



Access Manager Appliance 5.0

Installation and Upgrade Guide

March 2021

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.microfocus.com/en-us/legal>.

© Copyright 2022 Micro Focus or one of its affiliates.

Contents

About this Book and the Library	7
1 Planning Your Access Manager Environment	9
1.1 Deployment Models	9
1.2 Access Manager Versus Access Manager Appliance	11
1.3 Network Requirements	16
1.4 System Requirements	17
1.5 Basic Setup	17
1.6 Setting Up Firewalls	17
1.6.1 Required Ports	18
1.6.2 Restricted Ports	20
1.6.3 Sample Configurations	21
1.7 Using Certificates for Secure Communication	22
Part I Installing Access Manager Appliance	23
2 Installing Access Manager Appliance	25
2.1 Requirements for Installing Access Manager Appliance	25
2.1.1 Client Access Requirements	25
2.1.2 Installation Mode	25
2.1.3 Virtual Machine Requirements	26
2.2 Installing Access Manager Appliance	27
2.2.1 Prerequisites	27
2.2.2 Installing Access Manager Appliance	28
2.2.3 Installing Secondary Access Manager Appliance	30
2.2.4 Logging In to Administration Console	31
2.2.5 Administration Console Conventions	31
3 Installing Analytics Server	33
Part II Upgrading or Migrating Access Manager Appliance	35
4 Prerequisites for Upgrading or Migrating Access Manager Appliance	37
4.1 Maintaining Customized JSP Files for Identity Server	38
4.1.1 Using Customized JSP Pages from Access Manager 4.1 or Prior	38
4.1.2 Using Customized JSP Pages from Access Manager 4.1 or Prior and Enabling the New Access Manager Portal	39
4.2 Maintaining Customized JSP Files for Access Gateway	40

5	Upgrading Access Manager Appliance	41
6	Migrating Access Manager Appliance	43
6.1	Prerequisites for Migrating Access Manager Appliance	44
6.2	To Migrate Access Manager Appliance	44
6.3	Example Scenario: Access Manager Appliance Migration Using the Existing IP Address	47
7	Upgrading Analytics Server	49
7.1	Upgrade Analytics Server Cluster	50
8	Post Upgrade Considerations	51
8.1	Database Schema Changes for Risk Service	51
8.2	Configuration Files-specific Changes	51
8.3	Changes in Identity Server and Access Gateway Processes	52
8.4	Schema Changes of Attributes	52
9	Getting the Latest OpenSSL Updates for Access Manager Appliance	53
9.1	Installing or Updating Security Patches for Access Manager Appliance	53
	Part III Troubleshooting Installation and Upgrade	57
10	Troubleshooting Installation	59
10.1	Checking the Installation Logs	59
10.2	Some of New Hardware Drivers or Network Cards Are Not Detected during Installation	60
10.3	Installation Through Terminal Mode Is Not Supported	60
10.4	Access Manager Appliance Installation Fails Due to an XML Parser Error	60
10.5	DN Is Added as Provider ID While Installing the NMAS SAML Method	60
10.6	Troubleshooting Analytics Server	61
10.6.1	Dashboard Login Fails After Applying An External Signed Certificate to the Administration Console	61
10.6.2	Intermittent Issue With Cluster Configuration	61
10.7	Rsyslog Fails to Start After Access Manager Installation	62
11	Troubleshooting Upgrade	63
11.1	Access Gateway Throws a 403 Forbidden Page Error for a Resource Protected by a Form Fill Policy	63
11.2	Issue in SSL Communication between Access Gateway and Web Applications	63
11.3	Customized Login Pages Are Missing After Upgrading Access Manager	64
11.4	The Email OTP JSP Page Does Not Render Properly on Internet Explorer 11	64
11.5	X509 Authentication Does Not Work and Throws HTTP 500 Error After Upgrade	64
11.6	Changes Required in server.xml for Apache Tomcat 8.5.51 after Upgrading to Access Manager 4.5 Service Pack 2	65
11.7	Java Communication Channel Processes Run as Non-Root User After Upgrading to Access Manager 5.0	66
11.8	Rsyslog Fails to Start After Access Manager Upgrade	67

Part IV Appendix	69
A Configuring Ports 9000 and 9001 to Listen on the Specified Address	71
B Denormalizing SQL Database	73

About this Book and the Library

This guide provides an introduction to NetIQ Access Manager Appliance and describes the installation and upgrade procedures.

The Install or Upgrade sends the following information to the Telemetry server for checking product version currency:

- ♦ Product Name. For example, NAM
- ♦ Product Version: For example, 5.0.4.0-43
- ♦ Installation Type: For example, Service or Appliance
- ♦ Operating System: For example, SLES

This information does not contain any Personal Information (PI) and is collected only while installing or upgrading.

Intended Audience

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

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

Other Information in the Library

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

- ♦ [Access Manager Developer Resources \(https://www.microfocus.com/documentation/access-manager/developer-documentation-5.0/\)](https://www.microfocus.com/documentation/access-manager/developer-documentation-5.0/)

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

1 Planning Your Access Manager Environment

- ♦ [Section 1.1, “Deployment Models,” on page 9](#)
- ♦ [Section 1.2, “Access Manager Versus Access Manager Appliance,” on page 11](#)
- ♦ [Section 1.3, “Network Requirements,” on page 16](#)
- ♦ [Section 1.4, “System Requirements,” on page 17](#)
- ♦ [Section 1.5, “Basic Setup,” on page 17](#)
- ♦ [Section 1.6, “Setting Up Firewalls,” on page 17](#)
- ♦ [Section 1.7, “Using Certificates for Secure Communication,” on page 22](#)

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 manage each component on separate servers. Administration Console, Identity Server, Dashboard, and Access Gateway can also be deployed using Docker and on Cloud as services on AWS EC2 and on 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
- ♦ 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 11](#).

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

Figure 1-1 Typical Deployment of Access Manager

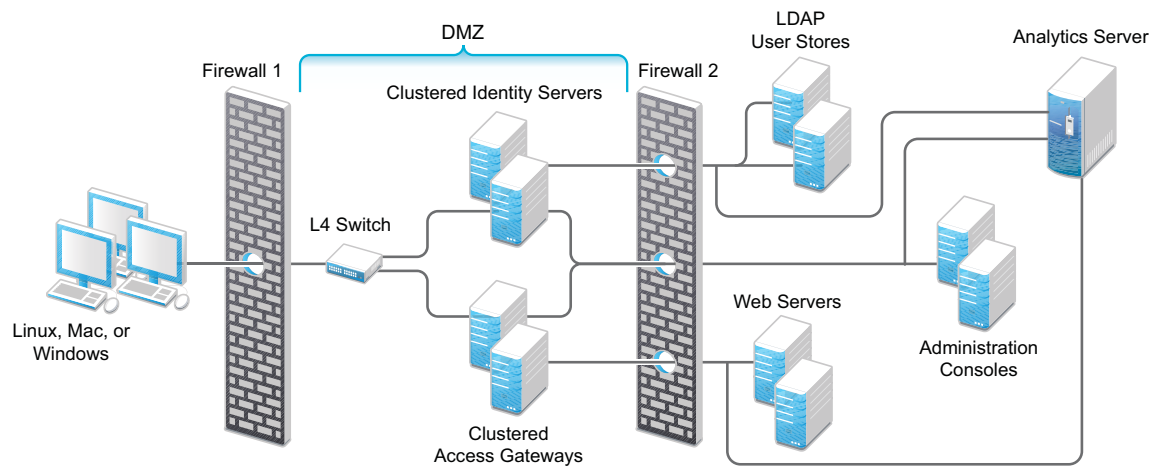
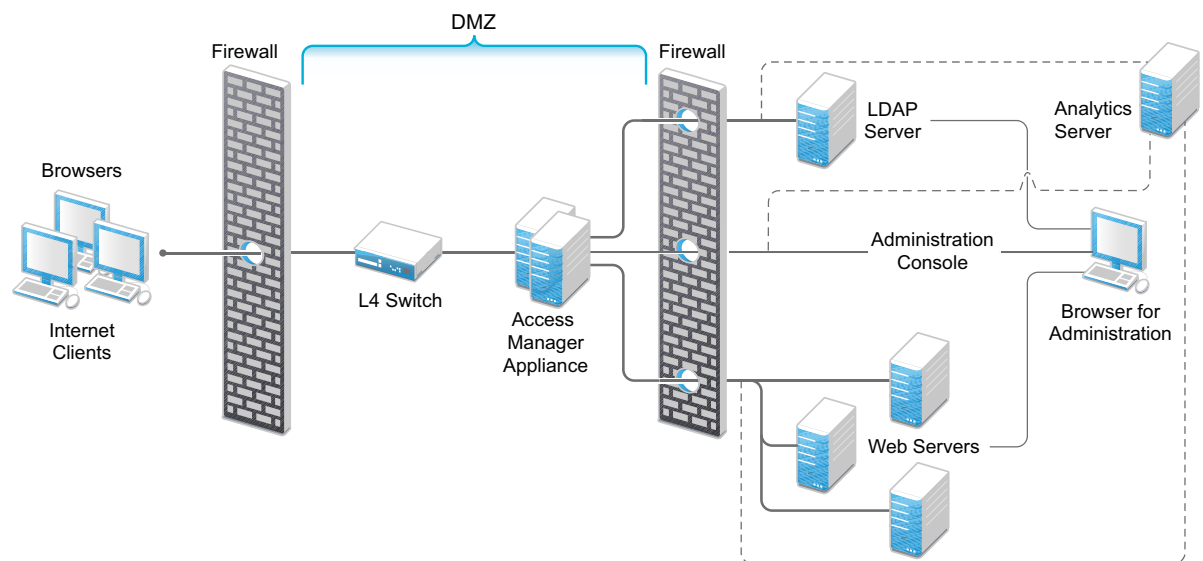


Figure 1-2 Typical Deployment of Access Manager Appliance



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 SP5 or SLES 15 SP2 with 64-bit operating system x86-64 hardware.
Host Operating System	<p>A soft appliance that includes a pre-installed and configured SUSE Linux operating system.</p> <p>NetIQ maintains both the operating system and Access Manager patches through the patch update channel.</p>	<p>Operating System choice is more flexible. Install Administration Console, Identity Server, and Access Gateway on a supported operating system (SUSE or Red Hat).</p> <p>The patch update channel maintains patches for Access Manager.</p> <p>You must purchase, install, and maintain the underlying operating system.</p>
Component Installation Flexibility	Access Manager components such as Administration Console, Identity Server, and Access Gateway cannot be selectively installed or uninstalled.	<p>Each Access Manager component such as Administration Console, Identity Server, and Access Gateway are installed on independent host servers.</p> <p>Although the ability to install multiple components on a single host server exists, it is very limited and not recommended.</p> <p>A typical highly available deployment requires 6-8 or more virtual or physical servers (2 Administration Consoles, 2 Identity Servers, 2 Access Gateways).</p>
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	<p>Scales vertically on adding CPU and memory resources to each node.</p> <p>See NetIQ Access Manager Performance and Sizing Guidelines .</p>	<p>Scales both vertically and horizontally on adding nodes.</p> <p>See NetIQ Access Manager Performance and Sizing Guidelines .</p>

Feature	Access Manager Appliance	Access Manager
High Availability	Supported	Supported
Upgrade	<p>You can upgrade from one version of Access Manager Appliance to another version.</p> <p>However, upgrading from Access Manager to Access Manager Appliance is not supported.</p>	<p>You can upgrade from one version of Access Manager to another version.</p> <p>However, upgrading from Access Manager Appliance to Access Manager is not supported.</p>
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.	<p>Separate installation and configuration phases for each component.</p> <p>After installation, each Access Manager component is separately configured.</p>
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. You can place Identity Server behind Access Gateway or place it separately in DMZ.
Ready-made Access Manager	<p>The following configuration is automatically done after Access Manager Appliance installation:</p> <ul style="list-style-type: none"> ♦ 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, and Administration Console. <p>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.</p>	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	<p>For additional capacity and for failover, cluster a group of Access Manager Appliances and configure them to act as a single server.</p> <p>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.</p> <p>A typical Access Manager Appliance deployment in a cluster is described in Figure 1-3.</p>	<p>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.</p> <p>To deploy the existing solution in a cluster mode, at least 6 systems are required.</p> <p>A typical Access Manager deployment in a cluster is described in Figure 1-4.</p>

Figure 1-3 Access Manager Appliance Cluster

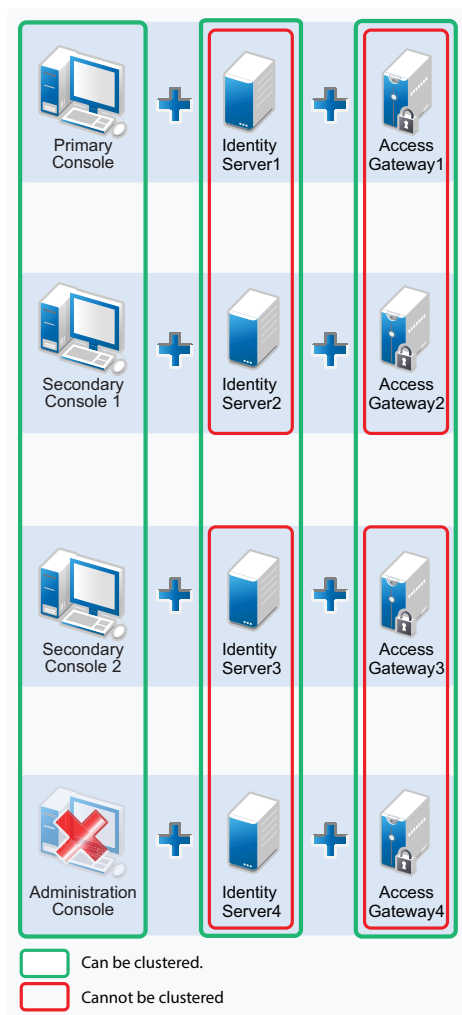
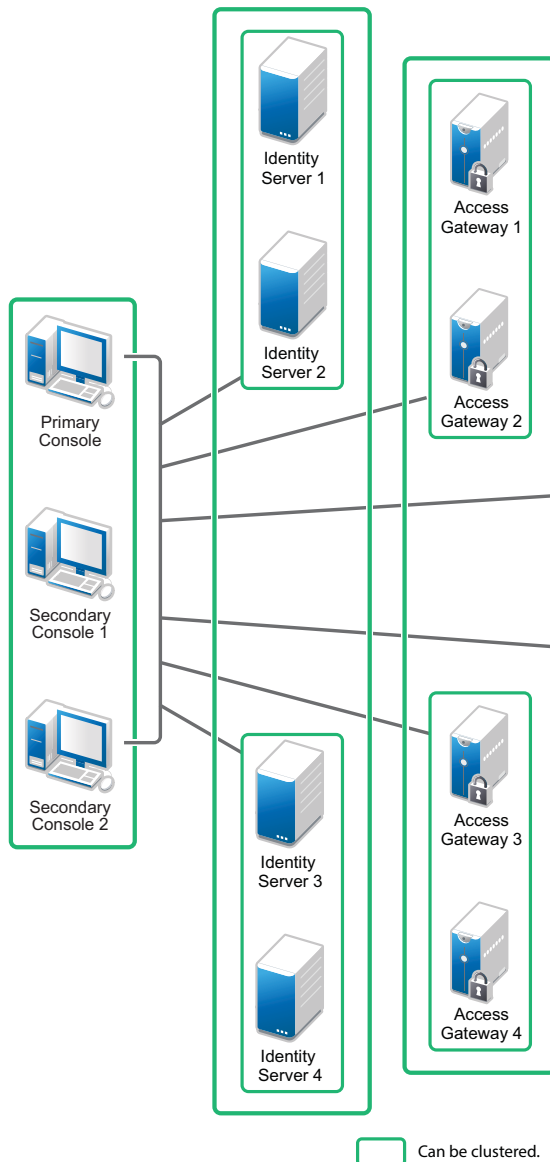


Figure 1-4 Access Manager Cluster



General Guidelines

- ♦ Adding an Access Gateway Service or Access Gateway Appliance to an Access Manager Appliance cluster is not possible.
- ♦ Deploying Administration Console in a DMZ network limits access from a private interface or network.
- ♦ It is recommended to not change the primary IP Address of Access Manager. This might result in corruption of the configuration store. However, you can modify the listening IP address of reverse proxy or the outbound IP address used to communicate with the web server. For more information, see [Changing the IP Address of Access Manager Appliance](#) in the [NetIQ Access Manager Appliance 5.0 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 costs by consolidating Access Manager services on fewer servers.
- ♦ You want to quickly set up a test environment to verify changes.
- ♦ You want to quickly set up 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, Active Directory, or Azure Active Directory) that contains your system users. Identity Server uses the LDAP directory to authenticate users.

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

- ♦ Web servers with content or applications that need protection and single-sign on.
- ♦ Static IP addresses for each Access Manager Appliance. If the IP address of the machine changes, Access Manager Appliance components cannot start.
- ♦ A domain name server, which resolves DNS names to IP addresses and which has reverse lookups enabled.

Access Manager Appliance communicates with 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 with RHEL 7.x. NTP is discontinued in RHEL 8, therefore with RHEL 8.x you must use Chrony. For more information, see [Configuring Chrony](#).

IMPORTANT: If time is not synchronized, you 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.

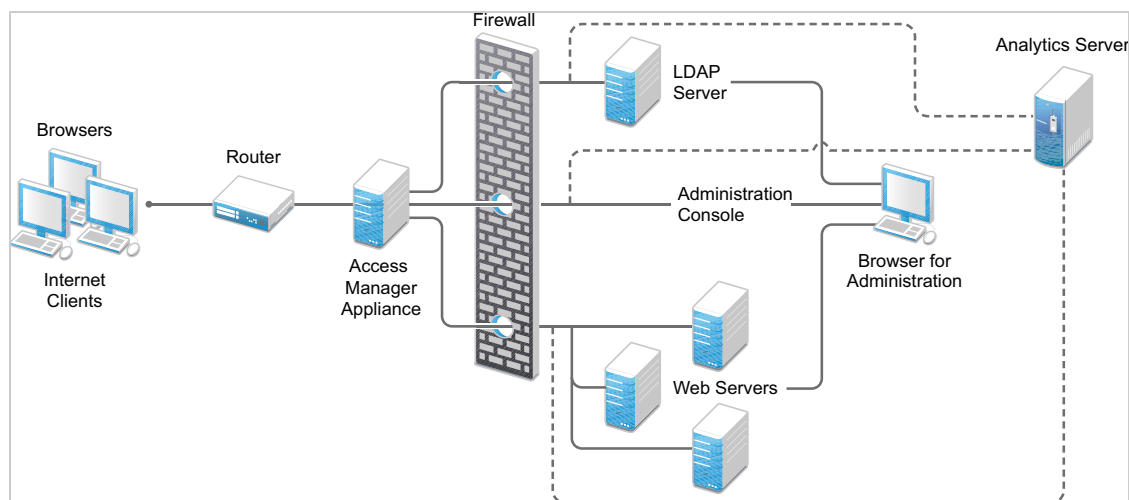
1.4 System Requirements

See the [NetIQ Access Manager System Requirements](#) guide.

1.5 Basic Setup

[Figure 1-5](#) illustrates the basic Access Manager Appliance installation, where Access Manager Appliance is installed outside your firewall. The figure provides an overview of the flexibility built into Access Manager Appliance. You can use it to design a deployment strategy that fits the needs of your company.

Figure 1-5 Basic Configuration



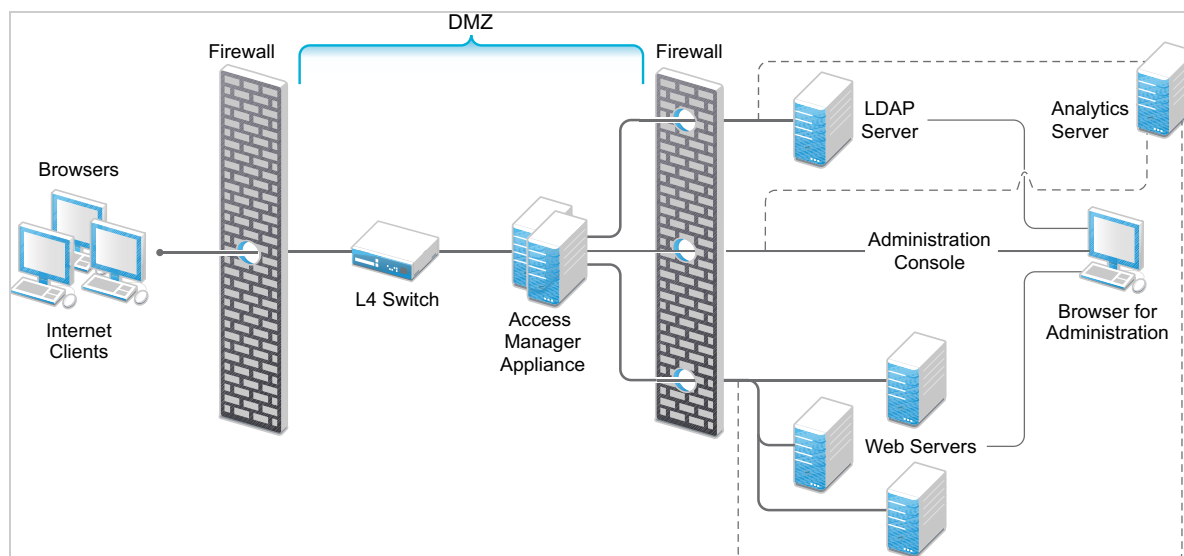
For more information, see [Section 2.2.2, “Installing Access Manager Appliance,”](#) on page 28.

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

1.6 Setting Up Firewalls

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

Figure 1-6 Access Manager Appliance and Firewall



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

This section describes the following topics:

- ♦ [Section 1.6.1, “Required Ports,” on page 18](#)
- ♦ [Section 1.6.3, “Sample Configurations,” on page 21](#)

1.6.1 Required Ports

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

Component	Port	Description
NTP Server	UDP 123	Access Manager Appliance must have time synchronized else the authentication fails. Configure Access Manager Appliance to use an NTP (network time protocol) server. Depending on where your NTP server is located in relationship to your firewalls, you might need to open UDP 123.
DNS Servers	UDP 53	Access Manager Appliance must be able to resolve DNS names. Depending upon where your DNS servers are located, you might need to open UDP 53 so that Access Manager Appliance can resolve DNS names.
Remote Linux Administration Workstation	TCP 22	To use SSH for remote administration of Access Manager Appliance.

Component	Port	Description
Access Manager Appliance	TCP 1443	For communication from Administration Console to devices.
	TCP 8444	For communication from devices to Administration Console.
	TCP 1290	For communication from devices to the Syslog server on Administration Console.
	TCP 524	For NCP certificate management with NPki. The port needs to be opened so that both the device and Administration Console can use the port.
	TCP 636	For secure LDAP communication from the devices to Administration Console.
	TCP 524	Required to synchronize the configuration data store.
	TCP 636	Required for the secure LDAP communication.
	TCP 8080, 8443	Used for the Tomcat communication.
	TCP 7801	Used for back-channel communication with cluster members.
LDAP User Store	TCP 524	Required only if the user store is eDirectory. When configuring a new eDirectory user store, NCP is used to enable Novell SecretStore by adding a SAML authentication method and storing a public key for Administration Console. It is not used in day-to-day operations.
Browsers	TCP 8080	For HTTP communication from browsers to Administration Console.
	TCP 8443	For HTTPS communication from browsers to Administration Console.
	TCP 8028, 8030	To use iMonitor or DSTrace from a client to view information about the configuration store on Administration Console.
	TCP 80	For HTTP communication from the client to Access Gateway. This is configurable.
	TCP 443	For HTTPS communication from the client to Access Gateway. This is configurable.
Web Servers	TCP 80	For HTTP communication from Access Gateway to web servers. This is configurable.
	TCP 443	For HTTPS communication from Access Gateway to web servers. This is configurable.

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

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

Component	Port	Description
Administration Console	TCP 1444	For communication between Administration Console and Analytics Server.
Browsers	TCP 8445	For HTTPS communication with Analytics Server for Access Manager Dashboard.
Syslog	TCP 1468	For sending Syslog messages from Access Manager components to Analytics Server.
Docker	TCP 2443	For Docker deployment.
Remote Administration Workstation	TCP 22	For communication from your remote administration workstation to Analytics Server.
Upgrade Assistant Agent	TCP 9968	For HTTPS communication from Upgrade Assistant agent to Administration Console or any services.

The following syslog ports for Docker are configured for Access Gateway, Administration Console, and Identity Server so they are unique and do not conflict:

Table 1-4 Syslog Ports on Docker

Ports for Administration Console	Ports for Access Gateway	Ports for Identity Server
1290	1490	1390
1291	1491	1391
1292	1492	1392

1.6.2 Restricted Ports

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

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

9090

If required, use port redirection by using IP tables.

1.6.3 Sample Configurations

- ♦ [Access Manager Appliance in DMZ](#)

1.6.3.1 Access Manager Appliance in DMZ

- ♦ [“First Firewall” on page 21](#)
- ♦ [“Second Firewall” on page 21](#)

First Firewall

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

See, [Figure 1-6 on page 18](#)

Table 1-5 Ports to Open in the First Firewall

Port	Purpose
TCP 80	For HTTP communication.
TCP 443	For HTTPS communication.
Any TCP port assigned to a reverse proxy or tunnel.	
TCP 8080	For HTTP communication with Identity Server.
TCP 8443	For HTTPS communication with Identity Server.
TCP 8445	For HTTP Identity Provider introductions. If you do not enable Identity Provider introductions, you do not need to open this port.
TCP 8446	For HTTPS Identity Provider introductions. If you do not enable Identity Provider introductions, you do not need to open this port.

Second Firewall

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

Table 1-6 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.

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

1.7 Using Certificates for Secure Communication

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

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

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

[“Strengthening Certificates”](#) in the *NetIQ Access Manager Appliance 5.0 Security Guide*.

Installing Access Manager Appliance

This section includes the following topics:

- ♦ [Chapter 2, “Installing Access Manager Appliance,” on page 25](#)
- ♦ [Chapter 3, “Installing Analytics Server,” on page 33](#)

2 Installing Access Manager Appliance

Installing Access Manager Appliance involves the following two-step process:

1. [“Installation Using the Access Manager Appliance ISO” on page 28](#)
2. [“Configure Access Manager Appliance Using Common Appliance Framework User Interface” on page 29](#)

This section includes the following topics:

- ♦ [Section 2.1, “Requirements for Installing Access Manager Appliance,” on page 25](#)
- ♦ [Section 2.2, “Installing Access Manager Appliance,” on page 27](#)

For information about differences between Access Manager and Access Manager Appliance, see [Access Manager Versus Access Manager Appliance](#).

2.1 Requirements for Installing Access Manager Appliance

For a list of relevant file names and for information about how to install a specific release, see the version-specific Release Notes on the [NetIQ Access Manager Documentation website](#).

For system requirements, see [NetIQ Access Manager System Requirements](#) guide.

For network requirements, see [Network Requirements](#).

For supported browsers, see [“Browser Support”](#) in the [NetIQ Access Manager System Requirements](#) guide.

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

2.1.1 Client Access Requirements

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

2.1.2 Installation Mode

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

2.1.3 Virtual Machine Requirements

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

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

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

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

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

The following sections contain installation tips for virtual machines:

- ♦ [Section 2.1.3.1, “Keeping Time Synchronized on Access Manager Appliances,” on page 26](#)
- ♦ [Section 2.1.3.2, “Number of Virtual Machines Per Physical Machine,” on page 26](#)
- ♦ [Section 2.1.3.3, “Using a Network Adapter for VMWare ESX,” on page 27](#)

2.1.3.1 Keeping Time Synchronized on Access Manager Appliances

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

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

- 1 Configure the NTP server in the `/etc/ntp.conf` file. For information about how to configure the NTP server, see [Configuring NTP \(https://support.ntp.org/bin/view/Support/ConfiguringNTP\)](https://support.ntp.org/bin/view/Support/ConfiguringNTP).
- 2 Run the `rcntp start` command on the primary Administration Console to start the NTP server.
- 3 Run the `ntpdate pool.ntp.org` command on the primary Administration Console to synchronize devices.

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

2.1.3.2 Number of Virtual Machines Per Physical Machine

The way you deploy your virtual machines can influence the performance of the Access Manager Appliance. Deploy a maximum of four Access Manager Appliance virtual machines on a single hardware. When you deploy more than four, the components of Access Manager Appliance start

competing with each other for the same hardware resources simultaneously. You can include other types of services that the machine can support if they do not use the same hardware resources that Access Manager Appliance components use.

The configured CPUs must match the hardware CPUs on the machine. Performance drastically reduces when the allocation of virtual CPUs is more than what exists on the machine.

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

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

2.1.3.3 Using a Network Adapter for VMWare ESX

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

2.2 Installing Access Manager Appliance

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

What you
need to know

- ◆ Root password of Access Manager Appliance.
 - ◆ Username and password of Administration Console administrator.
 - ◆ Static IP address for Access Manager Appliance.
 - ◆ DNS name (host and domain name) for Access Gateway that resolves to the IP address.
 - ◆ Subnet mask that corresponds to the IP address for Access Gateway.
 - ◆ IP address of your network's default gateway.
 - ◆ IP addresses of the DNS servers on your network.
 - ◆ IP address or DNS name of an NTP server.
 - ◆ The configuration store tree is named after the server on which you install Access Manager Appliance. Check the hostname and rename the machine if the name is not appropriate for a configuration tree name.
 - ◆ The ESXi server version supported is 6.0 and later.
-

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

2.2.1 Prerequisites

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

- ❑ Ensure that the machine meets the minimum requirements. See [Requirements for Installing Access Manager Appliance](#).
- ❑ (Optional) If you want to try any advanced installation options such as driver installation or network installation, see the [Deployment Guide](http://www.suse.com/documentation/sles11/book_sle_deployment/data/book_sle_deployment.html) (http://www.suse.com/documentation/sles11/book_sle_deployment/data/book_sle_deployment.html).

2.2.2 Installing Access Manager Appliance

Access Manager Appliance is installed with the following default partitions:

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

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

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

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

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

Installation Using the Access Manager Appliance ISO

NOTE: Access Manager Appliance does not support special characters in the **Username** and **Password** fields.

- 1 Insert the Access Manager Appliance CD into the CD drive.
- 2 Select **install_NAM-SingleBox-appliance**.
By default, the **Boot From Hard Disk** option is selected in the boot screen.
- 3 Press Enter.
- 4 Click **Yes** to the **Destroying ALL data on sda, continue?** prompt.
This loads the `NAM-SingleBox-appliance.x86_64-5.0.2.raw` file. After verifying the `sda`, the **Initializing Appliance Configuration** screen appears.
- 5 After checking the Appliance dependencies, the License page appears. Review the license agreement after selecting the language preference and then click **Accept**.
- 6 In the Access Manager Appliance Passwords and Time Zone screen, enter the root password and confirm the same.
In the Root Password section, specify password for the `root` user and name of the NTP server.
- 7 Select the region and time zone on the Clock and Time Zone page.
- 8 Review the Access Manager Appliance **Network Settings** and enter the **Hostname**. Example: `namapp.novell.com`.

9 Click **Next**.

10 Specify the following details:

Field	Description
IP Address	Configure the following options for the public IP: <ul style="list-style-type: none">♦ IP Address: The public IP address of Access Manager Appliance.♦ Network Mask: The subnet mask of Access Manager Appliance.♦ Gateway: The IP address of the default gateway.
DNS Server 1	IP address of your DNS server. You must configure at least one DNS server.
(Optional) DNS Server 2	IP address of your additional DNS server. This is an optional configuration.
Domain Name	The domain name for your network.

11 Wait for the configuration to complete and click **Next**. In the **Configuring password, time and network settings** screen, the **Finalizing configuration** progress bar is displayed. After the configuration is complete, The Access Manager appliance is ready for configuration message appears. Follow the instructions displayed.

To configure the appliance:

1. At your management workstation, open a browser and enter one of the following URLs"

`https://namapp.novell.com:9443`

`https://10.10.0.11:9443`

2. Log in as root with the password that you set during appliance first boot.

To change the IP address of the appliance:

1. At the command line, run the following as root:

`yast novell-vainit`

2. After making the desired changes, reboot the appliance.

IMPORTANT: Do not use the terminal prompt before consulting the documentation. Appliance administration requires appliance-specific tool.

Using standard tools can result in service disruption or failure.

Configure Access Manager Appliance Using Common Appliance Framework User Interface

When you log in to the Common Appliance Framework using the URL `https://<IP>:9443` (CAF), you can view the notifications and upgrade the operating system by clicking **Online Update**.

- 1 Access Manager appliance is ready for configuration. You can now log in as root user into the Common Appliance Framework user interface using `https://<IP>:9443` URL.
- 2 After successful login, the Micro Focus Access Manager Appliance Administration user interface is displayed.
- 3 Click **Access Manager Configuration** under **Access Manager Tools**, and specify the following fields:

Field	Description
Administration Console Type	Select either Primary or Secondary radio button. Select the Secondary option to specify if this Access Manager Appliance is not primary. If you are installing it as a secondary Access Manager Appliance, ensure that the primary Access Manager Appliance is reachable.
Primary Administration Console IP	Specify the IP address of the primary Access Manager Appliance if this is secondary.
Administration Console Config IP	Specify the IP address of the primary Administration Console.
Administration Console Published DNS Name	Specify the published DNS server name of the Administration Console.
Administration Console Username	Name of the Administration Console user. NOTE: Administration Console username does not accept special characters # (hash), & (ampersand), and () (round brackets).
Administration Console Password	Specify and confirm the password for the user. NOTE: Administration Console password does not accept special characters : (colon) and " (double quotes).
NAT IP	If you have mapped the private IP address of the Administration Console to the public NAT IP address. Specify that here.

4 Click **Save**.

The install process begins and it takes around 20 minutes for the install process to complete. After successful installation, refresh the Administration Console health status, wait for the same to turn green, and then log into the Administration Console using the `https://<ip>:9443` URL. Access Gateway and Identity Server are configured and available for use.

2.2.3 Installing Secondary Access Manager Appliance

If you have selected the **Secondary** radio button, provide the primary Administration Console IP and select the configuration IP of the specific server. Provide the Administration Console username and password.

NOTE: The first three nodes of Access Manager Appliance contain Administration Console, Identity Server, and Access Gateway. From the fourth installation onwards, the node does not contain Administration Console.

2.2.4 Logging In to Administration Console

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

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

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

To log in to:

- 1 Enable browser pop-ups.
- 2 From a client machine external to your Administration Console server, launch the browser and enter the URL for Administration Console.

If the hostname of your Access Manager Appliance is `www.host.com`, you might enter `https://www.host.com:8443/nps`.

- 3 Click **OK**. You can select the permanent or temporary session certificate option.
- 4 Specify the administrator name and password that you defined during installation, and click **Login**.

For information about configuring the view of Administration Console for Access Manager Appliance, see [Configuring the Default View](#) in the [NetIQ Access Manager Appliance 5.0 Administration Guide](#).

2.2.5 Administration Console Conventions

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

3 Installing Analytics Server

You can install Analytics Server after installing Administration Console.

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

IMPORTANT: Before installing the new Analytics Server, ensure to delete Analytics Server nodes of the earlier version from Administration Console. Ensure to use only three node cluster for Analytics Server as two node cluster is no longer supported.

Installation time: 10 minutes approximately

What you need to know to install Analytics Server	<ul style="list-style-type: none">◆ 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 of 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	2 GB
/var	3 GB

- ☐ Edit the `/etc/hosts` files on each instance and add an entry to resolve its hostname to its private IP address. For example, `10.10.10.11 kubew1`

NOTE: Install the `insserv-compat` package for SLES installation.

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 -xzf <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 in a sequential order one after the other, using the `tar.gz` file.

NOTE: It is highly recommended to take snapshots to avoid data loss. For more information, see [Snapshot and Restore](#).

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. The cluster health will be red till the second node is updated.

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

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

NOTE: Analytics Server cluster logs named `as_elasticsearch` cannot be downloaded from Administration Console if you have not configured a cluster setup. The error message "There were logs that failed to download...Requested resource is unavailable" appears.

Upgrading or Migrating Access Manager Appliance

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

For more information, see “[Back Up and Restore](#)” in the *NetIQ Access Manager Appliance 5.0 Administration Guide*.

NOTE: By default, the Access Manager configuration uses stronger TLS protocols, ciphers, and other security settings. If you want to revert these settings after upgrading, see “[Restoring Previous Security Level After Upgrading Access Manager Appliance](#)” in the *NetIQ Access Manager Appliance 5.0 Security Guide*.

Supported Upgrade Paths: For information about the latest supported upgrade paths, see the specific Release Notes on the [Access Manager Documentation](#) website.

Access Manager Version	Migration or Upgrade Path
4.5.x	Migrate to 5.0.1 and then upgrade to 5.0.2 or later
5.0.1 or higher	Direct upgrade

This section includes the following topics:

- ♦ [Chapter 4, “Prerequisites for Upgrading or Migrating Access Manager Appliance,” on page 37](#)
- ♦ [Chapter 5, “Upgrading Access Manager Appliance,” on page 41](#)
- ♦ [Chapter 6, “Migrating Access Manager Appliance,” on page 43](#)
- ♦ [Chapter 7, “Upgrading Analytics Server,” on page 49](#)
- ♦ [Chapter 8, “Post Upgrade Considerations,” on page 51](#)
- ♦ [Chapter 9, “Getting the Latest OpenSSL Updates for Access Manager Appliance,” on page 53](#)

4 Prerequisites for Upgrading or Migrating Access Manager Appliance

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



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

IMPORTANT: ♦ Access Manager 5.0 onwards, modification of `nidp.jar` is not recommended. If you have modified `nidp.jar` in the earlier release, then move those properties to `nidp_custom_resources_*.properties` as instructed in [Customizing the Error Pages](#) and upload the properties file to the Identity Server cluster using Advanced File Configurator. For information about how to add a file, see [Adding Configurations to a Cluster](#) in the [NetIQ Access Manager Appliance 5.0 Administration Guide](#).

- ♦ From Access Manager 5.0, modifying a configuration file directly on a device is not supported. Any modification made directly on a device is replaced when modifications made through Administration Console are applied. You must customize a configuration file using Advanced File Configurator on Administration Console. See [Modifying Configurations](#).
-

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

- ❑ Back up your current Access Manager configuration using `./ambkup.sh` command. For more information, see [Back Up and Restore](#) in the [NetIQ Access Manager Appliance 5.0 Administration Guide](#).
- ❑ 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 [Maintaining Customized JSP Files for Identity Server](#) or [Maintaining Customized JSP Files for Access Gateway](#).
- ❑ If you have customized any changes to `tomcat.conf` or `server.xml`, back up the files. After the upgrade, restore the files. For information about how to restore the file, see “[Managing Configuration Files](#)” in the “[NetIQ Access Manager Appliance 5.0 Administration Guide](#)”.
- ❑ 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. For information about how to restore the file, see “[Managing Configuration Files](#)” in the “[NetIQ Access Manager Appliance 5.0 Administration Guide](#)”.

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 `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>
```

For information about how to modify a file, see “[Modifying Configurations](#)” in the “[NetIQ Access Manager Appliance 5.0 Administration Guide](#)”.

- ❑ Some of the options are supported only through Administration Console. After the upgrade, configure those options through Administration Console. For the list of options that must be configured through Administration Console, see [Configuring Identity Server Global Options](#), [Configuring ESP Global Options](#), [Defining Options for SAML 2.0](#) in the [NetIQ Access Manager Appliance 5.0 Administration Guide](#).
- ❑ 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.
- ❑ Edit the /etc/hosts files on each instance and add an entry to resolve its hostname to its private IP address. For example, `10.10.10.11 kubew1`

NOTE: Post-Upgrade: (Applicable for upgrading from Access Manager 5.0 release only) To avoid any mismatch of customizations seen on Advanced File Configurator user interface and the file present in the VM server, it is recommended to click the [Send Configurations to Servers](#) icon () on all non-temporary files and folders in Identity Server, Administration Console, and Access Gateway from the Advanced File Configurator user interface. This action must be performed even if file status is displayed as Configuration sent successfully on the Advanced File Configurator user interface post-upgrade.

In addition to the these prerequisites, ensure that you also meet the hardware requirements. For more information about hardware requirements, see [NetIQ Access Manager Appliance System Requirements](#).

4.1 Maintaining Customized JSP Files for Identity Server

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

- ♦ [Using Customized JSP Pages from Access Manager 4.1 or Prior](#)
- ♦ [Using Customized JSP Pages from Access Manager 4.1 or Prior and Enabling the New Access Manager Portal](#)

4.1.1 Using Customized JSP Pages from Access Manager 4.1 or Prior

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

WARNING: The upgrade overwrites all existing JSP files.

- 2 Upgrade Access Manager Appliance.

- 3 Create an empty folder `legacy`.
- 4 Add the `legacy` folder to Identity Server in the `/opt/novell/nids/lib/webapp/WEB-INF/` directory using Advanced File Configurator.
For information about how to add a folder, see [“Adding Configurations to a Cluster”](#) in the *NetIQ Access Manager Appliance 5.0 Administration Guide*.

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

- 5 Add all backed up JSP files into the `/opt/novell/nids/lib/webapp/jsp` directory using Advanced File Configurator. For information about how to add files, see [“Adding Configurations to a Cluster”](#) in the *NetIQ Access Manager Appliance 5.0 Administration Guide*.
- 6 Refresh the browser to see the changes.

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

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

WARNING: The upgrade overwrites all existing JSP files.

- 2 Upgrade Access Manager Appliance.
- 3 Create an empty folder `legacy`.
- 4 Add the `legacy` folder to Identity Server in the `/opt/novell/nids/lib/webapp/WEB-INF/` directory using Advanced File Configurator.
For information about how to add a folder, see [“Adding Configurations to a Cluster”](#) in the *NetIQ Access Manager Appliance 5.0 Administration Guide*.

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

- 5 Open customized `nidp.jsp` and `content.jsp` files and make the following changes in both files:
For information about how to modify a file, see [“Adding Configurations to a Cluster”](#) in the *NetIQ Access Manager Appliance 5.0 Administration Guide*.
 - 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.

- 6 Refresh the browser to see the changes.

4.2 Maintaining Customized JSP Files for Access Gateway

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

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

WARNING: The upgrade overwrites all existing JSP files.

- 2 Upgrade Access Manager Appliance.
- 3 Create an empty folder `legacy`.
- 4 Add the `legacy` folder to Access Gateway in the `/opt/novell/nesp/lib/webapp/WEB-INF/` directory using Advanced File Configurator.

For information about how to add a folder, see [“Adding Configurations to a Cluster”](#) in the *NetIQ Access Manager Appliance 5.0 Administration Guide*.

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

- 5 Add all backed up JSP files into the `/opt/novell/nesp/lib/webapp/jsp` directory using Advanced File Configurator.

For information about how to add files, see [“Adding Configurations to a Cluster”](#) in the *NetIQ Access Manager Appliance 5.0 Administration Guide*.

- 6 Refresh the browser to see the changes.

5 Upgrading Access Manager Appliance

If you are on Access Manager 4.5.x, you first need to migrate to 5.0 Service Pack 1 and then upgrade to 5.0.2 or later.

For more information about migration, see [Chapter 6, “Migrating Access Manager Appliance,”](#) on page 43.

Prerequisites: See [Chapter 4, “Prerequisites for Upgrading or Migrating Access Manager Appliance,”](#) on page 37.

IMPORTANT: 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.

If you are on 5.0 Service Pack 1 and need to upgrade to 5.0 Service Pack 2 or later, perform the following steps:

- 1 Log in as the `root` user.
- 2 Download the `tar.gz` (`AM_50X_AccessManagerAppliance.tar.gz`) file of Access Manager Appliance from [Software Licenses and Downloads](#) and extract the `tar.gz` file using the following command:

```
tar -xzf <filename>
```

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

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

```
./sb_upgrade.sh
```

- 4 The system displays the following confirmation message:

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

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

- 5 Enter the Access Manager Administration Console user ID. For example, `admin`
- 6 Enter the Access Manager Administration Console password.
- 7 Re-enter the password for verification.
- 8 The system displays the following confirmation message:

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

- 9 Type **Y** and press Enter.

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

```
Upgrade completed successfully.
```

NOTE: If you have customized the Java settings in the `/opt/novell/nam/idp/conf/tomcat.conf` file, then copy the customized settings to the new file using [Advanced File Configurator](#). See [Modifying Configurations](#) in the [NetIQ Access Manager Appliance 5.0 Administration Guide](#).

6 Migrating Access Manager Appliance

In the earlier releases, Access Manager Appliance upgrade has been done using the `.tar` file. In the 5.0 Service Pack 1 and later versions, Access Manager Appliance is Common Appliance Framework (CAF) based. To upgrade Access Manager 4.5.x to this CAF-based approach, you are required to perform migration.

If you are on Access Manager Appliance 5.0 Service Pack 1, you can directly upgrade to 5.0 Service Pack 2 or later. For more information about upgrade [Chapter 5, “Upgrading Access Manager Appliance,” on page 41](#).

The migration process involves the following actions:

1. Install Access Manager Appliance 5.0 Service Pack 1 as a secondary appliance and point to the 4.5.x primary appliance.
2. After the device is imported, convert Access Manager Appliance 5.0 Service Pack 1 secondary appliance to primary. This is done using the migration script provided with the release.
3. Delete Access Manager Appliance 4.5.x. Follow the steps mentioned in this section to achieve this.
4. Migrate the additional nodes by first removing and then performing a fresh install and reimporting the nodes.

The supported paths for migration are:

- ♦ 4.5 Service Pack 2
- ♦ 4.5 Service Pack 2 Hotfix 1
- ♦ 4.5 Service Pack 2 Hotfix 2
- ♦ 4.5 Service Pack 3
- ♦ 4.5 Service Pack 3 Hotfix 1
- ♦ 4.5 Service Pack 3 Patch 2
- ♦ 4.5 Service Pack 3 Patch 3
- ♦ 4.5 Service Pack 4

This section includes the following topics:

- ♦ [Prerequisites for Migrating Access Manager Appliance](#)
- ♦ [To Migrate Access Manager Appliance](#)
- ♦ [Example Scenario: Access Manager Appliance Migration Using the Existing IP Address](#)

6.1 Prerequisites for Migrating Access Manager Appliance

IMPORTANT: ♦ If three nodes of Access Manager Appliance nodes are installed and configured in the 4.5.x setup, you must uninstall one secondary Access Manager Appliance node before installing 5.0 Service Pack 1 Access Manager Appliance as a secondary node. For more information, see [Restoring a Failed Secondary Console](#). Note that you will be expected to enter Access Manager administrator password at least 5-6 times during the migration process.

Before upgrading, see [Chapter 4, “Prerequisites for Upgrading or Migrating Access Manager Appliance,”](#) on page 37.

In addition to the procedure mentioned in [Restoring Secondary Console](#), perform the following steps as prerequisites before migrating Access Manager Appliance.

Remove any traces of Secondary Access Manager Appliance replicas from the replica ring if you are migrating a primary appliance if you already have three nodes or more and had to remove one of the secondary nodes and before migrating secondary nodes that hold an eDirectory replica which has an Administration Console:

- 1 Log in to Administration Console as a root user.
- 2 Run the `/opt/novell/eDirectory/bin/ndsrepair -P -Ad -a` command. This step might take about 5-7 minutes.
- 3 Select the replica and click **View replica ring**.
Select the name of the secondary server and click **Remove this server from replica ring**.
- 4 Specify the DN of the admin user in leading dot notation. For example, `.admin.novell`.
- 5 Specify the password and select **I Agree**.

6.2 To Migrate Access Manager Appliance

Prerequisites:

- ♦ Ensure that the health nodes of the primary server on 4.5.x version are green and add the 5.0.1 node as the secondary node.

For more information about adding the secondary node, see [Section 2.2, “Installing Access Manager Appliance,”](#) on page 27.

- ♦ Take a backup of the primary Administration Console which is on 4.5.x by using the `ambkup.sh` script located at `/opt/novell/devman/bin`. You will get a `.zip` file with the backup data. Copy this zip file to the 5.0.1 server prior to running the `sb_migrate.sh` script. The migration script asks for the path to this file as part of the migration process.
- ♦ (Conditional) From Access Manager Appliance 5.0 Service Pack 1 Patch 2 onwards, if you have installed Analytics Dashboard, follow the below procedure before migration.
 1. Stop the Administration Console service.
 2. Replace the `appcore.jar` file at `/opt/novell/nam/adminconsole/webapps/roma/WEB-INF/lib` in the Admin console [Primary Access Manager Appliance 4.5.x] for the release that you want to upgrade from, such as Access Manager 4.5.2, 4.5.3, 4.5.4, or 4.5.5.

NOTE: You must replace the `appcore.jar` only if Analytics Server is installed in Access Manager.

3. Restart the Administration Console service.
4. Install Access Manager Appliance 5.0 Service Pack 1 Patch 2 as a secondary node.

To migrate Access Manager Appliance, the administrator needs to carry out steps on the VM as well as the secondary Access Manager Appliance Administration Console. Following are steps required to be performed on the VM:

- 1 Switch off the primary VM which is on 4.5.x.
- 2 Log in as `root` at the secondary Access Manager Appliance and run the `/tmp/NAM5.0.1/sb_migrate.sh` script. Enter `Y` when prompted to confirm.
- 3 Enter `1` when prompted to select the replica number.

```
Select a replica to display an options menu. Enter a replica number(1-1)?
Total number of replicas = 1
PARTITION NAME                                REPLICATION TYPE    REPLICATION STATE
(1).[Root].                                    Read/Write           On
Enter 'q' to escape the operation.
```

- 4 Specify the replica option `5` from the list of 15 options and select **I Agree** when prompted. This option designates the selected server as the new master replica.
- 5 Specify the DN of the admin user in the leading dot notation. For example, `.admin.novell`. Specify the password.
- 6 Specify `1` to specify Root to the prompt.

```
This list shows information for each replica stored on this server.
Select a replica to display an options menu.
PARTITION NAME                                REPLICATION TYPE    REPLICATION STATE
(1).[Root].                                    Master               On
```

- 7 Specify `10` from the 0-15 replica options to view the Replica Ring.
- 8 Select the relevant server number. In the following example, `(1)` is applicable.

```
Finding all servers with replicas
Please Wait...
Replicas Of Partition: .[Root].
Total number of servers in the replica ring = 2
SERVER NAME                                REPLICATION TYPE    REPLICATION STATE
(1).lakhil_sb.novell                        Read/Write           On
(2).ntsdemo.novell                           Master               On
(3)Return to Replica Options
Enter 'q' to escape the operation.
```

- 9 Specify `6` to remove the primary server from the following Server Options:

SERVER OPTIONS

1. Report synchronization status on the selected server
 2. Synchronize the replica on the selected server
 3. Send all objects to every replica in the ring
 4. Receive all objects from the master to this replica
 5. View entire servers name
 6. Remove this server from replica ring
 7. Return to Server List
- Enter 'q' to escape the operation

- 10** Specify the DN of the admin user in the leading dot notation. For example, `.admin.novell`. Specify the password.

You can see the message: The server has been removed from the ring.

- 11** Specify the location of the backup file with absolute path. For example, `/root/nambkup/sb452_20230316_1532.zip`

- 12** (Conditional) Specify the password for decrypting the backup data. Re-enter the password for verification.

After verifying the encrypted password and restoring the certificates, the Access Manager Configuration Backup Utility terminal is displayed.

- 13** Specify the Access Manager Administration password. Re-enter the password for verification.

- 14** After the certificates are restored, enter the Access Manager Administration Console user ID.

- 15** Specify the Access Manager Administration Console password. Re-enter the password for verification.

NOTE: The administrator must wait for the completion of the migration script. The completion status is displayed on the terminal.

Following are steps required to be performed on the 5.0.1 Administration Console:

- 1** Log in to the new Administration Console in a web browser and click **Access Gateways**.
- 2** If the old primary Appliance's Access Gateway is the primary server (shows the red icon next to it), then change the primary Access Gateway server.
 - 2a** Click **[Access Gateway cluster name] > Edit**.
 - 2b** Select a different primary Access Gateway > click **OK > Close**.
Ignore any trust store related warnings.
 - 2c** Click **Update All**.
Wait until the status becomes current for all except the old primary Appliance.
- 3** Click **Troubleshooting**.
- 4** In **Other Known Device Manager Servers**, select the old primary Access Manager Appliance and click **Remove**.
- 5** Remove traces of the old primary Access Manager Appliance from the configuration datastore:
 - 5a** In the Access Manager menu bar, select **View Objects**.
 - 5b** In the Tree view, select **novell**.
 - 5c** Delete all objects that reference the old primary Access Manager Appliance.

You should find the following types of objects:

- ♦ SAS Service object with the hostname of the old primary console
- ♦ Any object that starts with the last octet of the IP address of the old primary console
- ♦ LDAP server object with the hostname of the old primary console
- ♦ LDAP group object with the hostname of the old primary console
- ♦ SNMP Group object with the hostname of the old primary console
- ♦ HTTP Server object with the hostname of the old primary console
- ♦ DNS AG object with the hostname of the old primary console
- ♦ DNS EC AG object with the hostname of the old primary console
- ♦ DNS IP object with the hostname of the old primary console
- ♦ SSL CertificateDNS with the hostname of the old primary console
- ♦ SSL EC CertificateDNS with the hostname of the old primary console
- ♦ SSL CertificateIP with the hostname of the old primary console
- ♦ IP AG object with the hostname of the old primary console
- ♦ IP EC AG object with the hostname of the old primary console
- ♦ NCP server object with the hostname of the old primary console
- ♦ PS object with the hostname of the old primary console

- 6 (Optional) Go to the user store that displays 4.5.x VM IP that was earlier primary machine and replace that with the new primary machine's IP. The health status of Identity Server will change to green.

NOTE: This step is required only if you are using the primary server as the user store in your environment.

6.3 Example Scenario: Access Manager Appliance Migration Using the Existing IP Address

You can migrate secondary Access Manager Appliance using the existing IP address. Consider a scenario where Access Manager Appliance has three nodes, perform the following steps for migration:

- 1 Select one of the three nodes from the cluster. Do not select the primary node.
- 2 Delete the selected node from the cluster.
Remove any traces of the Access Manager Appliance replica from the primary console using the information in [Prerequisites for Migrating Access Manager Appliance](#).
- 3 Clean up the eDirectory objects left in the environment.
- 4 Power off the system.
- 5 Install the Access Manager 5.0 Service Pack 1 Appliance using the IP address of the powered off system.
- 6 Add this as a secondary node in the current environment.

NOTE: It is recommended to use a different host name during the installation if you are planning to use the existing IP address. This is to avoid any failure because of remaining eDirectory objects in the primary console from the old node. To restore custom files, see [Managing Configuration Files](#).

- 7 Perform the migration. The Access Manager Appliance 5.0 Service Pack 1 node will now be the primary node after the migration.
- 8 Switch off the other nodes one after the one after deleting from the cluster.
- 9 Perform a fresh install and add it to the existing cluster.

All the devices will now be on the Access Manager 5.0 Service Pack 1 version.

Perform the migration on only the first node of Access Manager 5.0 Service Pack 1 node and the remaining nodes must be freshly installed.

If you have multiple network interfaces configured in the existing appliance and want to keep all network interfaces in the migrated Access Manager Appliance, ensure that you have configured the required network interfaces in the virtual machine or physical machine before installing Access Manager Appliance.

7 Upgrading Analytics Server

You can upgrade to the 5.0 version of Analytics Server only from the early access beta release and the Analytics Server 4.5 Service Pack 3 Hotfix 1 releases.

Hence, you cannot migrate the existing events realtime or offline indices from any earlier version other than the early access beta release and Analytics Server 4.5 Service Pack 3 Hotfix 1 release to the 5.0 version. However, you can use the new Analytics Server along with the earlier Sentinel-based Analytics Server 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 Server. For more information, see [“Setting Up Logging Server and Console Events”](#) in the *NetIQ Access Manager Appliance 5.0 Administration Guide*.

You cannot launch the old Analytics Server 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](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. Ensure to use only three node cluster for Analytics Server as two node cluster is no longer supported.

NOTE: For upgrading Analytics Server in the cluster environment, see [Section 7.1, “Upgrade Analytics Server Cluster,”](#) on page 50.

Use the following procedure to upgrade Analytics Server.

- 1 Ensure to delete Analytics Server nodes of the earlier version from Administration Console.
- 2 Open a terminal window.
- 3 Log in as the `root` user.
- 4 Download the upgrade file from [Micro Focus Downloads](#) and extract the `tar.gz` file by using the `tar -xzf <filename>` command.

NOTE: For information about the name of the upgrade file, see the specific Release Notes on the [Access Manager Appliance Documentation website \(https://www.netiq.com/documentation/access-manager-45-appliance/\)](https://www.netiq.com/documentation/access-manager-45-appliance/).

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

```
./ar_upgrade.sh
```

6 The system displays the following confirmation message:

```
This will upgrade Analytics Server. Would you like to continue (y/n) ?  
[y]:
```

7 Type **Y** and press Enter.

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. For example, admin

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.
```

7.1 Upgrade Analytics Server Cluster

Follow the below procedure to upgrade Analytics Server in the cluster environment:

1 Take a snapshot of the data from the primary Analytics Server.

For more information, see [Snapshot and Restore](#).

2 Upgrade the analytics servers one by one, for more information, see [Chapter 7, “Upgrading Analytics Server,” on page 49](#).

3 Run `/opt/novell/nam/scripts/restore_elk_objects.sh` script on any one of the nodes.

NOTE: This step is optional if you are upgrading the Analytics Server cluster from 5.0.1 to 5.0.2.

8 Post Upgrade Considerations

In this Chapter

- ♦ [Database Schema Changes for Risk Service](#)
- ♦ [Configuration Files-specific Changes](#)
- ♦ [Changes in Identity Server and Access Gateway Processes](#)
- ♦ [Schema Changes of Attributes](#)

8.1 Database Schema Changes for Risk Service

If you have configured the risk-based authentication, you must upgrade the database schema for the external database feature to work. Perform the following actions after the upgrade:

1. Recompile the custom rules and database-connector jars against the new libraries (NAMCommon.jar, nidp.jar, risk-service-sdk.jar, risk-auth-nidp.jar) and then copy all custom rules and database-connector jars from `/opt/novell/nids/lib/webapp/WEB-INF/lib` to `/opt/novell/rba-core/lib/webapp/WEB-INF/lib`.

NOTE: NIDPlug and RiskLog are not supported.

2. (Conditional) Upgrade the Database Schema for Risk Service.

8.2 Configuration Files-specific Changes

- ♦ **nidp.jar:** Access Manager 5.0 onwards, modification of `nidp.jar` is not recommended. If you have modified `nidp.jar` in the earlier release, then move those properties to `nidp_custom_resources_*.properties` as instructed in [“To Customize Identity Server Messages”](#) and upload the properties file to the Identity Server cluster using Advanced File Configurator. See [“Adding Configurations to a Cluster”](#) in the *NetIQ Access Manager Appliance 5.0 Administration Guide*.

The `jsp_resources_<language>.properties` files are now placed in `/opt/novell/nam/idp/webapp/nidp/WEB-INF/classes/com/novell/nidp/resource/jsp/` and can be directly modified using Advanced File Configurator.

You do not need to extract `nidp.jar`. If you have customized `“jsp_resources_<language>.properties”` in the previous release, extract `nidp.jar` and copy it from `nidp.jar` to `/opt/novell/nam/idp/webapp/nidp/WEB-INF/classes/com/novell/nidp/resource/jsp`.

- ♦ **Advanced Authentication Plug-in file:** The `config.xml` file is moved from `/etc/aaplugin` to `/opt/novell/nam/idp/plugins/aa/`.

♦ **Syslog configuration files:**

File Name	Access Manager 4.5.x and earlier	Access Manager 5.0
nam.conf	/etc/rsyslog.d/	/opt/novell/syslog/rsyslog.d/
Auditlogging.cfg	/etc/	/opt/novell/syslog/rsyslog.d/

- ♦ **JCC file:** The following files are moved from /opt/novell/devman/jcc/conf to /opt/novell/devman/jcc/conf/runtime:

```
clientlist.dat
alertdispatch.dat
tmp.dat
jcc.keystore
jcc.keystore.original
jcc_devman.keystore
keystore_info.xml
keystore_info.xml.original
Settings.properties
```

8.3 Changes in Identity Server and Access Gateway Processes

After upgrading to Access Manager 5.0, the Identity Server and Access Gateway processes running as the root user changes to a non-root user. To run the processes as the root user, see [Java Communication Channel Processes Run as Non-Root User After Upgrading to Access Manager 5.0](#).

8.4 Schema Changes of Attributes

After upgrading to Access Manager 5.0, the object type of attributes changes from octet to stream. This update is made to accommodate larger values in attributes.

9 Getting the Latest OpenSSL Updates for Access Manager Appliance

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

Prerequisites

- ☐ Before upgrading the kernel, ensure that you have updated the operating system to a supported version.
- ☐ Access Manager Appliance installs a customized version of SLES 12 SP5.
- ☐ If you want to install the security updates as they become available, you must have a user account to receive the Linux updates.
- ☐ Ensure that you have obtained the activation code for Access Manager Appliance from [Software Licenses and Downloads](#).

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.

9.1 Installing or Updating Security Patches for Access Manager Appliance

Use the **Online Update** option to register to the online update service from [Software Licenses and Downloads](#). It will get you the latest security updates for Access Manager Appliance. You can select to install updates automatically or manually.

If you want to control the updates further, you can configure Access Manager 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 Manager Appliance receive updates from this server. For more information, see *Subscription Management Tool Guide* (https://www.suse.com/documentation/smt11/book_yep/data/book_yep.html). To obtain the proper credentials to use the SMT server, see “Mirroring Credentials (https://www.suse.com/documentation/smt11/book_yep/data/smt_mirroring_getcredentials.html)” in the *Subscription Management Tool Guide* (https://www.suse.com/documentation/smt11/book_yep/data/book_yep.html).

To activate the Update Channel, you must obtain the key from [Software Licenses and Downloads](#). Use the license key associated with **NAM_APP_5_0** as the part number for Access Manager Appliance Channel 5.0.

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 [Section 1.6, “Setting Up Firewalls,”](#) on page 17.

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 [Micro Focus 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 list of the needed updates and the list of 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.



Troubleshooting Installation and Upgrade

- ♦ [Troubleshooting Installation](#)
- ♦ [Troubleshooting Upgrade](#)

10 Troubleshooting Installation

- [Section 10.1, “Checking the Installation Logs,” on page 59](#)
- [Section 10.2, “Some of New Hardware Drivers or Network Cards Are Not Detected during Installation,” on page 60](#)
- [Section 10.3, “Installation Through Terminal Mode Is Not Supported,” on page 60](#)
- [Section 10.4, “Access Manager Appliance Installation Fails Due to an XML Parser Error,” on page 60](#)
- [Section 10.5, “DN Is Added as Provider ID While Installing the NMAS SAML Method,” on page 60](#)
- [Section 10.6, “Troubleshooting Analytics Server,” on page 61](#)
- [Section 10.7, “Rsyslog Fails to Start After Access Manager Installation,” on page 62](#)

10.1 Checking the Installation Logs

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

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

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

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

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

If this happens, you must upgrade the hardware drivers manually as follows:

- 1 Start the Access Manager Appliance installation.
See [Chapter 2, “Installing Access Manager Appliance,”](#) on page 25.
- 2 Select **Kernel Module (Hardware Driver)** in the main menu, then click **OK**.
- 3 Select **Add Driver Update**, then click **OK**.
- 4 Select the driver update medium.
The driver update medium can be CD-ROM or floppy disk.
- 5 Click **OK** and continue with the installation.

10.3 Installation Through Terminal Mode Is Not Supported

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

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

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

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

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

To resolve this issue, perform the following steps:

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

10.6 Troubleshooting Analytics Server

10.6.1 Dashboard Login Fails After Applying An External Signed Certificate to the Administration Console

Access Manager Dashboard returns `Login Failure. Invalid Username or Password` after assigning an external signed x509 Certificate to the Administration Console.

Issue: Dashboard server is missing the Trusted Root Certificate chain in order to validate the external signed / issued certificate running with the administration console server. Using iManager to assign an external signed certificate to the Administration Console service will not add the required Root Certificates to the Dashboard servers truststore: `/opt/novell/devman/jcc/conf/runtime/jcc_devman.keystore`. Adding the required Root Certificates to the Access Manager Certificates => Trusted Roots will not add certs into the `/opt/novell/devman/jcc/conf/runtime/jcc_devman.keystore`.

Resolution: Use the following steps to manually add the missing Root Certificates into `/opt/novell/devman/jcc/conf/runtime/jcc_devman.keystore`.

- 1 SSH to your dashboard server.
- 2 Create a backup copy of the existing `/opt/novell/devman/jcc/conf/runtime/jcc_devman.keystore`
- 3 Obtain the required password to access the keystore:
 - 3a `cd /opt/novell/devman/jcc/conf`
 - 3b `./ksinfo.sh dump | grep -a2 "jcc_devman.keystore"`
 - 3c Use Keystore Explorer to add the required certificates.

NOTE: Opening the `/jcc_devman.keystore` you will be prompted for the keystore password which we discovered from above mentioned steps.

- 3d Save the changes and restart Analytics Server.

10.6.2 Intermittent Issue With Cluster Configuration

At times the nodes create their own cluster instead of joining the Elasticsearch cluster. In case the Elasticsearch cluster health displays red color in Administration Console user interface for any of the nodes, follow the steps on non-primary nodes only:

- 1 Stop the Elasticsearch service in all the nodes where cluster health is displaying red color. Do not stop the service on the primary server.
- 2 Run the `/opt/novell/nam/scripts/configure_cluster.sh` script on all the non-primary nodes one by one which display the cluster health in red color.

10.7 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 rsyslog 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.

11

Troubleshooting Upgrade

In this Chapter

- ♦ [Access Gateway Throws a 403 Forbidden Page Error for a Resource Protected by a Form Fill Policy](#)
- ♦ [Issue in SSL Communication between Access Gateway and Web Applications](#)
- ♦ [Customized Login Pages Are Missing After Upgrading Access Manager](#)
- ♦ [The Email OTP JSP Page Does Not Render Properly on Internet Explorer 11](#)
- ♦ [X509 Authentication Does Not Work and Throws HTTP 500 Error After Upgrade](#)
- ♦ [Changes Required in server.xml for Apache Tomcat 8.5.51 after Upgrading to Access Manager 4.5 Service Pack 2](#)
- ♦ [Java Communication Channel Processes Run as Non-Root User After Upgrading to Access Manager 5.0](#)
- ♦ [Rsyslog Fails to Start After Access Manager Upgrade](#)

11.1 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**.

11.2 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](#).

11.3 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.

11.4 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, perform the following steps:

- 1 Modify the `nidp_latest.jsp` file.

For information about how to modify a file, see “[Modifying Configurations](#)” in the *NetIQ Access Manager Appliance 5.0 Administration Guide*.

- 2 Add the following entry in the file:

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

 after the first `<%`.

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

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

For more information, see [TID 7022722](#).

11.5 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 `context.xml` file if you have customized it.
- 2 After upgrading Access Manager, add the customized content to the upgraded 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>
```

For more information about how to modify a file, see “[Modifying Configurations](#)” in the *NetIQ Access Manager Appliance 5.0 Administration Guide*.

11.6 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 Modify Access Gateway [server.xml](#).

For information about how to add a file or folder using the Configuration File page, see [“Modifying Configurations”](#) in the *NetIQ Access Manager Appliance 5.0 Administration Guide*.

- 2 Add the `secret required` attribute. Set it to `true` by specifying 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:

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

Access Manager Appliance:

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

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

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

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

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

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

Embedded Service Provider configuration:

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

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

11.7 Java Communication Channel Processes Run as Non-Root User After Upgrading to Access Manager 5.0

After upgrading to Access Manager 5.0, the Java Communication Channel (JCC) processes run as a non-root user in Identity Server and Access Gateway. You can revert the changes to run the process as a root user using the following procedure, which is applicable for both SLES and RHEL operating system:

Access Manager Non-Docker Deployment

- 1 Go to the `/etc/systemd/system/novell-jcc.service` directory.
- 2 Remove the following lines:
 - ♦ `User=novlwww`
 - ♦ `Group=novlwww`
- 3 Execute the following commands:
 - ♦ `systemctl daemon-reload`
 - ♦ `systemctl restart <service_name>`
- 4 Reboot the Identity Server machine.


Access Manager Docker Deployment

Perform the following steps:

- 1 In Administration Console Dashboard, click **Advanced File Configurator**.
- 2 Select **Administration Console**.
- 3 Click the plus icon (+) > **Edit Configurations on the Server**, and specify the following details:

Field	Description
Type	<ol style="list-style-type: none">1. Select File.2. Select <code>novell-jcc.xml</code> in File Name.3. File Path displays the default location for the selected file. Example: <code>/opt/novell/devman/jcc/bin</code>
Cluster Name	This option does not apply to Administration Console.
Source	Select the device from which you want to import the file, and click Fetch File .

Field	Description
File	Click File Editor and perform the following steps: <ol style="list-style-type: none"> 1. Search for <RUN_AS=novlwww>. 2. Modify the value to RUN_AS=root. 3. Click Save.
Restart Administration Console	By default, this option is turned on for novell-jcc. Do not turn it off. You will be prompted to restart Administration Console after sending the configuration change to devices.
Temporary Modification	Turn off the toggle to retain this configuration change in the next Access Manager upgrade.
Modification Type	Select the type of modification from the list. You can specify the type manually if the list does not contain the required type. You can later use this information to search for files that are updated for a specific type. For example, you can search for all files for which Modification Type is Security Setting.
Description	Specify the details of the changes you have made in the file. As you might require to update the configurations many times over the period, you can use these details to track when and what changes were done in the file. You can also use this information as criteria to search for specific files.

- 4 Click **OK**.
- 5 Select novell-jcc that you have modified.
- 6 Click the **Send Configurations to Servers** icon ()
- 7 Click **OK**.
- 8 Restart the service using `/etc/init.d/novell-jcc restart`.

11.8 Rsyslog Fails to Start After Access Manager Upgrade

Scenario:

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

Workaround:

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

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

IV Appendix

This section includes the following topics:

- ♦ [Appendix A, “Configuring Ports 9000 and 9001 to Listen on the Specified Address,” on page 71](#)
- ♦ [Appendix B, “Denormalizing SQL Database,” on page 73](#)

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

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

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

For example:

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

For information about how to modify a file, see [Modifying Configurations](#) in the [NetIQ Access Manager Appliance 5.0 Administration Guide](#).

B 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 Manager 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 <key=value> format.

Download the following c3p0 connection pool libraries from [Maven Repository](#):

- ♦ [c3p0-0.9.2.1.jar](#)
 - ♦ [hibernate-c3p0-4.3.6.Final.jar](#)
 - ♦ [mchange-commons-java-0.2.3.4.jar](#)
-

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

5 Specify the details that you noted in [Step 2](#) in the `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.