager. The higher version of jQuery is not compatible with the Skype for Business 2016 application. Hence, after the upgrade, you cannot log in to Skype for Business 2016 using the Identity Server login page.

If you want to continue using an old version of jQuery, which is less secure, see "Single Sign-on Fails in Skype for Business 2016" in the *Access Manager 4.5 Administration Guide*.

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

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

2. If you have customized the `tomcat.conf` file or the `server.xml` file at `C:\Program Files (x86)\Novell\Tomcat\conf\`, back up these files before upgrading. The registries and the file are overwritten during the upgrade process.
3. Download and run `AM_45_AccessManagerService_Win64.exe` file from NetIQ.

   This file starts the installation program. When the program detects an installed version of Identity Server, it automatically prompts you to upgrade.
4. On the Introduction page, click **Next.**
5. Accept the License Agreement.
6. At the upgrade prompt, click **Continue**.
7. Type **Y** and press Enter.

   The system displays an information message to enable Syslog after the upgrade.
8. Type **Y** to continue with the upgrade, then press Enter.
9. Specify the following information for Administration Console:

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

   Password and Re-enter Password: Specify and re-enter the password for the administration user account.
10. If you have customized login pages, decide whether you want your customized pages restored automatically. Be aware that any new feature introduced in the JSP files that have the same name as your files are lost when your file overwrites the installed file with the automatic restore.

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

    NOTE: Ensure that you sanitize the restored customized JSP file to prevent XSS attacks. For more information about how to sanitize the JSP file, see Preventing Cross-site Scripting Attacks in the Access Manager 4.5 Administration Guide.
11. Review the summary, then click **Install**.

NOTE: If OAuth and OpenID Connect protocol is enabled, then after upgrading all members of Identity Server cluster, you must update the Identity Server 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 Access Manager 4.5 Administration Guide.

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

```
C:\Program Files\Novell\log\AccessManagerServer_ InstallLog.log
```

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

14 Restore any customized files from the backup taken earlier.

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

server.xml

If you have customized the `server.xml` file from the backup taken in 4.4.x, ensure that you apply the same to the new `server.xml` located at `C:\Program Files\Novell\Tomcat\conf\` directory.

Also, add the following line to the `server.xml` file to use the new features on the user portal:

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

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

Tomcat properties:

Go to `C:\Program Files\Novell\Tomcat\bin\tomcat7w`. Double-click the `tomcat7w` file and make a note of any elements or attributes customized in 4.4.x.

On the 4.5 server, go to `C:\Program Files\Tomcat\bin\tomcat8w`. Change the values and attributes as required.

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

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

13 Upgrading Access Gateway

13.1 Upgrading Access Gateway on Linux

IMPORTANT: If the base operating system is RHEL 7.6, you must first upgrade to Access Manager 4.5, and then upgrade to RHEL 7.9.

13.1.1 Upgrading the Evaluation Version to the Purchased Version

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

After you have purchased the product, log in to the NetIQ Customer Center and follow the link that allows you to download the product.

Perform the following procedures to upgrade from the evaluation version to the purchased version:

13.1.1.1 Upgrading Access Gateway Appliance

From Access Manager 4.5 onwards, the format of the Access Gateway Appliance installer is changed to OVF. Therefore instead of a regular upgrade, you must migrate to the latest Access Gateway Appliance. For information about how to migrate, see Section “Migrating Access Gateway Appliance Setup” on page 144.

13.1.1.2 Upgrading Access Gateway Service

Perform the steps provided in Section 13.1.2.3, “Upgrading Access Gateway Service,” on page 150.

13.1.2 Upgrading Access Gateway

13.1.2.1 Upgrading Access Gateway Appliance

Upgrading from Access Gateway Appliance 4.4.*x*

Access Gateway Appliance is packaged as an OVF installer. Therefore if you are using Access Gateway Appliance 4.4 Service Pack 4 Hotfix 1 or earlier supported versions, you must migrate to latest version of Access Gateway Appliance. For information about how to migrate, see Section "Migrating Access Gateway Appliance Setup" on page 144.

If you are using Access Gateway appliance 4.4, ensure to upgrade to any of the following supported upgrade versions of Access Gateway Appliance before migrating to the latest version:

- 4.4 Service Pack 4 Hotfix 1
- 4.4 Service Pack 4
- 4.4 Service Pack 3
- 4.4 Service Pack 2

For information about upgrading from 4.4 to any of the supported upgrade version of Access Gateway, see Upgrading Access Gateway Appliance in the NetIQ Access Manager 4.4 Installation and Upgrade Guide (https://www.netiq.com/documentation/access-manager-44/install_upgrade/data/bookinfo.html).

NOTE: All versions of Access Gateway Appliance 4.4.x do not support a direct upgrade to the latest version. For the supported upgrade paths, see the release specific Release Notes.

Upgrading from Access Gateway Appliance 4.5

NOTE: You can use the latest upgrade file to upgrade from 4.5 to the latest version of Access Gateway Appliance.

If you are using Access Gateway Appliance 4.4 Service Pack 4 Hotfix 1 or earlier supported versions, see "Upgrading from Access Gateway Appliance 4.4.*x*" on page 142.

Upgrading the base Operating System and Common Appliance Framework

You must update the base Operating System and CAF before upgrading Access Gateway Appliance to the 4.5.2 version. Perform the following steps:

NOTE: Ignore **Product Upgrade** notifications if you are on Access Manager 4.5.x release version. For operating system updates, click **Online Update**. For Access Gateway release updates, click **Product Upgrade**. Click **Product Upgrade** only if you want to upgrade from Access Manager 4.5.x to 5.0.x release version.

---

1. Log in to the Configuration console (`https://<access_gateway_appliance-IP address>:9443`) as a `root` user.
2. Click **Online Update**.
3. Click **Update Now** to apply all patches.

NOTE: Some of the updates might require rebooting Access Gateway Appliance. It is recommended to reboot Access Gateway Appliance in the following scenarios:

- When Configuration console displays the **Reboot Needed** option in the upper right corner of the Appliance Configuration pane.
- When Configuration console displays a message or a warning to reboot.

4 Click **Product Upgrade** > **Start**.

5 Review and accept the License Agreement.

6 Register for the Online Update Service. For registering for the Online Update Service, see "To register for the Online Update Service:" on page 158.

7 Click **OK** to install all the required updates.

8 In the upper right corner of the Appliance Configuration pane, click **Reboot**.

Verifying the version of the base Operating System and Common Appliance Framework

(Applicable for upgrading Access Gateway Appliance to 4.5.2)

1 Open a terminal window and log in as the `root` user.

2 Use the following command to check the Operating System version:

```
cat /etc/os-release
```

Ensure that the version is SLES 12 SP4.

3 Use the following command to check the CAF version:

```
cat /etc/Novell-VA-base
```

Ensure that the version is 2.0.3.

Steps to upgrade from 4.5 to the latest version of Access Gateway Appliance:

1 Back up any customized JSP pages and related files.

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

2 Open a terminal window.

3 Log in as the `root` user.

4 Download the upgrade file from dl.netiq.com or from your purchased build, and then extract the `tar.gz` file using the following command:

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

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

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

```
./ma_upgrade.sh
```

6 A warning message regarding backup and restore is displayed followed by the message for including security settings.

If you have customized any files, take a backup and restore them after installation.

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

If you do not want to include the security configurations, then type n. This stops the upgrade.

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

9 Enter the Access Manager Administration Console user ID.

10 Enter the Access Manager Administration Console password

11 Re-enter the password for verification

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

```
Upgrade completed successfully.
```

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

- `/opt/novell/nam/mag/webapps/nesp/WEB-INF/web.xml`
- `/opt/novell/nam/mag/webapps/nesp/jsp`
- `/opt/novell/nam/mag/webapps/nesp/html`
- `/opt/novell/nam/mag/webapps/nesp/images`
- `/opt/novell/nam/mag/webapps/agm/WEB-INF/config/current`
- `/opt/novell/nam/mag/webapps/nesp/config`
- `/opt/novell/devman/jcc/scripts/presysconfig.sh`
- `/opt/novell/devman/jcc/scripts/postsysconfig.sh`

13.1.2.2 Migrating Access Gateway Appliance Setup

In migration, you install the latest version of Access Gateway Appliance on a new server, and then migrate the existing data to the new server.

During the migration process, you can either provide a new IP address and host name or reuse an existing IP address and host name.

Prerequisites

In addition to the Section 4.2.1, “Prerequisites for Installing Access Gateway Appliance,” on page 69, ensure that the following prerequisites are met before migrating Access Gateway Appliance:

- You have completed upgrading all instances of Administration Console and Identity Server before migrating the Access Gateway Appliance.

- (If the services are managed by an L4 switch) You have removed the device that needs to be migrated from the L4 switch. This prevents the L4 switch from sending the request of the users to that device during migration.

  Add the device to the L4 switch after the migration is complete.

- The upgrade path mentioned in the Release Notes applies to the migration path of Access Gateway Appliance. Ensure that you are migrating Access Gateway Appliance from 4.4 Service Pack 2 (4.4 SP2) or later to the latest version.

  If you have older versions prior to the Access Gateway Appliance 4.4 Service Pack 2, first upgrade from a supported upgrade path to 4.4 Service Pack 2 using the instructions at Upgrading Access Gateway Appliance (https://www.netiq.com/documentation/access-manager-44/install_upgrade/data/bzcvoqm.html#bzj208d) in the Access Manager 4.4 Installation and Upgrade Guide (https://www.netiq.com/documentation/access-manager-44/install_upgrade/data/bookinfo.html).

- (For using an existing IP address) You have backed up customized files, if any.

  It is important to take the backup of the customized files if you are reusing the same IP address.

  Take a backup of the following files if these are customized:

  - `/opt/novell/nam/mag/conf/server.xml`
  - `/opt/novell/nam/mag/conf/tomcat.conf`
  - `/opt/novell/nam/mag/conf/web.xml`
  - `/opt/novell/nesp/lib/webapp/WEB-INF/web.xml`
  - `/opt/novell/nam/mag/webapps/nesp/jsp/`
  - `/opt/novell/nam/mag/webapps/nesp/images/`
  - `/opt/novell/nam/mag/webapps/agm/WEB-INF/config/current/ErrorPagesConfig.xml`
  - `/etc/opt/novell/apache2/conf/extra/httpd-multilang-errordoc.conf`
  - `/opt/novell/apache2/share/apache2/error/include/top.html`
  - `/opt/novell/apache2/share/apache2/error/include/bottom.html`
  - `/opt/novell/apache2/share/apache2/error/images/`

- (For using new IP address) Adding the new Access Gateway Appliance in the existing cluster restores the files mentioned in the **Settings** tab of **Code Promotion** on Administration Console. If code promotion was performed earlier to get the existing version, a custom file cache is pushed instead of the files mentioned in the **Settings** tab.

  If you have customized the `server.xml` and the `web.xml` files, ensure to take a back up of those files because these files are not restored automatically.

- (For using existing IP address) Make a note of the IP address and the host name (with the domain name such as, *`server.domain.com`*) of the existing Access Gateway Appliance before migrating to the latest Access Gateway Appliance. The IP address that the existing Access Gateway Appliance uses to communicate with Administration Console will be used for installing the new Access Gateway Appliance.

- (For using existing IP address) The number of network interfaces along with their values are same for both the new Access Gateway Appliance and the existing Access Gateway Appliance.

- You have physical access to the server or server console (in case of VMWare setups) as a root user.

- The required ports are opened in the firewall. For more information about ports, see Section 1.8, “Setting Up Firewalls,” on page 28.
- Determine if you want to reuse your existing IP address or use a new IP address to setup the system.
- Verify if you have configured any Access Gateway advanced option that refers to a non-default folder in the file system. If yes, you must manually create the folders with the same name before migrating a new Access Gateway Appliance.

  For example, if you have configured the `CoreDumpDirectory` option as `CoreDumpDirectory /data/cores`, then before migrating Access Gateway Appliance, create the /data/cores folder.

Migrating Access Gateway Appliance

Migrating the existing Access Gateway Appliance to new Access Gateway Appliance will not cause any disruption to the existing setup. You can add new Access Gateway Appliance nodes into the existing Access Gateway Appliance cluster. They can co-exist, but it is recommended to replace all the existing nodes to the latest version.

You can select any one of the following approaches to migrate to Access Gateway Appliance 4.5:

- “Using the Existing IP Address” on page 146
- “Using a New IP Address” on page 147

Using the Existing IP Address

Workflow:

1. Back up any files that you have customized and note down the IP address and host name of the existing Access Gateway Appliance.
2. Shut down the existing Access Gateway Appliance.
3. Install Access Gateway Appliance with the IP address and host name noted in Step 1.
4. Restore any customized files from the backup taken earlier.

Use case:

You are upgrading Access Manager 4.4 Service Pack 2 (4.4 SP2) to Access Manager 4.5. After upgrading Administration Console and Identity Server to 4.5 version, you require to migrate Access Gateway Appliance to the 4.5 version using the existing IP address.

This scenario assumes that you have a server with the system requirements as mentioned at *NetIQ Access Manager System Requirements* to install the new Access Gateway Appliance.

Consider that the setup includes the following components:

- Access Manager 4.5 Administration Console (primary Administration Console: AC 1)
- Access Manager 4.5 Identity Server cluster (primary Identity Server: IDP 1 and secondary Identity Server: IDP 2)
- Access Manager 4.4 SP2 Access Gateway Appliance cluster (primary Access Gateway: AG 1 and secondary Access Gateway: AG 1, AG 2 and A G 3)

Migration process:

1 If you are first migrating AG 2 using the existing IP address of AG 2, ensure you do the following:

1a Shut down AG 2

1b Ensure that you have met the "Prerequisites" on page 144.

2 Install the Access Gateway Appliance (newAGA 2) with the same IP address and hostname as of the 4.4 SP2 Access Gateway Appliance (AG 2). For information about installing the new Access Gateway Appliance, see Section 4.2, "Installing Access Gateway Appliance," on page 68.

After the installation is complete, the configuration sync up takes some time. Do not modify any configuration during this time.

When the configuration is synced up, the health of this Access Gateway Appliance and the other members of the cluster turn green.

NOTE: After the installed Access Gateway Appliance turns green, it is recommended to migrate all the other members of Access Gateway Appliance to Access Gateway Appliance 4.5 before applying the changes by using the update option in Administration Console.

---

3 Restore any customized files that you backed up earlier as part of "Prerequisites" on page 144.

server.xml: If you have modified any elements or attributes in the 4.4 Service Pack 2 environment, the corresponding changes will need to be applied to the `/opt/novell/nam/mag/conf/server.xml` file of the new Access Gateway Appliance.

Typical changes done to the `server.xml` in 4.4 SP2 include modifying the 'Address=' attribute to restrict the IP address the application will listen on, or 'maxThreads=' attribute to modify the number of threads.

In the following example, 4.4 SP2 has customized `maxThreads` value.

```
<Connector port="9029" enableLookups="false"  protocol="AJP/1.3"
address="127.0.0.1" minSpareThreads="25" maxThreads="300" backlog="0"
connectionTimeout="20000", ...   ../>
```

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

4 Test the Access Gateway Appliance functionality by accessing Access Gateway protected resources and ensuring that pages are rendered successfully.

5 Repeat Step 1 through Step 4 until you have completely migrated all the existing 4.4 SP2 Access Gateway Appliance (AG 1 and AG 3) to Access Gateway Appliance 4.5.

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

Using a New IP Address

Workflow:

1 Back up any files that you have customized.

2 Install the new Access Gateway Appliance.

For information about installing the new Access Gateway Appliance, see Section 4.2, "Installing Access Gateway Appliance," on page 68.

3 Restore the customized files from the backup taken earlier.

Use case

You are upgrading Access Manager 4.4 SP2 to Access Manager 4.5. After upgrading Administration Console and Identity Server to 4.5 version, you require to migrate Access Gateway Appliance to the 4.5 version using the new IP address.

This scenario assumes that you have a server with the system requirements as mentioned at *NetIQ Access Manager System Requirements* to install the new Access Gateway Appliance.

Consider that the setup includes the following components:

- Access Manager 4.5 Administration Console (primary Administration Console: AC 1)
- Access Manager 4.5 Identity Server cluster (primary Identity Server: IDP 1 and secondary Identity Server: IDP2)
- Access Manager 4.4 SP2 Access Gateway Appliance cluster (primary Access Gateway: AG 1 and secondary Access Gateway: AG 2).

Migration process:

1 Determine the primary server in the 4.4 SP2 Access Gateway cluster.

In this scenario, AG 1 is the primary server. To verify which is the primary server in your set up, perform the following:

1a Log in to Administration Console.

1b Click **Devices > Access Gateways**, and select the cluster.

The primary server is indicated by a red mark beside the IP address.

2 Install the new Access Gateway Appliance (newAGA 1). For more information, see Section 4.2, “Installing Access Gateway Appliance,” on page 68.

After the installation, you must configure Access Gateway Appliance to specify the IP address of Administration Console (AC 1), user name, and password in the **Administration Console Configuration** field on the Appliance Configuration page.

3 Add the newly installed Access Gateway Appliance to the existing Access Gateway Appliance 4.4 Service Pack 2 cluster.

4 By default, all proxy services of newly added devices to the cluster listen on the same IP address and port. To configure each reverse proxy service to a specific IP address and port, perform the following steps:

4a Configure a primary IP Address in YaST for the remaining interfaces.

4a1 Go to `YaST > Network Devices > Network Settings > Overview`.

4a2 Select the network card and click **Edit**.

4a3 Specify the IP address.

Repeat the steps for all the interfaces.

4b Click **Devices** > **Access Gateways**, and select the device.

4c Click **New IP > OK**.

4d Add the secondary IP address, if applicable, to the interfaces from **Network Settings** > **Adapter List**.

4e Configure the DNS in **Network Settings** > **DNS**.

4f Add the Host entries (if any) in **Network Settings** > **Hosts**.

4g Set up the routing (if any) in **Network Settings** > **Gateways**.

4h Under Services, click **Reverse Proxy/Authentication**. In the **Reverse Proxy List**, click the proxy service name. Select the newly added cluster member and select the **listening IP address** for that service.

(Optional) If you want to specify the outbound connection to the web server, click **Web Servers > TCP Connect Options**. Select the **Cluster Member** and select the IP address from the list against **Make Outbound Connection Using** if you want to select the outbound IP address to communicate with the web server.

4i Restore any customized files that you backed up earlier as part of "Prerequisites" on page 144.

The files mentioned in Administration Console at ***<username>*** **> Code Promotion > Settings** get restored automatically:

Copy the content of the `server.xml` file to the corresponding file in the new location.

Typical changes done to the `server.xml` in 4.4 SP2 include modifying the '`Address=`' attribute to restrict the IP address the application will listen on, or '`maxThreads=`' attribute to modify the number of threads.

server.xml: If you have modified any elements or attributes in the 4.4 SP2 environment, the corresponding changes will need to be applied to the `/opt/novell/nam/mag/conf/server.xml` file of the new Access Gateway Appliance.

In the following example, 4.4 SP2 contains `maxThreads` value.

```
<Connector port="9009" enableLookups="false" redirectPort="8443"
protocol="AJP/1.3" address="127.0.0.1" minSpareThreads="25"
maxThreads="300" backlog="0" connectionTimeout="20000", ...   ../>
```

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

5 Test the Access Gateway Appliance functionality by accessing Access Gateway protected resources and ensuring that the pages are rendered successfully.

6 On the Administration Console, specify AGA 1 as the primary server and click **Update**.

7 Remove 4.4 SP2 Access Gateway Appliance (AG 1) from the cluster.

8 Install new Access Gateway Appliance (AGA 2) as in Step 2 and add it to the 4.4 SP2 Access Gateway Appliance cluster as in Step 3.

9 After you confirm that all the services are running remove 4.4 SP2 Access Gateway Appliance (AG 2) from the cluster.

10 Click **OK > Update all**.

11 Repeat Step 2 to Step 5 until you migrate all existing Access Gateway Appliance from 4.4 Service Pack 2 to 4.5.

After installing Access Gateway Appliance, delete all 4.4 SP2 Access Gateway Appliances from Administration Console.

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

13.1.2.3 Upgrading Access Gateway Service

Prerequisites

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

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

IMPORTANT: (Applicable for RHEL) When more than 60 proxy services are configured, Apache fails to start after upgrade. RHEL has 128 semaphore arrays by default which is inadequate for more than 60 proxy services. Apache 2.4 requires a semaphore array for each proxy service.

You must increase the number of semaphore arrays depending on the number of proxy services you are going to use. Perform the following steps to increase the number of semaphore arrays to the recommended value:

1. Open `/etc/sysctl.conf`
2. Add `kernel.sem = 250 256000 100 1024`

   This creates the following:

   Maximum number of arrays = 1024 (number of proxy services x 2)

   Maximum semaphores per array = 250

   Maximum semaphores system wide = 256000 (Maximum number of arrays x Maximum semaphores per array)

   Maximum ops per semop call = 100
3. Use command `sysctl -p` to update the changes
4. Start Apache.

Process

1. Download the `AM_45_AccessGatewayService_Linux_64.tar.gz` file from the NetIQ download site and extract it by using the following command:

   ```
   tar -xzvf <AM_45_AccessGatewayService_Linux_64.tar.gz>
   ```

2. Run the `ag_upgrade.sh` script from the folder to start the upgrade.
3. Specify the following information:

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

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

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

   ```
   Starting Access Manager services...
   Backup of customized files are available at /root/nambkup. Restore them
   if required.
   ```

4. View the log files. The install logs are located in the `/tmp/novell_access_manager/` directory.
5. Restore any customized files from the backup taken earlier as part of steps in "Prerequisites" on page 150.

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

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

server.xml:

If you have modified any elements or attributes in the 4.4.x environment the corresponding changes will need to be applied to the 4.5 `server.xml` file.

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

In the following example, 4.4.x has customized `maxThreads` value.

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

Make a note of the customizations and copy paste the changed values in the 4.5 `server.xml` file

tomcat.conf:

Copy any elements or attributes that you have customized in the `tomcat8.conf` file to the `tomcat.conf` file.

For example, if you have included the environment variable to increase the heap size by using -Xmx/Xms/Xss attributes in the `tomcat8.conf` file, copy this variable to the 4.5 `/opt/novell/nam/idp/conf/tomcat.conf` file.

6 Modify the required properties in `/opt/novell/nam/mag/webapps/agm/WEB-INF/agm.properties` using back up file `/root/novell_access_manager/agm/agm.properties`. If you have customized the `agm.properties` file from the backup taken in 4.4.x, ensure that you apply the same to the new 4.5 `/opt/novell/nam/mag/webapps/agm/WEB-INF/agm.properties` file. An example below shows the how to enable the backend webserver's web page caching and the cache location.

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

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

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

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

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

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

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

13.2 Upgrading Access Gateway Service on Windows

13.2.1 Upgrading the Evaluation Version to the Purchased Version

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

After you have purchased the product, log in to the NetIQ Customer Center (https://www.netiq.com/customercenter) and follow the link that allows you to download the product. Then follow the instructions in Section 13.2.2, “Upgrading Access Gateway Service,” on page 152.

13.2.2 Upgrading Access Gateway Service

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

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

IMPORTANT: Windows packages KB2919442 and KB2919355 must be installed before upgrading Access Gateway Service. These packages must be installed in the same sequence. You can verify if these packages are installed by using the following commands:

- `dism /online /get-packages | findstr KB2919442`
- `dism /online /get-packages | findstr KB2919355`

If these packages are installed, you will get a confirmation message. If the packages are not installed, you will not receive any response.

1. Download and run `AM_44_AccessGatewayService_Win64.exe` file from NetIQ.
2. Run the installation program. When the installation program detects an installed version of Access Gateway, it automatically prompts you to upgrade.
3. Answer `Yes` to the prompt to upgrade.
4. Read the Introduction, then click **Next.**
5. Review the Readme information, then click **Next**.
6. Accept the License Agreement, then click **Next.**
7. Specify the following information:

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

   Password and Re-enter Password: Specify the password and re-enter the password for the administration user account.
8. Review the installation summary, then click Install.

   Access Gateway Service is upgraded.
9. View the log files. The install logs are located in the `C:\Program Files\Novell\log` and `C:\agsinstall.log` directories.
10. Restore any customized files from the backup taken earlier.

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

    server.xml:

    If you have customized the `server.xml` file from the backup taken in 4.4.x, ensure that you apply the same to the new `server.xml` located at `C:\Program Files\Novell\Tomcat\conf\` directory.

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

    Tomcat properties:

    Go to `C:\Program Files\Novell\Tomcat\bin`. Click the `tomcat8w` (for 4.4.x) file and make a note of any elements or attributes that are customized.

    On the 4.4 server, go to `C:\Program Files\Novell\Tomcat\bin\tomcat8w`. Change the values and attributes as required.
11. Restart the tomcat server by using the Windows service. Go to **Start** > **Control Panel** > **System and Security** > **Administrative Tools** > **Services**.

14 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 *Access Manager 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.

---

15 Getting the Latest OpenSSL Updates for Access Manager

The OpenSSL open source project team regularly releases updates to known OpenSSL vulnerabilities. Access Gateway and Analytics Server use the OpenSSL library for cryptographic functions. It is recommended that you keep Access Gateway 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 Gateway 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 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.

15.1 Installing or Updating Security Patches for 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 4.4 Installation and Upgrade Guide.

15.2 Installing or Updating Security Patches for Access Gateway Appliance

Use the **Online Update** option to register to the online update service from the Software Licenses and Downloads portal. It will get you the latest security updates for Access Gateway Appliance. You can select to install updates automatically or manually.

If you want to control the updates further, you can configure Access Gateway Appliance to get the updates from a local Subscription Management Tool (SMT). This allows you to download the updates to a single SMT server in your network and all other nodes of Access Gateway Appliance receive updates from this server. For more information, see *Subscription Management Tool Guide*. To obtain the proper credentials to use the SMT server, see "Mirroring Credentials" in the *Subscription Management Tool Guide*.

To activate the Update Channel, you must obtain the key from the Customer Center. If the key is not available, contact the Customer Center through an email.

WARNING: Before performing the online update, ensure to add rules in the firewall to allow https traffic to the URLs such as nu.novell.com and secure-www.novell.com.

For more information about configuring the firewall and ports, see Setting Up Firewalls.

To register for the Online Update Service:

1. Log in to the Configuration console (`https://<access_gateway_appliance-IP address>:9443`) as the `root` user.
2. Click **Online Update**.
3. If the Registration dialog does not open automatically, click the **Register** tab.
4. Select the **Service Type**:
   - Local SMT (Proceed with Step 5.)
   - Micro Focus Customer Center (Proceed with Step 6.)
5. (Local SMT) Specify the following information for the SMT server, then continue with Step 7.
   - Hostname such as `smt.example.com`
   - (Optional) SSL certificate URL that communicates with the SMT server
   - (Optional) Namespace path of the file or directory
6. (Customer Center) Specify the following information about the Customer Center account for Access Gateway Appliance:
   - Email address of the account in Customer Center
   - Activation key (the same Full License key that you used to activate the product)
   - Allow data send (select any of the following) to share information with the Customer Center:
     - Hardware Profile
     - Optional information
7. Click **Register**.

Wait while Access Gateway Appliance registers with the service.

8 Click **OK**.

After completing the registration, you can view the lists of needed and installed updates.

Performing post-registration actions:

- **Update Now:** Click **Update Now** to activate the downloaded updates.

  NOTE: Some of the updates might require rebooting Access Gateway Appliance. It is recommended to reboot Access Gateway Appliance in the following scenarios:

  - When Configuration console displays the **Reboot Needed** option in the upper right corner of the Appliance Configuration pane.
  - When Configuration console displays a message or a warning to reboot.

- **Schedule:** Configure the type of updates to download and whether to automatically agree to the licenses.

  To schedule online update:

  1. Click the **Schedule** tab.
  2. Select a schedule for download updates (**Manual**, **Daily**, **Weekly**, **Monthly**).
- **View Info:** Click **View Info** to display a list of installed and downloaded software updates.
- **Refresh:** Click **Refresh** to reload the status of updates on Access Gateway Appliance.

15.3 Updating Security Patches for Access Gateway Service

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

15.3.1 Updating Linux Access Gateway Service with the Latest OpenSSL Patch

1 Download the openssl-update.sh script.

2 Change the file permission to executable:

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

3 Run the following command:

```
openssl-update.sh username password novell-nacm-apache-extra-4.2.1-1.0.2u
```

NOTE: This downloads the 1.0.2r version of OpenSSL. Change the version number depending on the version available on the appliance channel.

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

15.3.2 Updating Windows Access Gateway Service with the Latest OpenSSL Patch

1. Open the powershell command line with the admin privilege.

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

2. Navigate to `C:\Program Files\Novell\bin`, then run `patch_update.ps1` with the following three arguments:

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

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

   `patch_update.ps1 <myusername> <mypassword> <Openssl_Win_102k>`

NOTE: You must repeat these steps for all the Windows Access Gateway servers.

This command updates to OpenSSL 1.0.2r.

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

III Troubleshooting Installation and Upgrade

This section includes the following topics:

16 Troubleshooting Installation

16.1 Troubleshooting Windows Administration Console Installation

The following instructions explain how to run the installation program in the debug mode and how to clean up after such an installation:

1. Use the following command to start the installation program:

   `<filename>.exe -DAM_INSTALL_DEBUG=true -DAM_INSTALL_DEBUG_JAVA=true`

   Replace *<filename>* with the name of the executable.
2. Press the Ctrl key until the progress bar reaches 100% and goes away.

   A terminal window opens to display standard output.

   Additional verbose information is sent to the `\am32setup_debug.txt` file.
3. Use the output and the log file to discover the cause of the problem.
4. After you run the installation in the debug mode, you must clean up the results as follows:
   - **4a** Delete the temporary packages in the `\pkgdirs` directory, then delete the directory.
   - **4b** Delete the `\am32setup_debug.txt` file.
   - **4c** Delete the installation log files in the following directories:

     Windows 2012 Server: `\am32setup.log`

     Windows 2012 Server: `\Program Files\Novell\log`

     IMPORTANT: Delete the log files after debugging because they contain sensitive information in clear text.

16.2 (RHEL) The Health Status of Administration Console, Identity Server, and Access Gateway after Installation Is Not Green

Administration Console might display the timed-out error in the `catalina.out` file and might not be accessible using a web browser. Identity Server and Access Gateway might display an `Unable to read keystore` error message in the `JCC` log file. This issue occurs if SELinux is enabled on your system.

To disable SELinux, perform the following steps:

1. Open the `config` file located in the `/etc/sysconfig/selinux` directory.
2. Replace *SELINUX=enforcing* with *SELINUX=disabled*.
3. Save the change.
4. Restart the system.

16.3 Secondary Administration Console Installation Fails

Secondary Administration Console installation fails with a message "'Verifying time synchronization". If you are installing secondary Administration Console, ensure that time is in sync with primary Administration Console prior to installation.

If the time is in sync and secondary Administration Console installation fails or takes a long time, see the eDirectory install logs under `/tmp/novell_access_manager`. The log file name will be similar to `install_edir_xxxxxx`. If at the end of the log, you see an entry "Verifying time synchronization" multiple times, perform the following steps:

1. Log in to primary Administration Console and run the `ndsrepair -T` command.
2. run the `ndsrepair -N` command and select the server that has the problem.
3. Log in to secondary Administration Console and you can see that the installation has proceeded.

16.4 Troubleshooting Identity Server Import and Installation

16.4.1 Importing Identity Server into Administration Console Fails

Ensure that the following requirements are met if you have installed Administration Console and Identity Server on different machines:

- The following ports are opened between the machines:

8444
1443
1289
524
636

- Ports 8080 and 8443 must be open between the server and the clients for the clients to log in to Identity Server. For more information, see "Setting Up Firewalls" on page 28.
- Time is synchronized between the two machines. Ensure that both machines are configured to use a Network Time Protocol server.

If firewalls and time synchronization do not solve the problem, run the reimport script. See "Reimporting Identity Server" on page 165.

16.4.2 Reimporting Identity Server

1. Verify that Administration Console is up by logging in to Administration Console.
2. Verify that you can communicate with Administration Console. From the command line of Identity Server machine, enter a `ping` command with the IP address of Administration Console.

   If the `ping` command is unsuccessful, fix the network communication problem before continuing.
3. In Administration Console, delete Identity Server.

   For more information about how to delete Identity Server in Administration Console, see Identity Server Advanced Configuration in the *Access Manager 4.5 Administration Guide*.
4. On the Identity Server machine, change to the `jcc` directory:

   Linux: `/opt/novell/devman/jcc`

   Windows: `\Program Files\Novell\devman\jcc`
5. Run the following script to configure jcc:

   Linux: `./conf/reimport_nidp.sh jcc`

   Windows: `conf\reimport_nidp.bat jcc`
6. Run the following reimport script:

   Linux: `./conf/reimport_nidp.sh nidp`

   Windows: `conf\reimport_nidp.bat nidp <admin>`

   Replace *<admin>* with the name of your administrator for Administration Console.
7. If these steps do not work, reinstall the device.

16.4.3 Check the Installation Logs

If Identity Server installation fails, check the installation logs warning and error messages.

- Section 16.4.3.1, "Linux Installation Logs," on page 166
- Section 16.4.3.2, "Windows Installation Logs," on page 166

16.4.3.1 Linux Installation Logs

Installation logs are located in the `/tmp/novell_access_manager` directory.

Table 16-1 *Installation Log Files for the Linux Identity Server*

Log File	Description
`install_idp_<date&time>.log`	Contains the messages generated for Identity Server module.
`install_main_<date&time>.log`	Contains the Tomcat messages generated during the installation.
`install_jcc_<date&time>.log`	Contains the messages generated for the communications module.

16.4.3.2 Windows Installation Logs

Installation logs are located in the `\Program Files\Novell\Tomcat\webapps \nps\WEB-INF\logs\install` directory.

Table 16-2 *Installation Log Files for the Windows Identity Server*

Log File	Description
`basejar_InstallLog.log`	Contains the messages generated when installing Identity Server JAR files.
`base_InstallLog.log`	Contains the messages generated when installing Identity Server.
`nauditjar_InstallLog.log`	Contains the messages generated when installing Novell Audit JAR files.
`nauditjar_InstallLog.log`	Contains the messages generated for the auditing components.
`NIDS_Pluginjar_InstallLog.log`	Contains the messages generated when installing Identity Server plug-in JAR.
`NIDS_Plugin_InstallLog.log`	Contains the messages for the plug-in component.
`NMASjar_InstallLog.log`	Contains the messages generated when installing NMAS JAR files.
`NMAS_InstallLog.log`	Contains the messages for the NMAS component.

16.5 Troubleshooting Windows Access Gateway Service Installation

1. Run the following command to start the installation program:

   `<filename>.exe -DAM_INSTALL_DEBUG=true -DAM_INSTALL_DEBUG_JAVA=true`

   Replace *<filename>* with the name of the executable.
2. Press the Ctrl key until the progress bar reaches 100% and goes away.

   Additional verbose information is sent to the `\agsinstall_debug.txt` file.

3 Use the output and the log file to discover the cause of the problem.

4 After you run the installation in debug mode, you must clean up the results:

4a Delete the `\agsinstall_debug.txt` file.

4b Delete the installation log files in the following directories:

Windows 2012 Server: `\agsinstall.log`

Windows 2012 Server: `\Program Files\Novell\log`

IMPORTANT: Delete the log files because they contain sensitive information in clear text.

16.6 Access Gateway Appliance Installation Fails Due to an XML Parser Error

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

16.7 Troubleshooting Access Gateway Import

When you install Access Gateway, it is automatically imported into Administration Console you specified during installation. If Access Gateway does not appear in the server list, repair the import.

If the repair option does not resolve the problem, see the following sections:

- Section 16.7.1, “Repairing an Import,” on page 167
- Section 16.7.2, “Troubleshooting the Import Process,” on page 168

16.7.1 Repairing an Import

If Access Gateway does not appear in Administration Console within 10 minutes of installing an Access Gateway, perform the following steps:

1 If a firewall separates Administration Console and Access Gateway, ensure that the required ports are opened. See Table 1-3 on page 30.

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

3 Wait for a few minutes, then click **Refresh**.

4 If the device import fails, a message similar to the following appears at the bottom of the table:

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

5 Click **repair import**.

6 If the device still does not appear or you do not receive a repair import message, continue with “Triggering an Import Retry” on page 169.

7 If triggering an import retry does not solve the problem, reinstall the device.

16.7.2 Troubleshooting the Import Process

If the import process does not complete successfully, the device does not show up in the Access Gateway list. The following sections describe the import process, where to find the log files, and how to use them to determine where the failure occurred:

16.7.2.1 Understanding the Import Process

The following operations are performed during the import process:

1. A user specifies the IP address for Administration Console during installation.
2. A Java process called “JCC” (Java Communication Channel) detects that Administration Console IP address or port has changed between its own configuration and the CLI-updated settings.
3. An import message is sent to Administration Console, notifying it of the IP, port, and ID of Access Gateway.
4. Administration Console then connects to the Access Gateway device to fetch its configuration and version information. The Access Gateway import process is now complete.
5. As a separate asynchronous operation, the Embedded Service Provider (ESP) of Access Gateway connects and registers itself with the JCC.
6. When the ESP connects to the JCC, a similar import message is sent to Administration Console notifying it to import into the system.
7. Administration Console connects to the JCC, asking for the ESP configuration and version information. On Administration Console, an LDIF (Lightweight Directory Interchange Format) file containing the default configuration for the ESP is applied on the local eDirectory configuration store.
8. Administration Console then makes a link between the ESP and its configuration.
9. If the entire process completed properly, Access Gateway appears in the list of Access Gateways in Administration Console.

16.7.2.2 Locating the Log Files

Various Access Manager components produce log files. Use the following logs on Administration Console or Access Gateway:

- Administration Console log:

  Linux: `/opt/novell/devman/share/logs/app_sc.0.log`

  Windows: `\Program Files\Novell\log\app_sc.0.log`

- Tomcat Log on Administration Console:

  Linux: `/opt/novell/nam/`*`device name`*`/logs/catalina.out`

  The device name can be `idp`, `mag`, or `adminconsole`.

Windows: `\Program Files\Novell\Tomcat\logs\stdout.log` and `\Program Files\Novell\Tomcat\logs\stderr.log`

- JCC log on Access Gateway:

  Linux Appliance or Service: `/opt/novell/devman/jcc/logs/`

  Windows Service: `\Program Files\Novell\devman\jcc\logs`

16.7.2.3 Triggering an Import Retry

1. Go to the directory:

   Linux: `/opt/novell/devman/jcc/`

   Windows: `\Program Files\Novell\devman\jcc`

2. Run the following script:

   Linux: `sh conf/reimport_ags.sh jcc`

   Windows: `conf\reimport_ags.bat jcc`

   Specify details against the following prompts:

   - Choose a local listener IP address [x.x.x.x]:
   - (Optional) Choose a local NAT IP address [optional]:
   - Choose Administration Console's IP address []:
   - Enter Admin User's DN [cn=admin,o=novell]:
   - Enter Admin Password: *****

     Wait for a few minutes for the configuration to finish.

3. Run the following script:

   Linux: `sh conf/reimport_ags.sh agm`

   Windows: `conf\reimport_ags.bat agm <username>`

   For example, if the username is *admin*, then run conf\reimport_ags.bat agm admin

   Specify details against the following prompts:

   - (Linux) Do you want to import the device with current configuration or initial configuration after installation (Enter C for current configuration, I for initial configuration).
   - (Linux) Enter Admin User's DN [cn=admin,o=novell]:
   - Enter Admin password:

16.8 Troubleshooting Windows Identity Server Uninstallation

When you uninstall Windows Identity Server, the uninstall program prompts you for the credentials of the admin user for Administration Console. If the primary Administration Console is not available for the authentication request, the uninstall fails.

To force the uninstall program to skip the authentication request, run the following command:

```
\Program
Files\Novell\Uninstall_AccessManagerServer\UninstallAccessManagerServer.
exe -DAM_INSTALL_AUTH_BYPASS=true
```

16.9 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.

---

17 Troubleshooting Upgrade

17.1 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**.

17.2 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`

17.3 Troubleshooting Linux Administration Console Upgrade

17.3.1 Upgrade Hangs

If the upgrade process encounters an error while installing a component or encounters an unexpected condition that requires a user input, the installation hangs.

Perform the following steps to resolve this issue:

1. View the installation screen and determine which component is being upgraded.
2. Change to the `/tmp/novell_access_manager` directory.
3. View the log file of the component that is being upgraded.

   Solve the problem described in the log file before continuing with the upgrade.

For example, if the eDirectory health check fails, the `edir` log file indicates that the upgrade program is waiting for a response whether the upgrade should continue. Abort the upgrade, run `ndsrepair` to repair the configurations store, then restart with the upgrade process.

4 If the log file of the current component does not contain any errors, use the time stamps of the log files to determine which component just finished its upgrade and check it for errors.

If you cannot determine which component is causing the problem:

4a Stop the upgrade process.

4b Run the following command to lists all the files created in the specified directory:

```
tail -f /tmp/novell_access_manager/<file-name>
```

4c Restart the upgrade process.

17.3.2 Multiple IP Addresses

If your server has multiple IP addresses, you might see the following message during upgrading Linux Administration Console:

```
Failed to load any MDB driver - Error: Could not load driver /usr/lib/mdb/
mdbfile.so, error 9 - /usr/lib/mdb/mdbfile.so: cannot open shared object
file: No such file or directory
```

The error occurs when running Novell Audit on servers with more than one IP address. It occurs when the system attempts to upgrade the audit server. Systems with more than one IP address have problems running Novell Audit because the multiple directory database (MDB) driver does not know which IP address to use with eDirectory. You can point Novell Audit to a specific IP address by creating an MDB configuration file.

The required filename and path for the MDB configuration file is `/etc/mdb.conf`.

To point Novell Audit to a specific IP address for eDirectory, the MDB configuration file must store the following parameters:

```
driver=mdbds referral=eDirectory_IP_ Address.
```

For example, `driver=mdbds referral=10.10.123.45.`

You might only have one IP address, but your server might have two network adapters. If you create the `/etc/mdb.conf` file and specify your IP address, you do not encounter this error message when you upgrade.

17.3.3 Certificate Command Failure

Certificate commands are generated when you upgrade Administration Console. Ensure that this process has been completed successfully. Click **Security** > **Command Status**.

If a certificate command fails, note the store, click **Troubleshooting** > **Certificates**. Select the store, then click **Re-push certificates** to push the certificates to the store.

17.4 Upgrading Secondary Administration Console Fails with an Error

Upgrading secondary Administration Console fails with the following error:

```
Configuring HTTP service... Failed to configure HTTP service: no referrals
err=-634
```

This issue might occur because of some eDirectory issues. You can run the script again. If you access the console remotely, run the script from the machine directly.

17.5 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).

17.6 Administration Console Fails to Start When You Upgrade the Operating System After Upgrading Access Manager

When you upgrade the operating system from SLES 11 SP3 to SLES 12 after upgrading Access Manager, Administration Console does not start. This issue occurs because eDirectory services do not start after the upgrade.

To resolve this issue, perform the following steps:

1. Run `ndsconfig upgrade` at the SLES 12 server, where Administration Console is upgraded.

   This generates the necessary template files so that eDirectory starts without any issues.
2. Run `ndsmanage startall`.

   This starts eDirectory services on the SLES 12 server.

17.7 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.

17.8 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).

17.9 Access Manager Upgrade Hangs While Upgrading eDirectory

On Windows, the Access Manager upgrade hangs while upgrading eDirectory. This occurs because the `nservmsg.dll` file gets locked. This is a random issue.

To workaround this issue, perform the following steps:

1. Manually stop the Windows Event Log service.
2. On the upgrade pop-up screen, click **Retry**.
3. Restart the Windows Event Log service manually again and proceed with the upgrade.

17.10 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>
```

17.11 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:

   Windows: `C:\Program Files\Novell\Tomcat\conf\server.xml`

   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
   ```

   Administration Console:

Windows: `C:\Program Files\Novell\Tomcat\conf\server.xml`

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443"
secret="namnetiq" />
```

Identity Service Provider (IDP):

Windows: `C:\Program Files\Novell\Tomcat\conf\server.xml`

```
<Connector URIEncoding="utf-8" port="8009" protocol="AJP/1.3"
redirectPort="8443" secret="namnetiq" useBodyEncodingURI="false"/>
```

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

```
<Connector address="127.0.0.1" backlog="0" connectionTimeout="20000"
enableLookups="false" maxPostSize="2097152" maxThreads="600"
minSpareThreads="25" port="9019" protocol="AJP/1.3" scheme="https"
secure="true" secret="namnetiq" />^M
```

3 Save the file and restart the Apache Tomcat Service.

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

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
```

Path: `/etc/opt/novell/apache2/conf/vhosts.d/proxy.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
```

17.12 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:

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

Administration Console ports 9000 and 9001 listen on 127.0.0.1 by default. Administration Console 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` (Linux) or `tomcat8w.exe` (Windows) file:

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

Windows: Navigate to `C:\Program Files\Novell\Tomcat\bin` and then double-click `tomcat8w.exe`

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

For example:

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

B Recommendations for Scaling Access Manager Components in Public Cloud

In the public cloud environment, you can manually add or remove Access Manager components nodes to a cluster depending on the varying scalability requirements.

Scaling Up the Access Manager Nodes

As the number of users and demands for web resources increase, you can easily add another Identity Server or Access Gateway to handle the load. The cluster configuration is sent to the newly added components automatically.

Scaling up a node when the Access Manager component is not deployed in the cloud virtual machine

Perform the following steps to scale up a node:

1. Create new virtual machines. For AWS EC2, see Section 6.2.2, "Creating and Deploying Instances," on page 87 and for Azure, see Section 7.2.2, "Creating and Deploying Virtual Machines," on page 99.
2. Install the required Access Manager component and import that component to Administration Console.
3. After importing the component, log in to Administration Console and assign the imported component to the required cluster.
4. Access the cloud console (Azure or AWS EC2) and add the newly imported component to the load balancer group or target group.

Scaling up a node when the Access Manager component is installed in the cloud virtual machines, but not imported into the cluster

Perform the following steps to scale up a node:

1. Switch on the cloud virtual machine on which the required component is installed.
2. Access the terminal of the server and initiate the `ag_import` or `idp_import` script depending on the type of server.
3. Specify the Administration Console IP address while importing the component.
4. After importing, log in to Administration Console and assign the imported component to the required cluster.
5. Access the cloud console (Azure or AWS EC2) and add the newly imported component to the load balancer group or target group.

Scaling Down the Access Manager Nodes

1. Remove the Access Manager component's IP address from the load balancer rule.
2. Stop the service. (Identity Server or Access Gateway)
3. Stop the virtual machine on which the component is installed. You can also optionally delete the virtual machine.
4. Log in to Administration Console, select the non-reporting node from the cluster, and delete it from the configuration.

C 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.

D Recommendations for Scaling Access Manager Components in Public Cloud

In the public cloud environment, you can manually add or remove Access Manager components nodes to a cluster depending on the varying scalability requirements.

Scaling Up the Access Manager Nodes

As the number of users and demands for web resources increase, you can easily add another Identity Server or Access Gateway to handle the load. The cluster configuration is sent to the newly added components automatically.

Scaling up a node when the Access Manager component is not deployed in the cloud virtual machine

Perform the following steps to scale up a node:

1. Create new virtual machines. For AWS EC2, see Section 6.2.2, "Creating and Deploying Instances," on page 87 and for Azure, see Section 7.2.2, "Creating and Deploying Virtual Machines," on page 99.
2. Install the required Access Manager component and import that component to Administration Console.
3. After importing the component, log in to Administration Console and assign the imported component to the required cluster.
4. Access the cloud console (Azure or AWS EC2) and add the newly imported component to the load balancer group or target group.

Scaling up a node when the Access Manager component is installed in the cloud virtual machines, but not imported into the cluster

Perform the following steps to scale up a node:

1. Switch on the cloud virtual machine on which the required component is installed.
2. Access the terminal of the server and initiate the `ag_import` or `idp_import` script depending on the type of server.
3. Specify the Administration Console IP address while importing the component.
4. After importing, log in to Administration Console and assign the imported component to the required cluster.
5. Access the cloud console (Azure or AWS EC2) and add the newly imported component to the load balancer group or target group.

Scaling Down the Access Manager Nodes

1. Remove the Access Manager component's IP address from the load balancer rule.
2. Stop the service. (Identity Server or Access Gateway)
3. Stop the virtual machine on which the component is installed. You can also optionally delete the virtual machine.
4. Log in to Administration Console, select the non-reporting node from the cluster, and delete it from the configuration.