



# Migration and Upgrade Guide

## Access Manager 4.0 SP2

June 2015

## Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

**© 2014 NetIQ Corporation. All Rights Reserved.**

For information about NetIQ trademarks, see <https://www.netiq.com/company/legal/>.

---

# Contents

<b>About NetIQ Corporation</b>	<b>5</b>
<b>About this Book and the Library</b>	<b>7</b>
<b>1 Understanding Migration and Upgrade</b>	<b>9</b>
1.1 Planning to Move to Access Manager 4.0 Service Pack 1 . . . . .	9
1.1.1 General Prerequisites . . . . .	9
1.1.2 Understanding Migration and Upgrade . . . . .	10
1.1.3 Assessing Your Current Setup . . . . .	11
1.1.4 Port Details . . . . .	12
1.1.5 IP Address Considerations . . . . .	13
1.2 Order of Migrating/Upgrading the Access Manager Components . . . . .	13
1.3 Limitations . . . . .	13
<b>2 Migrating Access Manager</b>	<b>15</b>
2.1 Migrating Access Manager on SLES . . . . .	15
2.1.1 Migrating Administration Consoles . . . . .	15
2.1.2 Migrating Identity Server . . . . .	24
2.1.3 Migrating 3.1 SP4 or 3.1 SP5 Access Gateway Appliance to 4.0 Access Gateway Appliance . . . . .	31
2.1.4 Migrating SSL VPN . . . . .	40
2.2 Migrating Access Manager on Red Hat From Windows . . . . .	49
2.2.1 Migrating Administration Consoles . . . . .	49
2.2.2 Migrating Identity Server . . . . .	56
2.2.3 Migrating 3.1 SP4 or 3.1 SP5 Access Gateway Appliance to 4.0 Access Gateway Appliance . . . . .	62
2.3 Migrating Access Manager on Windows . . . . .	70
2.3.1 Prerequisites . . . . .	70
2.3.2 Migrating Administration Consoles From Windows 2003 to Windows 2008 . . . . .	71
2.3.3 Migrating the Standalone Identity Servers from Windows 2003 to Windows 2008 . . . . .	73
<b>3 Upgrading Access Manager</b>	<b>75</b>
3.1 Upgrading on Linux . . . . .	75
3.1.1 Upgrading from the Evaluation Version to the Purchased Version . . . . .	75
3.1.2 Upgrading the 3.1 SP4 or 3.1 SP5 Access Gateway Service . . . . .	78
3.1.3 Upgrading to Access Manager 4.0 SP1 . . . . .	80
3.1.4 Applying Access Manager 4.0 Hotfix Patch for Linux . . . . .	87
3.2 Upgrading on Windows . . . . .	89
3.2.1 Prerequisites . . . . .	90
3.2.2 Upgrading from Evaluation Version to the Purchased Version . . . . .	90
3.2.3 Upgrading Access Manager from 3.1 SP4 and 3.1 SP5 to 3.2.2 or 4.0 . . . . .	90
3.2.4 Upgrading Access Manager from 3.2.2 to 4.0 . . . . .	95
3.2.5 Applying Access Manager 4.0 Hotfix* Patch for Windows . . . . .	98
<b>4 Upgrading Kernel to the Latest Linux Security Patch</b>	<b>101</b>
4.1 Installing or Updating Security Patches for the Access Gateway Appliance . . . . .	101
4.2 Configuring Subscription Management Tool for the Access Gateway Appliance . . . . .	102
4.2.1 SMT Configuration . . . . .	103

4.2.2	Configuring the Access Gateway Appliance	103
4.2.3	Troubleshooting	104
4.3	Upgrading the Operating System for Access Gateway Appliance	104

## 5 TroubleShooting 105

5.1	During Primary Administration Console Migration, ndsconfig rm Exits with "Error /opt/novell/eDirectory/bin/ndsconfig return value = 79"	105
5.2	While Migrating 3.1 SP4 Access Gateway with SSL VPN, ESP is in a Halted State After Rip and Replace	106
5.3	When Migration to 4.0 Access Manager Terminates Abruptly	106
5.4	Migration Exits Stating That the Server's DIB Does Not Contain Replicas	107
5.5	Exception During the Access Gateway Migration	107
5.6	Device Is Not Reachable After Migrating From the 3.1 SP4 Access Gateway Appliance to Access Gateway Appliance	108
5.7	Service Provider Does Not Start	108
5.8	The Access Gateway Throws a 403 Forbidden Page Error for a Resource Protected by a Form Fill Policy	108
5.9	Datastore Authentication Error, Bad Password or Certificate	108
5.10	DN Is Added as Provider ID While Installing NMAS SAML Method	109
5.11	Troubleshooting a Linux Administration Console Upgrade	109
5.11.1	Upgrade Hangs	109
5.11.2	Multiple IP Addresses	110
5.11.3	Certificate Command Failure	110
5.12	WS-Trust Service Provider Attributes Sets Have to be Reconfigured After Upgrading Access Manager From 4.0 to 4.0 SP1	110
5.13	Unable to Access Identity Server Configuration Page After Upgrading from 3.2 SP3 to 4.0 SP1	111

## A Utility Scripts 113

---

# About NetIQ Corporation

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

## Our Viewpoint

### **Adapting to change and managing complexity and risk are nothing new**

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

### **Enabling critical business services, better and faster**

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

## Our Philosophy

### **Selling intelligent solutions, not just software**

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

### **Driving your success is our passion**

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

## Our Solutions

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

## Contacting Sales Support

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

<b>Worldwide:</b>	<a href="http://www.netiq.com/about_netiq/officelocations.asp">www.netiq.com/about_netiq/officelocations.asp</a>
<b>United States and Canada:</b>	1-888-323-6768
<b>Email:</b>	<a href="mailto:info@netiq.com">info@netiq.com</a>
<b>Web Site:</b>	<a href="http://www.netiq.com">www.netiq.com</a>

## Contacting Technical Support

For specific product issues, contact our Technical Support team.

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

## Contacting Documentation Support

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

## Contacting the Online User Community

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

---

# About this Book and the Library

This documentation describes how to migrate and upgrade Access Manager components to a higher version.

## Intended Audience

This guide is intended for network administrators, installers, and consultants who are involved in upgrading or migrating to Access Manager 4.0.

## Other Information in the Library

The library provides the following information resources:

- ♦ [\*NetIQ Access Manager 4.0 SP2 Installation Guide\*](#)
- ♦ [\*NetIQ Access Manager 4.0 SP1 Administration Console Guide\*](#)
- ♦ [\*NetIQ Access Manager 4.0 SP1 Best Practices Guide\*](#)
- ♦ [\*NetIQ Access Manager 4.0 SP1 Identity Server Guide\*](#)
- ♦ [\*NetIQ Access Manager 4.0 SP1 Access Gateway Guide\*](#)
- ♦ [\*NetIQ Access Manager 4.0 SSL VPN User Guide\*](#)

---

**NOTE:** Contact [namsdk@netiq.com](mailto:namsdk@netiq.com) for any query related to Access Manager SDK.

---





---

# 1 Understanding Migration and Upgrade

A basic Access Manager installation has three Access Manager components (an Administration Console, an Identity Server, and an Access Gateway), an LDAP server, and Web servers with applications and data.

By moving to the Access Manager 4.0 Service Pack 1 release, you get all the important fixes and features that enhance the existing capabilities of the product.

The following sections in this chapter explain how to move to Access Manager 4.0 Service Pack 1.

- ♦ [Section 1.1, “Planning to Move to Access Manager 4.0 Service Pack 1,” on page 9](#)
- ♦ [Section 1.2, “Order of Migrating/Upgrading the Access Manager Components,” on page 13](#)
- ♦ [Section 1.3, “Limitations,” on page 13](#)

## 1.1 Planning to Move to Access Manager 4.0 Service Pack 1

In this release of Access Manager, all components are native 64-bit applications running on 64-bit architecture.

---

**IMPORTANT:** Migration from Access Manager 3.1 SP4 or 3.1 SP5 to Access Manager 4.0 SP1 or a higher version is not supported.

To move to Access Manager 4.0 SP1 or a higher version, first migrate Access Manager 3.1 SP4 or 3.1 SP5 to 4.0 and then upgrade to the latest release of Access Manager 4.0 Service Pack 1. For information about upgrading and migrate upgrade paths, [Upgrading Access Manager](#).

---

This section contains details on the following:

- ♦ [Section 1.1.1, “General Prerequisites,” on page 9](#)
- ♦ [Section 1.1.2, “Understanding Migration and Upgrade,” on page 10](#)
- ♦ [Section 1.1.3, “Assessing Your Current Setup,” on page 11](#)
- ♦ [Section 1.1.4, “Port Details,” on page 12](#)
- ♦ [Section 1.1.5, “IP Address Considerations,” on page 13](#)

### 1.1.1 General Prerequisites

Ensure that you meet the following requirements before you decide to move to Access Manager 4.0 Service Pack 1:

- ☐ For upgrade: You are currently on Access Manager 3.2 SP2 or higher.
- ☐ All components are configured to the same Network Time Protocol (NTP) server. This is required to synchronize the time across all components.

- ☐ You have physical access to the server or server console (in case of VMWare setups) as a root user and are familiar with firewall configurations. The required ports also must be opened in the firewall. For more information about the ports, see [Section 1.1.4, “Port Details,” on page 12](#).
- ☐ You have read and understood the network requirements. For details, see “[Network Requirements](#)” in the *NetIQ Access Manager 4.0 SP2 Installation Guide*.

## 1.1.2 Understanding Migration and Upgrade

- ♦ “[What is Migration?](#)” on page 10
- ♦ “[What is Upgrade?](#)” on page 10

### What is Migration?

Migration is the process in which you install the latest version of Access Manager on a new server and then migrate the existing data to the new server.

During the migration process you can either provide a new IP address and host name or reuse an existing IP address.

---

**IMPORTANT:** The host name of the new 4.0 Administration Console must be different from the existing primary and secondary Administration Consoles.

---

Migration can be used in the following cases:

- ☐ You are on a 32-bit architecture and you need to move to a 64-bit architecture. For example, your existing setup is on a 32-bit SLES (SUSE Linux Enterprise Server) 10 SP2 and you plan to move to a 64-bit SLES 11 SP2 or SP3 operating system.
- ☐ You are on a 32-bit architecture and you need to move to a 64-bit architecture. For example, your existing setup is on a 32-bit Windows 2003 and you plan to move to a 64-bit Red Hat 6.4, 6.5 or 6.6 version.
- ☐ You have an existing 64-bit architecture but your operating system is 32-bit. For example, you have a 64-bit server on which a 32-bit operating system is installed.
- ☐ You plan to re-architecture your Access Manager setup. For example, you already have one Administration Console installed but you plan to add one more Administration Console to the setup.

### What is Upgrade?

Upgrade is the process through which the existing components are moved to a higher version on the same machine. As the underlying operating system does not change, this process is also referred to as an in-place upgrade.

Upgrade can be used in a scenario where you are already on a 64-bit architecture setup. During the process of upgrade, the existing IP addresses and hardware are reused.

For example: If you are already on Windows 2008 64-bit platform, you can directly upgrade to Access Manager 4.0. For more information, see *Upgrading Access Manager from 3.1 SP4 and 3.1 SP5 to 3.2.x or 4.0* in the *NetIQ Access Manager 4.0 Migration and Upgrade Guide*.

In addition to the migrate and upgrade process described above, you can also choose to install Access Manager 4.0 Service Pack 1 on a new 64-bit setup. After manually reconfiguring and confirming that the new 4.0 Service Pack 1 setup is working fine, you can decommission the old setup.

---

**IMPORTANT:** To avoid service disruptions, you can install Access Manager 4.0 Service Pack 1 devices such as Identity Provider, Access Gateway Service and SSL VPN on a new 64-bit server and then add them to the existing cluster. When the version 4.0 Service Pack 1 setup is functional, you can de-commission the old setup.

---

### 1.1.3 Assessing Your Current Setup

Before you decide to upgrade or migrate, it is important to assess your current setup in terms of version of Access Manager and components installed, hardware, and operating system.

- ♦ **Current Version of Access Manager:** Before you upgrade to Access Manager 4.0 Service Pack 1, ensure that you are on Access Manager 3.2 Service Pack 2 or higher.
- ♦ **Current Hardware:** If your current operating system is on a 32-bit architecture, migrate to a 64-bit architecture. This is required because all the components of Access Manager 4.0 are on 64-bit architecture.
- ♦ **Current Operating System:** You can move to Access Manager 4.0 from a SLES platform or a Windows platform.

You are on SLES: To move to Access Manager 4.0, the operating system must be SLES 11 SP2 or SP3 (64-bit). If you are on SLES 10.x, upgrade to SLES 11 SP2 or SP3(64-bit) operating system.

You are on Windows: If your current operating system is Windows 2008, you can directly upgrade to Access Manager 4.0. But if your current operating system is Windows 2003, migrate to Windows 2008 and then install Access Manager 4.0.

- ♦ **Access Manager components:** Identify the combination of Access Manager components that are currently installed in your setup. This will help you determine if you need to upgrade, migrate or do a combination of both.

For example, assume you have Administration Console and Identity Server installed in Windows 2008 and the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance.

In this scenario, you will first upgrade the Administration Console and the Identity Server. But the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance needs to be migrated to 4.0 Access Gateway Appliance.

## Determining Whether to Migrate or Upgrade

The following table indicates if you must migrate or upgrade based on your existing setup:

**Table 1-1** *Determining the Path to Move to Access Manager 4.0*

Platforms	Windows 2003	Windows 2008	SLES
Administration Console/ Identity Server	Migrate	Upgrade  For more information see, <ul style="list-style-type: none"><li>♦ <a href="#">Upgrading the Administration Console</a></li><li>♦ <a href="#">Upgrading the Identity Server</a></li></ul> Migrate	Migrate
Access Gateway Appliance (also known as Linux Access Gateway)	NA	Migrate	Migrate
Access Gateway Service	NA	Upgrade  For more information, see <a href="#">Upgrading the Access Gateway Service</a>	Upgrade  For more information see, <a href="#">Upgrading the 3.1 SP4 or 3.1 SP5 Access Gateway Service</a>
SSL VPN	NA	NA	Migrate

### 1.1.4 Port Details

In version 4.0, the Administration Console, Identity Server and SSL VPN run in separate instances of tomcat. By default, each component's tomcat uses ports 8080 (http) and 8443 (https). Installing multiple components on the same server can cause a port conflict. To avoid this conflict, each component is assigned a unique port number on which the device can listen.

If a component is installed on a dedicated server no port changes are required. By default, the http port is 8080 and the https port is 8443.

The browser requests made to ports 8080/8443 are automatically redirected to the port on which the component is listening. Depending on the configuration, you must open ports 2080, 2443, and 3443 in the firewall.

The following table describes the ports for all the components of Access Manager:

Configuration	Identity Server	Administration Console	SSL VPN
Access Gateway + SSL VPN	NA	NA	8080/8443
Administration Console + SSL VPN	NA	2080/2443	8080/8443

Configuration	Identity Server	Administration Console	SSL VPN
Administration Console only	NA	8080/8443	NA
Identity Server + Administration Console	8080/8443	2080/2443	NA
Identity Server + Administration Console + SSL VPN	8080/8443	2080/2443	3080/3443
Identity Server + SSL VPN	8080/8443	NA	3080/3443
Identity Server only	8080/8443	NA	NA
SSL VPN only	NA	NA	8080/8443

### 1.1.5 IP Address Considerations

Before you migrate to the Access Manager 4.0 setup, you must decide if you want to reuse your existing IP address or use a new IP address to setup the system.

If you are already on a 64-bit architecture (the older version of Access Manager is installed on a 64-bit hardware), you can choose to reuse the existing IP address, whereas if you have decided to move to new 64-bit servers, you must use new IP addresses.

**NOTE:** For the primary Administration Console migration, you will need a new IP address, that will be temporarily used by the new 4.0 Administration Console. During the migration process, this new IP address is replaced with the original old Administration Console IP address.

## 1.2 Order of Migrating/Upgrading the Access Manager Components

Whether you need to upgrade or migrate, it is important that you move each component in the following order. Doing this will ensure that the integrity of the application and data is maintained.

1. Administration Console
2. Identity Server
3. Access Gateway Appliance
4. SSL VPN

## 1.3 Limitations

- ♦ Cross-platform migrations are currently not supported. For example, it is not possible to migrate from Access Manager installed in a SLES environment to a Windows environment and vice versa.
- ♦ NetIQ Access Manager Appliance (single-box solution) deployment is supported only for new installations. You cannot migrate from Access Manager to Access Manager Appliance 4.0.

- ♦ Migration from the Access Gateway Appliance to the Access Gateway Service and vice versa is not supported.
- ♦ Cookie mangling should not be enabled in the mixed-mode cluster. The 3.1 SP4 or 3.1 SP5 Access Gateways do not understand mangled cookies.

---

# 2 Migrating Access Manager

Migration is the process in which you install the latest version of Access Manager on a new server and then migrate the existing data to the new server.

During the migration process you can either provide a new IP address and host name or reuse an existing IP address.

You can perform migration on a SLES 11 or a Windows 2003 server. If you are on Windows 2008, you must upgrade to Access Manager 4.0.

- ♦ [Section 2.1, “Migrating Access Manager on SLES,” on page 15](#)
- ♦ [Section 2.2, “Migrating Access Manager on Red Hat From Windows,” on page 49](#)
- ♦ [Section 2.3, “Migrating Access Manager on Windows,” on page 70](#)

---

**NOTE:** If you encounter any errors while migrating, see [Chapter 5, “TroubleShooting,” on page 105](#).

---

## 2.1 Migrating Access Manager on SLES

- ♦ [Section 2.1.1, “Migrating Administration Consoles,” on page 15](#)
- ♦ [Section 2.1.2, “Migrating Identity Server,” on page 24](#)
- ♦ [Section 2.1.3, “Migrating 3.1 SP4 or 3.1 SP5 Access Gateway Appliance to 4.0 Access Gateway Appliance,” on page 31](#)
- ♦ [Section 2.1.4, “Migrating SSL VPN,” on page 40](#)

### 2.1.1 Migrating Administration Consoles

- ♦ [“Prerequisites for the Administration Console Migration” on page 15](#)
- ♦ [“Migration Scenarios for the Administration Console” on page 17](#)
- ♦ [“Migrating the Primary Administration Console” on page 18](#)
- ♦ [“Migrating the Secondary Administration Console” on page 21](#)

#### Prerequisites for the Administration Console Migration

In addition to the following prerequisites, ensure that you also meet the hardware requirements for the Administration Console. For details, see [“Installation Requirements on Linux”](#) in the *NetIQ Access Manager 4.0 SP2 Installation Guide*.

- ☐ A new IP address, that will be temporarily used during the Primary Administration Console migration.
- ☐ Timeout Per Protected Resource (TOPPR) is enabled and applied in the Access Gateway. In the Administration Console, click **Devices > Access Gateways > Edit**, then click **Enable Timeout Per Protected Resource**.

If the **Enable Timeout Per Protected Resource** option has already been applied, it will not be displayed on the screen.

- ☐ The primary and secondary 3.1 SP4 or 3.1 SP5 Administration Console time is synchronized. You can synchronize the time by enabling the Network Time Protocol (NTP) server through YaST. To do this, go to **YaST > Network Services > NTP Configuration** page.
- ☐ The new 4.0 Administration Console that you want to install should be on the same subnet as the existing primary console.
- ☐ The health statuses for all devices in the Administration Console are green in color.  
For more information, see “[Viewing Device Health](#)” in the *NetIQ Access Manager 4.0 SP1 Administration Console Guide*.
- ☐ You have physical access to the server or server console (in case of VMWare setups) as a root user and you are familiar with iptables.  
The required ports are opened in the firewall. For more information about ports, see [Section 1.1.4, “Port Details,” on page 12](#).
- ☐ Note down the contracts selected under the **Satisfies contract** list of SAML2.0 and Liberty identity providers. These are under **Devices > Identity Servers > Edit > [Protocol] > [IdentityProvider] > Authentication Card**.  
The application interface for this feature has changed in version 4.0. You must manually configure these contracts after migration. This configuration will be effective after the Identity Server migration is done.  
(Optional) If federation is configured, see the contracts configured for 3.1 SP4 or 3.1 SP5, and navigate to **Administration Console > Devices > Identity Servers > Edit > [Protocol] > [Identity Provider] > Authentication Card**. The **Satisfies Contract** field lists all the configured contracts.
- ☐ The host name of the new 4.0 Administration Console should be different from the existing primary and secondary Administration Consoles.
- ☐ Ensure that the `/etc/hosts` file of the system where you are installing Access Manager 4.0 has the host name and IP address for the new 4.0 Administration Console server. If the hostname of the Administration Console is not listed in DNS, the `/etc/hosts` file is used to resolve the hostname of the machine to a valid IP address.

---

**WARNING:** If three Administration Consoles are already installed and configured in the existing setup, uninstall one secondary Administration Console before running the `install_and_migrate.sh` script.

For more information about how to deconfigure and uninstall the Administration Console, see [Step 12 on page 20](#) and “[Uninstalling the Linux Administration Console](#)” in the *NetIQ Access Manager 4.0 SP2 Installation Guide*.

---



## Migration Scenarios for the Administration Console

The following scenarios are supported for migrating NetIQ Access Manager from 3.1 SP4 and 3.1 SP5 to 4.0 on Linux.

---

**IMPORTANT:** Ensure that you identify the scenario that best describes your migration environment and review the appropriate steps before you begin the process of migration.

---

- ♦ [“Administration Console, Identity Server, 3.1 SP4 or 3.1 SP5 Access Gateway Appliance, and SSL VPN Are Installed on Different Servers” on page 17](#)
- ♦ [“Administration Console and Identity Server Are on the Same Server, and 3.1 SP4 or 3.1 SP5 Access Gateway Appliance Is on a Different Server” on page 17](#)
- ♦ [“Secondary Administration Console and Identity Server are on the Same Server” on page 17](#)
- ♦ [“The Administration Console, Identity Server, and SSL VPN Are on the Same Server” on page 18](#)

### **Administration Console, Identity Server, 3.1 SP4 or 3.1 SP5 Access Gateway Appliance, and SSL VPN Are Installed on Different Servers**

Workflow:

- 1 Migrate the Administration Consoles.
- 2 Migrate the Identity Server.
- 3 Migrate the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance to the 4.0 Access Gateway Appliance.
- 4 Migrate the SSL VPN from 3.1 SP4 or 3.1 SP5 to 4.0.

### **Administration Console and Identity Server Are on the Same Server, and 3.1 SP4 or 3.1 SP5 Access Gateway Appliance Is on a Different Server**

Workflow:

- 1 Migrate the primary Administration Console.
- 2 Migrate the Identity Server.
- 3 Migrate the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance to the 4.0 Access Gateway Appliance.

### **Secondary Administration Console and Identity Server are on the Same Server**

Workflow:

- 1 Migrate the primary Administration Console.
- 2 Migrate the secondary Administration Console.
- 3 Migrate the Identity Server.

## The Administration Console, Identity Server, and SSL VPN Are on the Same Server

Workflow:

- 1 Migrate the Administration Consoles.
- 2 Migrate the Identity Server.
- 3 Migrate SSL VPN.

---

**NOTE:** If the device has multiple interfaces, use YaST to manually configure the primary IP address on each NIC.

To do this, go to *YaST > Network Devices > Network Settings > Overview*. Select the network card and click *Edit*. Enter the primary IP address. Click *Next > Ok > Quit*.

---

## Migrating the Primary Administration Console

---

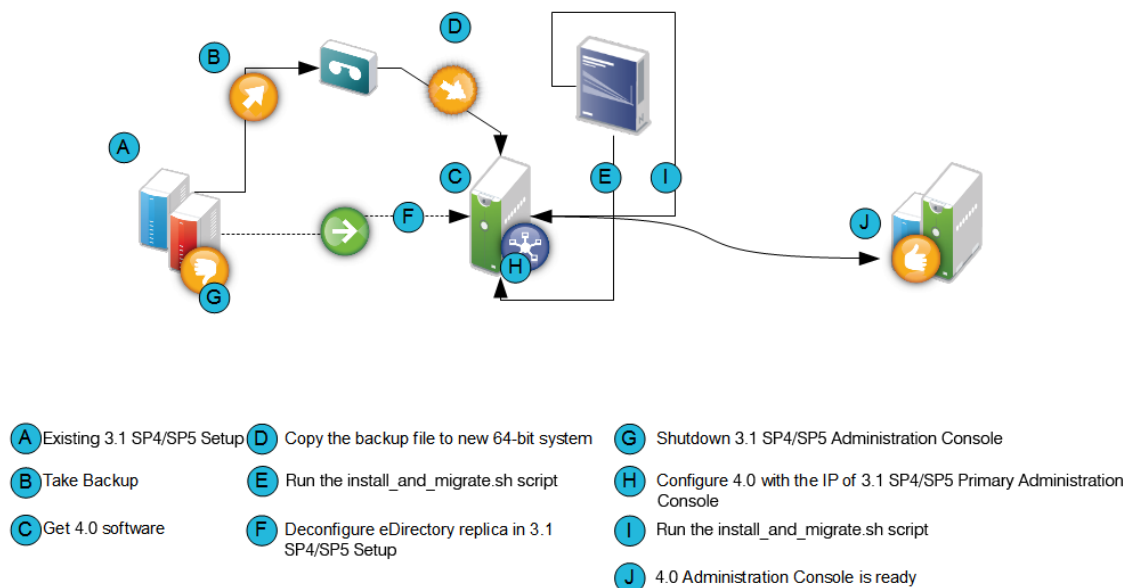
**IMPORTANT:** Before you proceed with the steps for migration, ensure that you have followed the instructions in the [Prerequisites for the Administration Console Migration](#).

If you have multiple components installed on the same system, before starting migration of any component, ensure that you read the migration prerequisites of all components.

---

### Migration Process

**Figure 2-1** Process of Migration of the Primary Administration Console



- 1 Back up the 3.1 SP4 or 3.1 SP5 primary Administration Console configuration by using the `/opt/novell/devman/bin/ambkup.sh` script.

Remember the password that you enter while saving the backup file. You will need this password in [Step 10](#).

The NetIQ Access Manager backup file is used only for restoring the certificates. The rest of the data is synchronized through eDirectory replication.

For more information about how to perform a backup, see [“Backing Up and Restoring”](#) in the *NetIQ Access Manager 4.0 SP1 Administration Console Guide*.

---

**IMPORTANT:** It is strongly recommended that you review the log file to confirm if the backup process was completed without any errors.

---

- 2 Copy the backup zip file to `/tmp` or any other folder on the new 64-bit server where you plan to install the 4.0 Administration Console.

Make a note of the location and file name in absolute format. You need to provide this information in the installation and migration script (for example, `/tmp/idpq_20120111_1314.zip`).

- 3 Ensure you have downloaded the software or you have the CD available.

- 4 Do one of the following:

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

```
cd /media
```

Browse to your CD-ROM drive.

- ♦ If you downloaded the `AM_40_AccessManagerService_Linux64.tar.gz` file, unpack the file using the following command:

```
tar -xzf AM_40_AccessManagerService_Linux64.tar.gz
```

- 5 Browse to the `novell-access-manager` folder.

All the files are extracted to the `novell-access-manager` folder.

- 6 Run the `install_and_migrate.sh` script from the folder to migrate the primary Administration Console from 3.1 SP4 or 3.1 SP5 to 4.0.

Ensure that you install the 4.0 Administration Console in the same subnet as the 3.1 SP4 or 3.1 SP5 Administration Console. For more information about the ports, see [Section 1.1.4, “Port Details,”](#) on page 12.

---

**NOTE:** Ensure that there is no duplicate entry of the host name in the `/etc/hosts` file.

---

- 7 Type `y` and press Enter when the system prompts you.
- 8 Accept the license agreement by entering `y` when the system prompts you.
- 9 Type `y` and press Enter when the system displays the confirmation message.
- 10 Provide the following details:

**3.1 Primary Administration Console IP address:** Enter the 3.1 SP4 or 3.1 SP5 primary IP address. Ensure that the IP address is static.

**Access Manager Administration user ID:** Enter the administrator user ID.

**Access Manager Administration password:** Enter the administrator password. Re-enter the password for verification.

**Enter the backup file with absolute path:** Enter the absolute path of the backup file that you created in [Step 1](#).

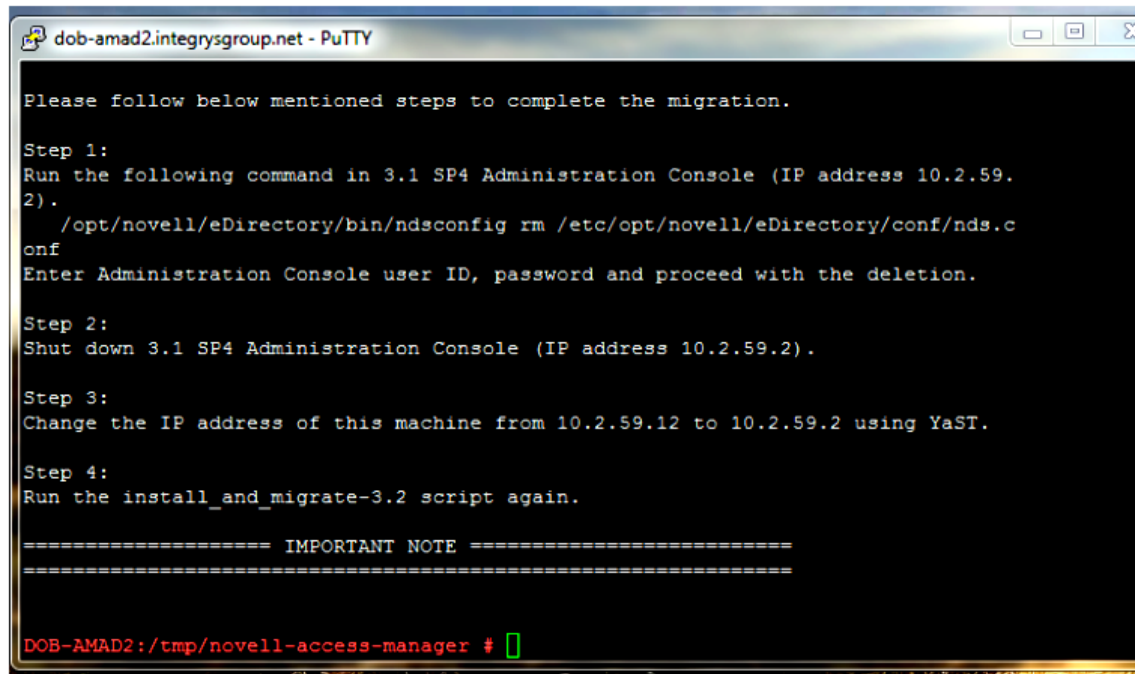
**Enter a password for decrypting the data:** Enter the private key encryption password of the backup file. Re-enter the password for verification.

---

**NOTE:** To view installation progress, refer to the log files in `/tmp/novell_access_manager`.

---

After installing the 4.0 Administration Console, the system displays the following:



```
dob-amad2.integritysgroup.net - PuTTY

Please follow below mentioned steps to complete the migration.

Step 1:
Run the following command in 3.1 SP4 Administration Console (IP address 10.2.59.2) .
    /opt/novell/eDirectory/bin/ndsconfig rm /etc/opt/novell/eDirectory/conf/nds.conf
Enter Administration Console user ID, password and proceed with the deletion.

Step 2:
Shut down 3.1 SP4 Administration Console (IP address 10.2.59.2).

Step 3:
Change the IP address of this machine from 10.2.59.12 to 10.2.59.2 using YaST.

Step 4:
Run the install_and_migrate-3.2 script again.

===== IMPORTANT NOTE =====
=====

DOB-AMAD2:/tmp/novell-access-manager #
```

- 11 Verify if the 4.0 Access Manager server is functional. Perform one of the following steps from the 4.0 terminal:
  - 11a Run `/opt/novell/eDirectory/bin/ndsstat -r` command. This lists all the replicas available. Verify that the status of the 4.0 replica is On.
  - 11b Run `/opt/novell/eDirectory/bin/ldapsearch -A -LLL -b "ou=accessManagerContainer,o=novell" -D "cn=<username>,o=novell" -w <password>` command. This lists all the objects in the NAM container. You can run the same command on the 3.1 SP4 or 3.1 SP5 terminal to verify if the object list is complete and accurate.
- 12 In the Access Manager 3.1 SP4 or 3.1 SP5 Administration Console, run the following command to deconfigure the eDirectory replica in the 3.1 SP4 or 3.1 SP5 server:

```
/opt/novell/eDirectory/bin/ndsconfig rm /etc/opt/novell/eDirectory/conf/nds.conf
```

  - 12a Enter admin credentials in the `admin.novell` format and proceed with deletion.  
The system displays the following warning:  
  
Deconfiguring Novell eDirectory might cause problems in the operation of modules dependent on eDirectory. Do you wish to continue? (y/n)
  - 12b Enter `y` to proceed with deletion.  
After deletion, the following message will be displayed:  
  
Deconfiguration of eDirectory server is complete.  
The instance at `/etc/opt/novell/eDirectory/conf/nds.conf` is successfully removed.  
Stopping the service 'ndsd'... Done
- 13 Shut down the 3.1 SP4 or 3.1 SP5 Administration Console.

- 14 In the Access Manager 4.0 Administration Console, use YaST to change the IP address to the old primary Administration Console IP address:

14a Go to **YaST > Network Devices > Network Settings > Overview**.

---

**NOTE:** Launch YaST from the physical server or if you are using a virtual machine, use the console. We do not recommend that you use a remote connection for changing the IP address, since you may lose the remote connection.

---

14b Select the network card and click **Edit**.

14c Change the IP address to the 3.1 SP4 or 3.1 SP5 primary Administration Console IP address.

14d Click **Next > Ok > Quit**.

- 15 Run the `install_and_migrate.sh` script from the `novell-access-manager` folder again to complete the installation. A confirmation message is displayed.

15a Enter `y` and the following message is displayed:

```
Installation will continue to finish the rest of the 4.0 migration tasks
Would you like to continue this installation (y/n)?
```

15b Enter `y` and then provide the following details:

- ♦ Enter the Access Manager Administration user ID.
- ♦ Enter the Access Manager Administration password.
- ♦ Re-enter the password for verification.

After migration is complete, the system displays the following message:

```
4.0 Administration Console migration completed successfully.
```

## Migrating the Secondary Administration Console

To install the secondary Administration Console you can either use a new server that supports a 64-bit installer to install the secondary Administration Console or you can reuse the existing server for installation if it supports the 64-bit installer.

To migrate the secondary Administration Console to 4.0, use one of the following procedures:

- ♦ [“Using a New Server for the Secondary Administration Console” on page 22](#)
- ♦ [“Reusing the Existing Server or IP Address for the Secondary Administration Console” on page 23](#)

## Using a New Server for the Secondary Administration Console

---

**IMPORTANT:** Before you install the 4.0 secondary Administration Console on a 64-bit server, it is important to de-commission the 3.1 SP4 or 3.1 SP5 secondary Administration Console. This process helps ensure that the number of Administration Consoles do not exceed three instances.

---

- 1 Verify if the 4.0 Access Manager server is functional. Perform one of the following steps from the 4.0 terminal:

- 1a Run `/opt/novell/eDirectory/bin/ndsstat -r` command. This lists all the replicas available. Verify that the status of the 4.0 replica is On.

- 1b Run `/opt/novell/eDirectory/bin/ldapsearch -A -LLL -b "ou=accessManagerContainer,o=novell" -D "cn=<username>,o=novell" -w <password>` command. This lists all the objects in the NAM container. You can run the same command on the 3.1 SP4 or 3.1 SP5 terminal to verify if the object list is complete and accurate.

- 2 Run the following command to delete the eDirectory replica in the 3.1 SP4 or 3.1 SP5 secondary Administration Console server:

```
/opt/novell/eDirectory/bin/ndsconfig rm /etc/opt/novell/eDirectory/conf/nds.conf
```

- 3 Enter admin credentials in the `admin.novell` format and proceed with deletion.

- 4 Log in to the 4.0 primary Administration Console.

- 5 Click **Auditing > Troubleshooting > Other Known Device Manager Servers**.

- 6 Click **Remove** for this server.

- 7 Install the 64-bit SLES 11 SP2 or SP3 on the new 64-bit server with a *different host name*.

- 7a Go to **YaST > Network Devices > Network Settings > Overview**.

- 7b Select the network card and click **Edit**.

- 7c Specify a different host name.

For more information, see *SLES 11 Installation Quick Start* ([http://www.suse.com/documentation/sles11/book\\_quickstarts/data/book\\_quickstarts.html](http://www.suse.com/documentation/sles11/book_quickstarts/data/book_quickstarts.html)).

- 8 Ensure that you have downloaded the software or you have the CD available.

- 9 Do one of the following:

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

```
cd /media
```

Browse to your CD-ROM drive.

- ♦ If you downloaded the `AM_40_AccessManagerService_Linux64.tar.gz` file, unpack the file using the following command:

```
tar -xzf AM_40_AccessManagerService_Linux64.tar.gz
```

- 10 Browse to the `novell-access-manager` folder.

All the files are extracted to the `novell-access-manager` folder.

## Reusing the Existing Server or IP Address for the Secondary Administration Console

To use the existing server for installing the secondary Administration Console, ensure it is a 64-bit server.

- 1 Verify if the 4.0 Access Manager server is functional. Perform one of the following steps from the 4.0 terminal:
  - 1a Run `/opt/novell/eDirectory/bin/ndsstat -r` command. This lists all the replicas available. Verify that the status of the 4.0 replica is On.
  - 1b Run `/opt/novell/eDirectory/bin/ldapsearch -A -LLL -b "ou=accessManagerContainer,o=novell" -D "cn=<username>,o=novell" -w <password>` command. This lists all the objects in the NAM container. You can run the same command on the 3.1 SP4 or 3.1 SP5 terminal to verify if the object list is complete and accurate.
- 2 Run the following command to delete the eDirectory replica in the 3.1 SP4 or 3.1 SP5 secondary Administration Console server:

```
/opt/novell/eDirectory/bin/ndsconfig rm /etc/opt/novell/eDirectory/conf/nds.conf
```
- 3 Enter the admin credentials in `admin.novell` format and proceed with deletion.
- 4 Log in to the 4.0 primary Administration Console.
- 5 Click **Auditing > Troubleshooting > Other Known Device Manager Servers**.
- 6 Click **Remove** for this server.
- 7 Format the server with the 64-bit SLES 11 SP2 or higher operating system and a different host name or configure the same IP address with a different host name.
  - 7a Go to **YaST > Network Devices > Network Settings > Overview**.
  - 7b Select the network card and click **Edit**.
  - 7c Specify a different host name.

---

**IMPORTANT:** Even after formatting the server, old certificates are not cleaned up from the user store. If you are using an existing host name during Access Manager installation, it may lead to a conflict with the existing certificates. It is recommended to use a different host name during IP address configuration.

---

- 8 Ensure you have downloaded the software or you have the CD available.
- 9 Do one of the following:
  - ♦ Insert the CD into the drive, then navigate to the device. Enter the following:

```
cd /media
```

Browse to your CD-ROM drive.
  - ♦ If you downloaded the `AM_40_AccessManagerService_Linux64.tar.gz` file, unpack the file using the following command:

```
tar -xzvf AM_40_AccessManagerService_Linux64.tar.gz
```
- 10 Browse to the `novell-access-manager` folder.

All the files are extracted to the `novell-access-manager` folder.

- 11 Install the secondary Administration Console by using the `install.sh` script.

For more information about how to install the secondary Administration Console, see [“Installing Secondary Versions of the Administration Console”](#) in the *NetIQ Access Manager 4.0 SP1 Setup Guide*.

---

**NOTE:** If the secondary Administration Console migration exits stating that the Server’s DIB does not contain replicas, see [Section 5.4, “Migration Exits Stating That the Server’s DIB Does Not Contain Replicas,”](#) on page 107.

---

## 2.1.2 Migrating Identity Server

- ♦ [“Prerequisites for the Identity Server Migration”](#) on page 24
- ♦ [“Reusing an Existing IP Address”](#) on page 25
- ♦ [“Using a New IP Address”](#) on page 26
- ♦ [“Process of Migration”](#) on page 28

It is recommended that you replace the Identity Servers individually. The 3.1 SP4 or 3.1 SP5 and 4.0 Identity Servers can coexist until the migration is complete.

### Prerequisites for the Identity Server Migration

In addition to the following prerequisites, ensure that you also meet the hardware and software requirements for the Identity Server. For details, see [“Installation Requirements on Linux”](#) in the *NetIQ Access Manager 4.0 SP2 Installation Guide*.

- ♦ The Identity Server can perform a DNS resolution with the ESP (Embedded Service Provider) host name of the Access Gateway.

For more information, see [“DNS Name Resolution”](#) in the *NetIQ Access Manager 4.0 SP1 Identity Server Guide*.

- ♦ The Identity Server time is synchronized with the time of the Administration Console. You can synchronize the time by enabling the Network Time Protocol (NTP) server through YaST. To do this, go to **YaST > Network Services > NTP Configuration**.
- ♦ You have physical access to the server or server console (in case of VMWare setups) as a root user and are familiar with firewall configurations. The required ports also must be opened in the firewall. For more information about the ports, see [Section 1.1.4, “Port Details,”](#) on page 12.
- ♦ Determine if you want to reuse an existing IP address or use a new IP address for the migration process.
- ♦ If the services are managed by an L4 switch, remove the device that you are migrating from the L4 switch. Add the device back to the L4 switch once the migration is done successfully. This is required so that no user requests are sent by L4 switch to that device during migration.
- ♦ If you have customized any files use the `migrate_backup.sh` script to back up the files. This script is located in the `novell-access-manager` folder in the `AM_40_AccessManagerService_Linux64.tar.gz` file. Copy this script to the 3.1 SP4 or 3.1 SP5 server and run the script to do the back up. It is important to take the backup regardless of whether you are reusing the same machine or a new machine.

As part of the backup process, the files that get backed up are:

- ♦ `/var/opt/novell/tomcat5/webapps/nidp/jsp`
- ♦ `/var/opt/novell/tomcat5/webapps/nidp/html`



- ♦ /var/opt/novell/tomcat5/webapps/nidp/images
  - ♦ /var/opt/novell/tomcat5/webapps/nidp/config
  - ♦ /var/opt/novell/tomcat5/webapps/nidp/WEB-INF/lib
  - ♦ /var/opt/novell/tomcat5/webapps/nidp/WEB-INF/web.xml
  - ♦ /var/opt/novell/tomcat5/webapps/nidp/WEB-INF/classes
  - ♦ /var/opt/novell/tomcat5/webapps/nidp/WEB-INF/conf
  - ♦ /opt/novell/java/jre/lib/security/nidpkey.keytab
  - ♦ /opt/novell/java/jre/lib/security/bcslogin.conf
  - ♦ /var/opt/novell/tomcat5/webapps/nidp/classUtils
  - ♦ /var/opt/novell/tomcat5/conf/server.xml
  - ♦ /var/opt/novell/tomcat5/conf/tomcat5.conf
- ♦ (Conditional) If the Identity Server cluster has been assigned to delegated administrators, remove them before migration and re-add them after the migration is complete.
- If you do not perform this action, the delegated administrators will not be able to log in and configure devices assigned to them. You must manually re-create these administrators and assign the respective devices.

For more information about delegated users, “[Managing Delegated Administrators](#)” in the *NetIQ Access Manager 4.0 SP1 Administration Console Guide*.

## Reusing an Existing IP Address

- ♦ “[The Identity Server Is the Only Component on the Server](#)” on page 25
- ♦ “[The Identity Server and SSL VPN Are on the Same Server](#)” on page 25

## The Identity Server Is the Only Component on the Server

Workflow:

1. Back up the files if they have been customized.
2. Stop and remove the 3.1 SP4 or 3.1 SP5 Identity Server.
3. Delete the 3.1 SP4 or 3.1 SP5 Identity Server which is removed from the Identity Servers cluster.
4. Uninstall the 3.1 SP4 or 3.1 SP5 Identity Server if you are going to use the current server to install 4.0 Identity Server.
5. Add the 4.0 Identity Server to the existing Identity Server cluster in the Administration Console.
6. Update the Identity Server and apply changes.
7. Restore any customized files from the backup taken earlier.

## The Identity Server and SSL VPN Are on the Same Server

Workflow:

- 1 Back up the customized files.
- 2 Stop the source Identity Server. (Source can be a 3.1 SP4 or 3.1 SP5 server)
- 3 Remove the source Identity server from the cluster.
- 4 Delete the source Identity Server from the Identity Servers cluster.

- 5 Uninstall the source Identity Server if you are going to use the current server to install 4.0 Identity Server.
- 6 Uninstall the source SSL VPN Server if you are going to use the current server to install 4.0 SSL VPN Server.

---

**WARNING:** Ensure that you uninstall the SSL VPN server and do not delete the SSL VPN server object. Deleting the SSL VPN server instead of uninstalling the server will result in loss of settings.

---

- 7 Use the NetIQ Access Manager 4.0 installer to install the 4.0 Identity Server on a 64-bit SLES 11 SP2 or 64-bit SLES 11 SP3 operating system.
- 8 Add the 4.0 Identity Server to the existing Identity Servers cluster in the Administration Console.
- 9 Update the Identity Server and apply changes.
- 10 Restore any customized files from the backup taken earlier.
- 11 Install SSL VPN on the same server.
- 12 **(Optional) For the ESP-enabled SSL VPN:** When the Identity Server and ESP-enabled SSL VPN are migrated to the same server:
  - 12a Click *Device > SSL VPN > Edit > Authentication Configuration*.
  - 12b In the *Embedded Service Provider Base URL* field, change the ports to 3080 and 3443 for http and https respectively.
- 13 **(Optional) For the traditional SSL VPN:** When the Identity Server and traditional SSL VPN are migrated to the same server:
  - 13a Click *Access Gateway > Edit > Service*.
  - 13b Click the SSL VPN Web server address and change the connection ports to 3080 and 3443 for http and https respectively.

---

**NOTE:** For NetIQ Access Manager 3.2 and later, release onwards, SSL VPN will be accessible on ports 3080 (http) and 3443 (https) when installed on the same server as the Identity Server.

---

## Using a New IP Address

- ♦ [“The Identity Server Is the Only Component on the Server” on page 26](#)
- ♦ [“The Identity Server and SSL VPN Are on the Same Server” on page 27](#)

## The Identity Server Is the Only Component on the Server

Workflow:

- 1 Back up the customized files.
- 2 Use the NetIQ Access Manager 4.0 installer to install the 4.0 Identity Server on a 64-bit SLES 11 SP2 or higher operating system.
- 3 Add the 4.0 Identity Server to the existing Identity Server cluster in the Administration Console.
- 4 Update the Identity Server and apply changes.
- 5 Restore any customized files from the backup taken earlier.

## The Identity Server and SSL VPN Are on the Same Server

Workflow:

- 1 Back up the customized files.
- 2 Run the NetIQ Access Manager 4.02 installer on a 64-bit SLES 11 SP2 or SP3 operating system and install the Identity Server.
- 3 Add the 4.0 Identity Server to the existing Identity Servers cluster in the Administration Console.
- 4 Update the Identity Server and apply the changes.
- 5 Install SSL VPN on the same server.
- 6 Add the 4.0 SSL VPN to the existing SSL VPN cluster in the Administration Console.
- 7 Update and apply changes.
- 8 Restore any customized files from the backup taken earlier.
- 9 **(Optional) For the ESP-enabled SSL VPN:** When the Identity Server and ESP-enabled SSL VPN are migrated to the same server:
  - 9a Click *Device > SSL VPN > Edit > Authentication Configuration*.
  - 9b In the *Embedded Service Provider Base URL* field, change the ports to 3080 and 3443 for http and https respectively.
- 10 **(Optional) For the traditional SSL VPN:** When the Identity Server and traditional SSL VPN are migrated to the same server:
  - 10a Click *Access Gateway > Edit > Service*.
  - 10b Click the SSL VPN Web server address and change the connection ports to 3080 and 3443 for http and https respectively.

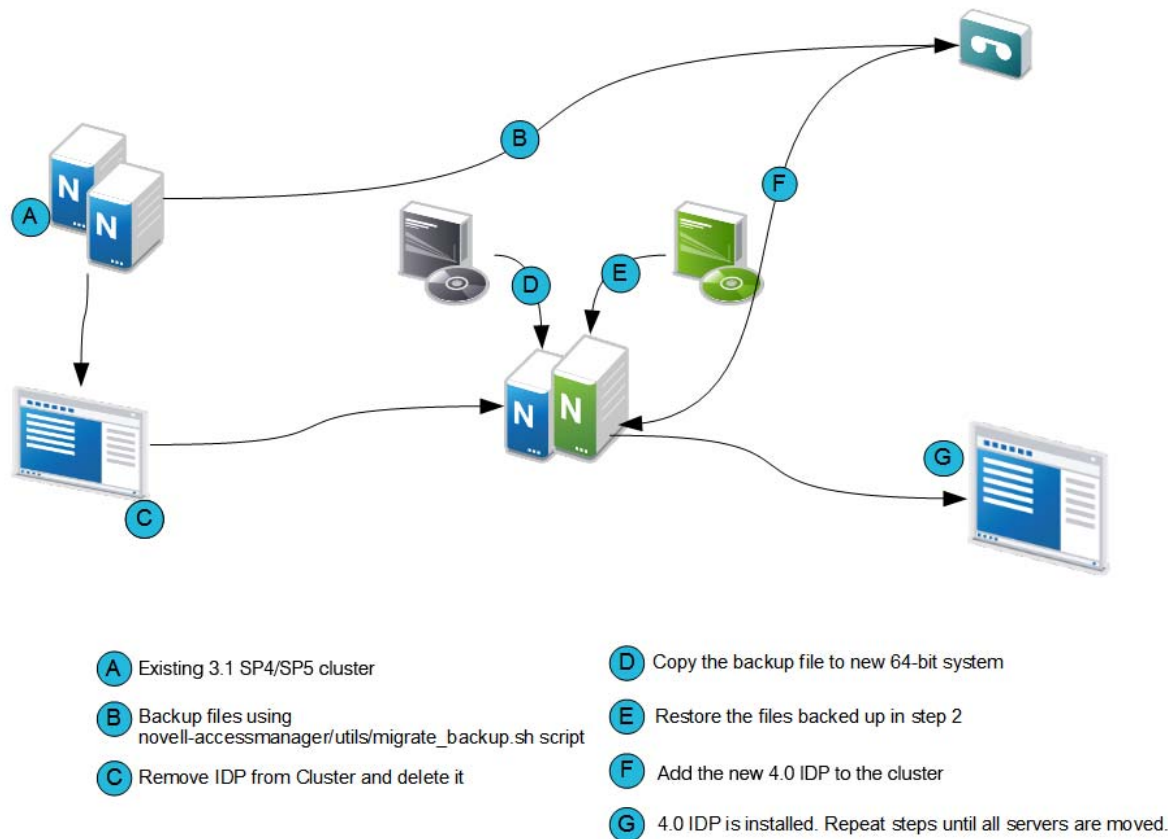
---

**NOTE:** For NetIQ Access Manager 3.2 and later, SSL VPN is accessible on ports 3080 (http) and 3443 (https) when it is installed on the same server as the Identity Server.

---

## Process of Migration

Figure 2-2 Process of Migrating the Identity Server



**IMPORTANT:** Before you proceed with the steps for migration, ensure that you have followed the instructions in the [Prerequisites for the Identity Server Migration](#).

- 1 Stop the Identity Server and remove the Identity Server from the cluster configuration.
  - 1a In the Administration Console, click **Devices > Identity Servers**.
  - 1b Select the server, then click **Stop**.
  - 1c Select the server, then choose **Actions > Remove from cluster**.
  - 1d Update the cluster configuration.
- 2 If you are using an existing machine, delete the existing Identity Server from the Administration Console before installing the new Identity Server.
  - 2a In the Administration Console, click **Devices > Identity Servers**.
  - 2b Select the server, then click **Stop**.
  - 2c Click **Actions > Delete**.
- 3 If the operating system is 32-bit (i586), perform a new installation of 64-bit SLES 11 SP2 or higher. For more information, see *SLES 11 Installation Quick Start* ([http://www.suse.com/documentation/sles11/book\\_quickstarts/data/book\\_quickstarts.html](http://www.suse.com/documentation/sles11/book_quickstarts/data/book_quickstarts.html)).  
 If the operating system is already 64-bit SLES 11 SP2 or higher, uninstall the 3.1 SP4 or 3.1 SP5 version and install the 4.0 Identity Server.

4 Ensure the following packages are installed:

- ♦ **perl-gettext, gettext-runtime:** The required library and tools to create and maintain message catalogs.
- ♦ **python:** The Python library.
- ♦ **compat:** Libraries to address compatibility issues. On SLES 11 SP2 or SP3 platform, the `compat-32bit` package is available in the SLES11-Extras repository. For information about enabling this repository, see [TID 7004701](http://www.novell.com/support/kb/doc.php?id=7004701) (<http://www.novell.com/support/kb/doc.php?id=7004701>).

4a Use YaST to install the packages that have not yet been installed.

4b Use the following command to verify the installation:

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

Replace *<package name>* with the name of the package you want to verify. For example:

```
rpm -qa | grep compat
```

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

4d Do one of the following:

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

```
cd /media
```

Browse to your CD-ROM drive.

- ♦ If you downloaded the `AM_40_AccessManagerService_Linux64.tar.gz` file, unpack the file using the following command:

```
tar -xzf AM_40_AccessManagerService_Linux64.tar.gz
```

4e Browse to the `novell-access-manager` folder.

All the files are extracted to the `novell-access-manager` folder.

4f Run the `install.sh` script from the `novell-access-manager` folder on a 64-bit SLES 11 SP2 or SP3 platform and choose the option to install the Identity Server.

5 Enter the following details:

- ♦ IP address of the 4.0 primary Administration Console as the primary Administration Console IP address
- ♦ Access Manager Administration User ID
- ♦ Access Manager Administration password
- ♦ Re-enter the password for verification

6 If local NAT is available for the Identity Server, enter the NAT IP address. For more information about configuring Network Address Translation, see “[Configuring Network Address Translation](#)” in the [NetIQ Access Manager 4.0 SP2 Installation Guide](#)

7 Enter `y` to proceed with installation.

After installation, this Identity Server device is displayed in the Administration Console.

8 Restore any customized files from the backup taken earlier as part of steps in “[Prerequisites for the Identity Server Migration](#)” on page 24.

---

**NOTE:** Ensure that you sanitize the restored customized JSP file to prevent XSS attacks. For more information about how to sanitize the JSP file, see “[Preventing Cross-site Scripting Attacks](#)” in the [NetIQ Access Manager 4.0 SP1 Identity Server Guide](#).

---

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

**Table 2-1** Restoring Files During IDP Migration

Old File Location	New File Location
/var/opt/novell/tomcat5/webapps/nidp/jsp	/opt/novell/nam/idp/webapps/nidp/jsp
/var/opt/novell/tomcat5/webapps/nidp/html	/opt/novell/nam/idp/webapps/nidp/html
/var/opt/novell/tomcat5/webapps/nidp/images	/opt/novell/nam/idp/webapps/nidp/images
/var/opt/novell/tomcat5/webapps/nidp/config	/opt/novell/nam/idp/webapps/nidp/config
/var/opt/novell/tomcat5/webapps/nidp/WEB-INF/lib	/opt/novell/nam/idp/webapps/nidp/WEB-INF/lib
/var/opt/novell/tomcat5/webapps/nidp/WEB-INF/web.xml	/opt/novell/nam/idp/webapps/nidp/WEB-INF/web.xml
/var/opt/novell/tomcat5/webapps/nidp/WEB-INF/classes	/opt/novell/nam/idp/webapps/nidp/WEB-INF/classes
/var/opt/novell/tomcat5/webapps/nidp/WEB-INF/conf	/opt/novell/nam/idp/webapps/nidp/WEB-INF/conf
/opt/novell/java/jre/lib/security/bcslogin.conf	/opt/novell/java/jre/lib/security/bcslogin.conf
/opt/novell/java/jre/lib/security/nidpkey.keytab	/opt/novell/java/jre/lib/security/nidpkey.keytab
/var/opt/novell/tomcat5/webapps/nidp/classUtils	/opt/novell/nam/idp/webapps/nidp/classUtils

**server.xml:** If you have modified any elements or attributes in the 3.1 SP4 or 3.1 SP5 environment, the corresponding changes will need to be applied to the 4.0 `/opt/novell/nam/idp/conf/server.xml` file.

Typical changes done to the `server.xml` in 3.1 SP4 or 3.1 SP5 include modifying the 'Address=' attribute to restrict the IP address the application will listen on, or 'maxThreads=' attribute to change the number of threads.

In the following example, 3.1 SP4 or 3.1 SP5 is customized to use the following ciphers.

```
<Connector NIDP_Name="connector" port="8443" address=""
ciphers="SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA,, ... .."/>
```

When migrating to 4.0, copy the cipher list from your 3.1 SP4 or 3.1 SP5 `server.xml` and replace it in the SSL connector section of the 4.0 `server.xml` file.

**tomcat5.conf:** Copy any elements or attributes that you have customized in the 3.1 SP4 or 3.1 SP5 `tomcat5.conf` file to the 4.0 `tomcat7.conf` file.

For example, if you have included the environment variable in the 3.1 SP4 or 3.1 SP5 `tomcat5.conf` file to increase the heap size by using `-Xmx/Xms/Xss` settings, the variables should be copied to the 4.0 `/opt/novell/nam/idp/conf/tomcat7.conf` file.

- 9 Add the newly installed Identity Server to the existing Identity Servers cluster.

For more information, see [“Clustering Identity Servers”](#) in the *NetIQ Access Manager 4.0 Setup Guide*.

The cluster object stores all the existing Identity Server configurations. The newly added Identity Servers inherit these configurations.

- 9a Delete the 3.1 SP4 or 3.1 SP5 Identity Server from the Administration Console. Shutdown the corresponding machine.
- 10 On the newly added Identity Server, restart Tomcat using the `/etc/init.d/novell-idp restart` or `renovell-idp restart` command.
- 11 Repeat [Step 1](#) through [Step 10](#) until all the 3.1 SP4 or 3.1 SP5 Identity Servers are replaced with 4.0 Identity Servers.

## 2.1.3 Migrating 3.1 SP4 or 3.1 SP5 Access Gateway Appliance to 4.0 Access Gateway Appliance

- ♦ [“Prerequisites for the Access Gateway Appliance Migration” on page 31](#)
- ♦ [“Reusing an Existing IP Address” on page 32](#)
- ♦ [“Using a New IP Address” on page 33](#)
- ♦ [“Migration Process” on page 34](#)

### Prerequisites for the Access Gateway Appliance Migration

In addition to the following prerequisites, ensure that you also meet the hardware and software requirements for Access Gateway. For details, see [“Access Gateway Appliance Requirements”](#) in the *NetIQ Access Manager 4.0 SP2 Installation Guide*.

- ☐ Timeout Per Protected Resource (TOPPR) is enabled and applied in the Access Gateway. In the Administration Console, click **Devices > Access Gateways > Edit**, then click **Enable Timeout Per Protected Resource**.  
  
If the **Enable Timeout Per Protected Resource** option has already been applied, it will not be displayed on the screen.
- ☐ Access Gateway should be in a cluster before migration. If the Access Gateway is on a single device, create an access gateway cluster with a single device before migration.  
  
For more information, see [“Managing a Cluster of Access Gateways”](#) in the *NetIQ Access Manager 4.0 SP1 Access Gateway Guide*.
- ☐ You have physical access to the server or server console (in case of VMWare setups) as a root user and are familiar with firewall configurations. The required ports must be opened in the firewall. For more information about the ports, see [Section 1.1.4, “Port Details,” on page 12](#).
- ☐ Ensure that you have migrated all the Administration Consoles and Identity Servers before migrating the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance to the 4.0 Access Gateway Appliance.
- ☐ Make a note of the IP addresses and host name of the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance before installing the Access Gateway Appliance. The IP address used by 3.1 SP4 or 3.1 SP5 Access Gateway Appliance to communicate with the Administration Console will be used for installing the Access Gateway Appliance.
- ☐ Determine if you want to reuse an existing IP address or use a new IP address for the migration process.
- ☐ Ensure that you have the same number of network interfaces on the new 4.0 Access Gateway as in the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance.

- ❑ If the services are managed by an L4 switch, remove the device that you are migrating from the L4 switch. Add the device back to the L4 switch once the migration is done successfully. This is required so that no user requests are sent by the L4 switch to that device during migration.
- ❑ If you have older versions prior to the 3.1 SP4 Access Gateway Appliance, first upgrade to 3.1 SP4 or 3.1 SP5 by using the instructions at [Access Manager 3.1 Installation Guide](#).
- ❑ If you have customized any files back them up using the `migrate_backup.sh` script. This script is located in the `novell-access-manager` folder in the `AM_40_AccessManagerService_Linux64.tar.gz` file. Copy this script to the 3.1 SP4 or 3.1 SP5 server and run the script to back up.

It is important to take the backup regardless of whether you are reusing the same machine or a new server.

The files that get backed up are:

- ♦ `/var/opt/novell/tomcat5/conf/server.xml`
- ♦ `/var/opt/novell/tomcat5/conf/tomcat5.conf`
- ♦ `/var/opt/novell/tomcat5/conf/web.xml`
- ♦ `/var/opt/novell/tomcat5/webapps/nesp/WEB-INF/web.xml`
- ♦ `/var/opt/novell/tomcat5/webapps/nesp/jsp`
- ♦ `/var/opt/novell/tomcat5/webapps/nesp/html`
- ♦ `/var/opt/novell/tomcat5/webapps/nesp/images`
- ♦ `/var/opt/novell/tomcat5/webapps/nesp/config`
- ♦ `/chroot/lag/opt/novell/bin/preapply.sh`
- ♦ `/chroot/lag/opt/novell/bin/postapply.sh`
- ♦ `/var/novell/errorpagesconfig/current/ErrorMessage.xml`
- ♦ `/var/novell/ErrorPagesConfig.xml`

- ❑ If you have touch files configured in the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance, copy the touch file migration utility files `lag2mag_touchfiles.csv` and `migrate_touchfiles.sh` to the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance. These files are located in the `novell-access-manager/utils` folder in the `AM_40_AccessManagerService_Linux64.tar.gz` file.

Use the `sh migrate_touchfiles.sh > touchfile_list` command and back up the output file `touchfile_list`.

The `touchfile_list` file contains the options that needs to be mapped to the advanced options in the Access Gateway Appliance.

Here is an example of sample output:

```
# Global Option example
NAGGlobalOptions InPlaceSilent=on

# Virtual Host/Server Option example
NAGGlobalOptions DebugHeaders=on
```

## Reusing an Existing IP Address

- ♦ [“The 3.1 SP4 or 3.1 SP5 Access Gateway Appliance Is the Only Component on the Server” on page 33](#)
- ♦ [“The SSL VPN and 3.1 SP4 or 3.1 SP5 Access Gateway Appliance Are on the Same Server” on page 33](#)



## The 3.1 SP4 or 3.1 SP5 Access Gateway Appliance Is the Only Component on the Server

Workflow:

- 1 Back up any files that you have customized and note down the IP address and host name of the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance.
- 2 Shut down the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance.
- 3 Install the Access Gateway Appliance with the IP address and host name noted in [Step 1](#).
- 4 Restore any customized files from the backup taken earlier.

## The SSL VPN and 3.1 SP4 or 3.1 SP5 Access Gateway Appliance Are on the Same Server

Workflow:

- 1 Back up any files that you have customized and note down the IP address and host name of 3.1 SP4 or 3.1 SP5 Access Gateway Appliance.
- 2 Shut down the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance.
- 3 Install the Access Gateway Appliance with the IP address and host name noted in [Step 1](#)
- 4 Select Install and *Enable SSL VPN service* checkbox in the Appliance configuration page.
- 5 Restore any customized files from the backup taken earlier.

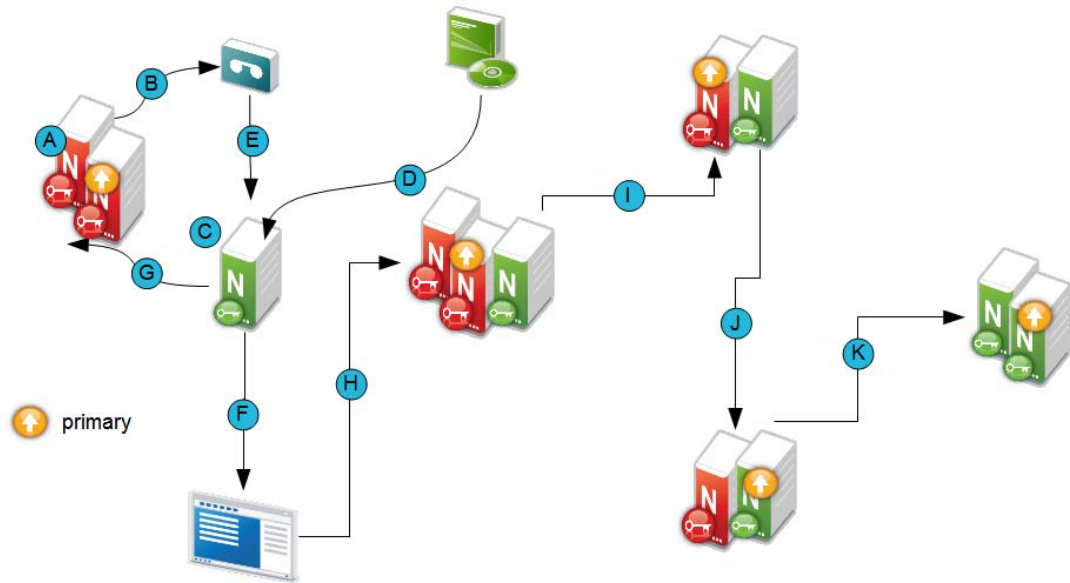
## Using a New IP Address

### The SSL VPN and 3.1 SP4 or 3.1 SP5 Access Gateway Appliance Are on the Same Server

Workflow:

- 1 Back up any files that you have customized.
- 2 Mount the Access Gateway Appliance ISO. Start the installation.
- 3 Select install and *Enable SSL VPN service* checkbox in the Appliance configuration page.
- 4 Click *Access Gateway > Edit > Service*.
- 5 Click the SSL VPN Web server address and change the connection ports to 3080 and 3443 for http and https respectively.
- 6 Restore the customized files.
- 7 Add the SSL VPN server to the existing SSL VPN cluster to get the configuration.

## Migration Process



**A** Existing 3.1 SP4/SP5 Access Gateway Appliances

**B** (Optional) Take backup of customized files

**C** 64-bit Server

**D** Install 4.0 Access Gateway Appliance

**E** (Optional) Restore the files from the backup taken

**F** Add the newly installed 4.0 Gateway Appliance to the existing 3.1 SP4/SP5 cluster

**G** Copy the customized error message files

**H** Mixed cluster setup

**I** Remove one Linux Access Gateway from the cluster

**J** Specify the Access Gateway as the Primary server

**K** Convert all Linux Access Gateways to Access Gateways

Migrating the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance to 4.0 Access Gateway Appliance will not cause any disruption to the existing setup. You can add new Access Gateway Appliance nodes into the existing 3.1 SP4 or 3.1 SP5 Access Gateway Appliance cluster. They can co-exist together.

If you are using a different server with a different IP address, see [“Use case scenario 1:” on page 34](#) and if you are reusing the same IP address, see [“Use case scenario 2:” on page 37](#).

### Use case scenario 1:

This scenario assumes that you have a new 64-bit server to install the 4.0 Access Gateway Appliance and explains how to migrate from 3.1 SP4 or 3.1 SP5 by using a different IP address.

Consider that the setup includes the following components:

- Administration Console (AC 1)
- Identity Server cluster (IDP 1 and IDP2)
- 3.1 SP4 or 3.1 SP5 Access Gateway Appliance cluster (LAG 1 and LAG 2).

## Migration Process

- 1 Determine which server in the 3.1 SP4 or 3.1 SP5 Access Gateway cluster is the primary server.

**1a** Login to Administration Console

**1b** Click **Devices > Access Gateways** > Select the device.

The list of servers are displayed. The primary server is indicated by a red mark beside the IP address.

### Access Gateways

Access Gateway Servers								
<a href="#">New Cluster...</a>   <a href="#">Restart</a>   <a href="#">Stop</a>   <a href="#">Refresh</a>   <a href="#">Actions</a> ▼								
<input type="checkbox"/> Name	Status	Health	Alerts	Commands	Statistics	Type	Configuration	
<a href="#">NAMAutomationLAG</a>	Current		0		<a href="#">View</a>		<a href="#">Edit</a>	
<input type="checkbox"/> <a href="#">172.16.0.0</a> ±	Current		0	<a href="#">Succeeded</a>	<a href="#">View</a>	Gateway Appliance		
<input type="checkbox"/> <a href="#">172.16.0.1</a>	Current		0	<a href="#">Succeeded</a>	<a href="#">View</a>	Gateway Appliance		
<input type="checkbox"/> <a href="#">172.16.0.2</a>	Current		0	<a href="#">Succeeded</a>	<a href="#">View</a>	Gateway Appliance		
<input type="checkbox"/> <a href="#">172.16.0.6</a>	Current		0	<a href="#">Succeeded</a>	<a href="#">View</a>	Gateway Appliance		

- 2 Install the Access Gateway Appliance (AG 1). For more information, see “[Installing the Access Gateway Appliance](#)” in the *NetIQ Access Manager 4.0 SP2 Installation Guide*. While installing the Access Gateway Appliance, specify the Administration Console's (AC 1) IP address, user name and password in the Administration Console Configuration field on the Appliance Configuration page.
- 3 Add the newly installed Access Gateway Appliance to the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance cluster. For more information, see “[Managing Access Gateways](#)”.
- 4 By default, all proxy services of newly added devices to the cluster are listening on the same IP address and port. To configure each reverse proxy service to a specific IP address and port, follow the steps below.
  - 4a** Configure a primary IP Address in YaST for the remaining interfaces.
    - 4a1** Go to YaST > Network Devices > Network Settings > Overview.
    - 4a2** Select the network card and click **Edit**.
    - 4a3** Specify the IP address.

Repeat the steps for all the interfaces.
  - 4b** Click **Devices > Access Gateways** > Select the device > **New IP** > click **OK**.
  - 4c** Add the secondary IP address if applicable to the interfaces from **Network Settings > Adapter List**.
  - 4d** Configure the DNS from **Network Settings > DNS**.
  - 4e** Add the Host entries (if any) from **Network Settings > Hosts**.
  - 4f** Set up the routing (if any) from **Network Settings > Gateways**.
  - 4g** Under Services, click on **Reverse Proxy/Authentication**. In the **Reverse Proxy List**, click the proxy service name. Select the newly added cluster member and select the **listening IP address** for that service.

(Optional) If you want to specify the outbound connection to the Web server, click **Web Servers**, then click **TCP Connect Options**. Select the **Cluster Member** and select the IP address from the drop down list against **Make Outbound Connection Using** if you want to select the outbound IP address to communicate with the Web server.

For more information about configuring the network settings, see “Configuring Network Settings” in the *NetIQ Access Manager 4.0 SP1 Access Gateway Guide*.

- 4h Restore any customized files backed up earlier as part of “Prerequisites for the Access Gateway Appliance Migration” on page 31.

Copy the content of the following files to the corresponding file in the new location.

**Table 2-2** Restoring Files during 4.0 Access Gateway Appliance Migration - Scenario 1

Old File Location	New File Location
/var/opt/novell/tomcat5/conf/web.xml	/opt/novell/nam/mag/conf/web.xml
/var/opt/novell/tomcat5/webapps/nesp/ WEB-INF/web.xml	/opt/novell/nam/mag/webapps/nesp/WEB- INF/web.xml
/var/opt/novell/tomcat5/webapps/nesp/jsp	/opt/novell/nam/mag/webapps/nesp/jsp
/var/opt/novell/tomcat5/webapps/nesp/ html	/opt/novell/nam/mag/webapps/nesp/html
/var/opt/novell/tomcat5/webapps/nesp/ images	/opt/novell/nam/mag/webapps/nesp/images
/var/novell/errorpagesconfig/current/ (Contains error messages and error pages configuration)	/opt/novell/nam/mag/webapps/agm/WEB-INF/ config/current
/var/opt/novell/tomcat5/webapps/nesp/ config	/opt/novell/nam/mag/webapps/nesp/config
/chroot/lag/opt/novell/bin/preapply.sh	/opt/novell/devman/jcc/scripts/ presysconfig.sh
/chroot/lag/opt/novell/bin/postapply.sh	/opt/novell/devman/jcc/scripts/ postsysconfig.sh

**NOTE:** The names of `preapply.sh` and `postapply.sh` files are different in the 4.0 environment. To restore these files, open the file and copy paste the entire content to the files in the 4.0 environment. Refer [Table 2-2 on page 36](#) for details of file locations.

**server.xml:** If you have modified any elements or attributes in the 3.1 SP4 or 3.1 SP5 environment the corresponding changes will need to be applied to the 4.0 `/opt/novell/nam/mag/conf/server.xml` file.

Typical changes done to the `server.xml` in 3.1 SP4 or 3.1 SP5 include modifying the 'Address=' attribute to restrict the IP address the application will listen on, or 'maxThreads=' attribute to modify the number of threads.

In the following example, 3.1 SP4 or 3.1 SP5 has customized `maxThreads` value.

```
<Connector port="9009" enableLookups="false" redirectPort="8443"
protocol="AJP/1.3" address="127.0.0.1" minSpareThreads="25"
maxThreads="300" backlog="0" connectionTimeout="20000", ... ..>
```

Make a note of the customizations and copy paste the changed values in the 4.0 `server.xml` file.

- 4i If you have customized the error pages for branding purposes, you will need to redo the changes in the 4.0 setup. For details on modifying messages and customizing pages, see [“Customizing the Error Pages”](#). The customized error messages can be restored by copying over the files as indicated in [Table 2-2 on page 36](#).

- 4j In the Administration Console, copy and paste the content of the previously referenced `touchfile_list` output file, under the following:

- ♦ Global Option files to **Access Gateways > Edit > Advanced Options**.

Example of Global Options in the `touchfile_list` file.

```
# Global Option example
NAGGlobalOptions InPlaceSilent=on
```

- ♦ Virtual Host/Server Option files to **Servers > Configuration > Reverse Proxy > Proxy Service > Advanced Options**.

Example of Virtual Host/Server Options in the `touchfile_list` file.

```
# Virtual Host/Server Option
NAGGlobalOptions DebugHeaders=on
```

- ♦ Files under the Administration Console are already available in the Access Gateway Appliance.

---

**NOTE:** Ensure that you do not have blank lines between each advanced option and also do not alter the content of `touchfile_list`.

For information about the migration utility files, `lag2mag_touchfiles.csv` and `migrate_touchfiles.sh` see, [“Utility Scripts” on page 113](#)

---

- 5 Test the Access Gateway Appliance functionality by accessing Access Gateway protected resources and making sure that the pages are rendered successfully.
- 6 Specify AG 1 as the primary server and click **Update**. For more information, see [“Changing the Primary Cluster Server”](#).
- 7 Remove 3.1 SP4 or 3.1 SP5 Access Gateway Appliance (LAG 1) from the cluster. For more information, see [“Viewing and Modifying Gateway Settings”](#).
- 8 Install 4.0 Access Gateway Appliance (AG 2) as in [Step 2](#) and add it to the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance cluster as in [Step 3](#).
- 9 After you confirm that all the services are up and running remove LAG2 from the cluster.
- 10 Remove 3.1 SP4 or 3.1 SP5 Access Gateway Appliance (LAG 2) from the cluster as in [Step 7](#).
- 11 Click **OK** and **Update all**.
- 12 Repeat [Step 2](#) to [Step 8](#) (except step 4j) until you have completely migrated all the existing 3.1 SP4 or 3.1 SP5 Access Gateway Appliance to 4.04.0 Access Gateway Appliance.  
After installing the Access Gateway Appliance, delete all the 3.1 SP4 or 3.1 SP5 Access Gateway Appliances from the Administration Console.
- 13 On the newly added Access Gateway server, restart Tomcat by using the `/etc/init.d/novell-mag restart` or `rcnovell-mag restart` command.

## Use case scenario 2:

This scenario assumes that you have a new/existing 64-bit server to install the 4.0 Access Gateway Appliance and explains how to migrate from 3.1 SP4 or 3.1 SP5 by using the existing IP address.

Consider that the setup includes the following components:

- ♦ Administration Console (AC 1)
- ♦ Identity Server cluster (IDP 1 and IDP 2)
- ♦ 3.1 SP4 or 3.1 SP5 Access Gateway Appliance cluster (LAG 1 and LAG 2)

## Migration Process

- 1 If you have a new 64-bit server to install 4.0 Access Gateway Appliance, ensure you do the following:

- 1a Shut down LAG2

- 1b Have the same number of Network Interface Cards as on LAG 2 and then proceed to step 2.

If you are reusing the existing LAG hardware, proceed to step 2.

- 2 Install the Access Gateway Appliance (AG 2) with the same IP address as of the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance (LAG 2). After the installation is complete, it will take some time to sync up the configuration. Ensure that you do not modify any configuration during this time.

When the configuration is synced up, the Access Gateway Appliance and the health of all the cluster members turns green.

- 3 Test the Access Gateway Appliance functionality by accessing Access Gateway protected resources and making sure pages are rendered successfully.
- 4 If you have customized the error pages for branding purposes, you will need to redo the changes in the 4.0 setup. For details on modifying messages and customizing pages, see [“Customizing the Error Pages”](#). The customized error messages can be restored by copying over the files as indicated in [Table 2-3 on page 39](#).
- 5 In the Administration Console, copy and paste the content of the previously referenced `touchfile_list` output file under the following:

- ♦ Global Option files to **Access Gateways > Edit > Advanced Options**.

Example of Global Options in the `touchfile_list` file.

```
# Global Option example
NAGGlobalOptions InPlaceSilent=on
```

- ♦ Virtual Host/Server Option files to **Servers > Configuration > Reverse Proxy > Proxy Service > Advanced Options**.

Example of Virtual Host/Server Options in the `touchfile_list` file.

```
# Virtual Host/Server Option
NAGGlobalOptions DebugHeaders=on
```

- ♦ Files under the Administration Console are already available in the Access Gateway Appliance.

---

**NOTE:** Ensure that you do not have blank lines between each advanced option and also do not alter the content of the `touchfile_list` file.

For information about the migration utility files, `lag2mag_touchfiles.csv` and `migrate_touchfiles.sh` see, [“Utility Scripts” on page 113](#)

---

- 6 Click **OK** and **Update**.
- 7 Restore any customized files backed up earlier as part of [“Prerequisites for the Access Gateway Appliance Migration” on page 31](#).

Copy the content of the following files to the corresponding file in the new location.

**Table 2-3** Restoring Files during 4.0 Access Gateway Appliance Migration -Scenario 2

Old File Location	New File Location
/var/opt/novell/tomcat5/conf/web.xml	/opt/novell/nam/mag/conf/web.xml
/var/opt/novell/tomcat5/webapps/nesp/ WEB-INF/web.xml	/opt/novell/nam/mag/webapps/nesp/WEB- INF/web.xml
/var/opt/novell/tomcat5/webapps/nesp/jsp	/opt/novell/nam/mag/webapps/nesp/jsp
/var/opt/novell/tomcat5/webapps/nesp/ html	/opt/novell/nam/mag/webapps/nesp/html
/var/opt/novell/tomcat5/webapps/nesp/ images	/opt/novell/nam/mag/webapps/nesp/images
/var/novell/errorpagesconfig/current/ (Contains error messages and error pages configuration)	/opt/novell/nam/mag/webapps/agm/WEB-INF/ config/current
/var/opt/novell/tomcat5/webapps/nesp/ config	/opt/novell/nam/mag/webapps/nesp/config
/chroot/lag/opt/novell/bin/preapply.sh	/opt/novell/devman/jcc/scripts/ presysconfig.sh
/chroot/lag/opt/novell/bin/postapply.sh	/opt/novell/devman/jcc/scripts/ postsysconfig.sh

**NOTE:** The names of `preapply.sh` and `postapply.sh` files are different in the 4.0 environment. To restore these files, open the file and copy paste the entire content to the files in the 4.0 environment. Refer [Table 2-2 on page 36](#) for details of file locations.

**server.xml:** If you have modified any elements or attributes in the 3.1 SP4 or 3.1 SP5 environment the corresponding changes will need to be applied to the 4.0 `/opt/novell/nam/mag/conf/server.xml` file.

Typical changes done to the `server.xml` in 3.1 SP4 or 3.1 SP5 include modifying the 'Address=' attribute to restrict the IP address the application will listen on, or 'maxThreads=' attribute to modify the number of threads.

In the following example, 3.1 SP4 or 3.1 SP5 has customized `maxThreads` value.

```
<Connector port="9029" enableLookups="false" protocol="AJP/1.3"
address="127.0.0.1" minSpareThreads="25" maxThreads="300" backlog="0"
connectionTimeout="20000", ... ..>
```

Make a note of the customizations and copy paste the changed values in the 4.0 `server.xml` file.

- 8 Repeat [Step 1](#) through [Step 6](#) except step 5 until you have completely migrated all the existing 3.1 SP4 or 3.1 SP5 Access Gateway Appliance to 4.0 Access Gateway Appliance.
- 9 On the newly added Access Gateway server, restart Tomcat by using the `/etc/init.d/novell-mag restart` or `rcnovell-mag restart` command.



---

**NOTE:** The Advanced options from the Administration Console are available only for the Access Gateway Appliance. For the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance, you should have touch files configured.

---

## 2.1.4 Migrating SSL VPN

- ♦ [“Prerequisites for the SSL VPN Migration” on page 40](#)
- ♦ [“Reusing an Existing IP Address” on page 41](#)
- ♦ [“Using a New IP Address” on page 41](#)
- ♦ [“Migration Process” on page 43](#)
- ♦ [“Installing the Key for the High-Bandwidth SSL VPN” on page 48](#)

### Prerequisites for the SSL VPN Migration

In addition to the following prerequisites, ensure that you also meet the hardware and software requirements for SSLVPN. For details, see [“SSL VPN Installation Requirements”](#) in the *NetIQ Access Manager 4.0 SP2 Installation Guide*.

- ☐ The high-bandwidth RPM is installed on the SSL VPN for clustering.  
  
For more information about how to install high bandwidth RPM, see [“Installing the Key for High-Bandwidth SSL VPN”](#) in the *NetIQ Access Manager 4.0 SP2 Installation Guide*
- ☐ If you are reusing the same server for migrating the SSL VPN cluster, manually uninstall the high bandwidth RPM before migration. You must then reinstall it after migration.  
  
For more information about how to uninstall high-band-width RPM, see [“Uninstalling the RPM Key for High Bandwidth SSL VPN”](#) in the *NetIQ Access Manager 4.0 SP2 Installation Guide*.
- ☐ If the services are managed by an L4 switch, remove the device that you are migrating, from the L4 switch. Add the device back to the L4 switch once the migration is done successfully. This is required so that no user requests are sent by the L4 switch to the device during migration.
- ☐ You have physical access to the server or server console (in case of VMWare setups) as a root user and are familiar with firewall configurations. The required ports also must be opened in the firewall. For more information on the ports, see [Section 1.1.4, “Port Details,” on page 12](#).
- ☐ Determine if you want to reuse an existing IP address or use a new IP address for the migration process.
- ☐ If you have customized any files back it up using the `migrate_backup.sh` script. This script is located in the `novell-access-manager` folder in the `AM_AccessManagerService_Linux64.tar.gz` file. Copy this script to the 3.1 SP4 or 3.1 SP5 machine and run the script to do the backup. It is important to take the backup regardless of whether you are reusing the same server or a new server.

This script backs up the following files:

- ♦ `/var/opt/novell/tomcat5/conf/server.xml`
- ♦ `/var/opt/novell/tomcat5/conf/tomcat5.conf`
- ♦ `/var/opt/novell/tomcat5/webapps/sslvpn/WEB-INF/web.xml`
- ♦ `/var/opt/novell/tomcat5/webapps/sslvpn/WEB-INF/conf`
- ♦ `/var/opt/novell/tomcat5/webapps/sslvpn/*.jsp`
- ♦ `/var/opt/novell/tomcat5/webapps/sslvpn/pages*`



- ♦ `/var/opt/novell/tomcat5/webapps/sslvpn/jsp`
- ♦ `/var/opt/novell/tomcat5/webapps/sslvpn/html`
- ♦ `/var/opt/novell/tomcat5/webapps/sslvpn/images`
- ♦ `/var/opt/novell/tomcat5/webapps/sslvpn/common`
- ♦ `/var/opt/novell/tomcat5/webapps/sslvpn/SSLVPNClientHelp`

---

**NOTE:** This step is required in all the SSL VPN migration scenarios even if you reuse the existing 64-bit compatible server.

---

## Reusing an Existing IP Address

- ♦ [“The SSL VPN and 3.1 SP4 or 3.1 SP5 Access Gateway Appliance Are on the Same Server” on page 33](#)
- ♦ [“The SSL VPN Is the Only Component on the Server” on page 41](#)

## The SSL VPN and 3.1 SP4 or 3.1 SP5 Access Gateway Appliance Are on the Same Server

Workflow:

- 1 Back up any files that you have customized.
- 2 Mount the Access Gateway Appliance ISO. Start the installation.
- 3 Provide a host name same as the one on 3.1 SP4 or 3.1 SP5 Access Gateway Appliance.
- 4 Select install. Enable SSL VPN service checkbox in the Appliance configuration page.
- 5 Restore any customized files from the backup taken earlier.

## The SSL VPN Is the Only Component on the Server

Workflow:

- 1 Back up any customized files.
- 2 Run the `uninstall.sh` script from the existing 3.1 SP4 or 3.1 SP5 Access Manager installation folder.
- 3 Install SSL VPN.
- 4 Restore any customized files from the backup taken earlier.

## Using a New IP Address

- ♦ [“The SSL VPN and 3.1 SP4 or 3.1 SP5 Access Gateway Appliance Are on the Same Server” on page 41](#)
- ♦ [“The SSL VPN Is the Only Component on the Server” on page 42](#)

## **The SSL VPN and 3.1 SP4 or 3.1 SP5 Access Gateway Appliance Are on the Same Server**

Workflow:

- 1 Back up any customized files.
- 2 Mount the Access Gateway Appliance ISO and install the Access Gateway Appliance.
- 3 Click *Access Gateway > Edit > Service*.
- 4 From the administration console, click the SSL VPN Web server address and change the connection ports to 3080 and 3443 for http and https respectively.
- 5 Restore the customized files.
- 6 Add the SSL VPN server to the existing SSL VPN cluster.

## **The SSL VPN Is the Only Component on the Server**

Workflow:

- 1 Back up the customized files.
- 2 Install SSL VPN.
- 3 Add the 4.0 SSL VPN to the existing SSL VPN cluster in the Administration Console.
- 4 Restore any customized files from the backup taken earlier.

## **The SSL VPN and Administration Console Are on the Same Server**

Workflow:

- 1 Back up the customized files.
- 2 Migrate the Administration Console from 3.1 SP4 or 3.1 SP5 to 4.0
- 3 Migrate the Identity Server.
- 4 Migrate SSL VPN.
- 5 Restore backed up files.

## **The SSL VPN and Identity Server Are on the Same Server**

Workflow:

- 1 Back up the customized files.
- 2 Stop the 3.1 SP4 or 3.1 SP5 Identity Server.
- 3 Remove the 3.1 SP4 or 3.1 SP5 Identity server from the cluster.
- 4 Delete the 3.1 SP4 or 3.1 SP5 Identity Server from the Identity Servers cluster.
- 5 Uninstall the 3.1 SP4 or 3.1 SP5 Identity Server if you are going to use the current machine to install 4.0 Identity Server.
- 6 Uninstall the 3.1 SP4 or 3.1 SP5 SSL VPN Server if you are going to use the current machine to install 4.0 SSL VPN Server.

---

**WARNING:** Ensure that you uninstall the SSL VPN server and not delete the SSL VPN server object. Deleting the SSL VPN server instead of uninstalling the server will result in loss of settings.

---

- 7 Use the NetIQ Access Manager 4.0 installer to install the 4.0 Identity Server on a 64-bit SLES 11 SP2 or SP3 operating system.
- 8 Add the 4.0 Identity Server to the existing Identity Servers cluster in the Administration Console.
- 9 Update the Identity Server and apply changes.
- 10 Restore any customized files from the backup taken earlier.
- 11 Install the SSL VPN by running the NetIQ Access Manager 4.0 installer on the same server.
- 12 **(Optional) For the ESP-enabled SSL VPN:** When the Identity Server and ESP-enabled SSL VPN are migrated to the same server:
  - 12a Click *Device > SSL VPN > Edit > Authentication Configuration*.
  - 12b In the *Embedded Service Provider Base URL* field, change the ports to 3080 and 3443 for http and https respectively.
- 13 **(Optional) For the traditional SSL VPN:** When the Identity Server and traditional SSL VPN are migrated to the same server:
  - 13a Click *Access Gateway > Edit > Service*.
  - 13b Click the SSL VPN Web server address and change the connection ports to 3080 and 3443 for http and https respectively.

---

**NOTE:** For NetIQ Access Manager 3.2 and later, release onwards, SSL VPN will be accessible on ports 3080 (http) and 3443 (https) when installed on the same server as the Identity Server.

---

## Migration Process

- ♦ [“Reusing an Existing Server” on page 43](#)
- ♦ [“Migrating ESP-enabled SSL VPN or Traditional SSL VPN Server” on page 45](#)
- ♦ [“Traditional SSL VPN server installed with 3.1 SP4 or 3.1 SP5 Access Gateway Appliance” on page 47](#)

---

**IMPORTANT:** Before you proceed with the steps for migration, ensure that you have followed the instructions in the [“Prerequisites for the SSL VPN Migration” on page 40](#)

---

## Reusing an Existing Server

If the existing server supports the 64-bit installer, you can reuse the server to install the Access Manager SSL VPN 4.0.

- 1 Continue with the steps for the related SSL VPN migration scenarios. For more information, see [“Reusing an Existing IP Address” on page 41](#) and [“Using a New IP Address” on page 41](#).
- 2 Restore any customized files from the backup taken earlier as part of steps in [“Prerequisites for the SSL VPN Migration” on page 40](#).

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

Old Location	New Location
/var/opt/novell/tomcat5/webapps/sslvpn/ WEB-INF/web.xml	/opt/novell/nam/sslvpn/webapps/sslvpn/ WEB-INF/web.xml
/var/opt/novell/tomcat5/webapps/sslvpn/ WEB-INF/conf	/opt/novell/nam/sslvpn/webapps/sslvpn/ WEB-INF/conf
/var/opt/novell/tomcat5/webapps/sslvpn/ *.jsp	/opt/novell/nam/sslvpn/webapps/sslvpn/ *.jsp
/var/opt/novell/tomcat5/webapps/sslvpn/ pages*	/opt/novell/nam/sslvpn/webapps/sslvpn/ pages*
/var/opt/novell/tomcat5/webapps/sslvpn/ html	/opt/novell/nam/sslvpn/webapps/sslvpn/ html
/var/opt/novell/tomcat5/webapps/sslvpn/ images	/opt/novell/nam/sslvpn/webapps/sslvpn/ images
/var/opt/novell/tomcat5/webapps/sslvpn/ common	/opt/novell/nam/sslvpn/webapps/sslvpn/ common
/var/opt/novell/tomcat5/webapps/sslvpn/ SSLVPNClientHelp	/opt/novell/nam/sslvpn/webapps/sslvpn/ SSLVPNClientHelp

**server.xml:** If you have modified any elements or attributes in the 3.1 SP4 or 3.1 SP5 environment the corresponding changes will need to be applied to the 4.0 /opt/novell/nam/sslvpn/conf/server.xml file.

Typical changes done to the server.xml in 3.1 SP4 or 3.1 SP5 include modifying the 'Address=' attribute to restrict the IP address the application will listen on, or 'maxThreads=' attribute to modify the number of threads.

In the following example, the source 3.1 SP4 server has customized maxThreads value.

```
<Connector port="9029" enableLookups="false" protocol="AJP/1.3"
address="127.0.0.1" minSpareThreads="25" maxThreads="300" backlog="0"
connectionTimeout="20000", ... ..>
```

Make a note of the customizations and copy paste the changed values in the 4.0 server.xml file.

**tomcat5.conf:** Copy any elements or attributes that you have customized in the 3.1 SP4 or 3.1 SP5 tomcat5.conf file to the 4.0 tomcat7.conf file

For example, if you have included the environment variable in the 3.1 SP4 or 3.1 SP5 tomcat5.conf file to increase the heap size by using -Xmx/Xms/Xss settings, the variables should be copied to the 4.0 /opt/novell/nam/idp/conf/tomcat7.conf file.

- 3 Add the newly installed SSL VPN device to the existing SSL VPN cluster if you are not reusing the existing IP address.

For more information, see [“Clustering SSL VPN Servers”](#) in the *NetIQ Access Manager 4.0 Setup Guide*.

The cluster object stores all the existing SSL VPN configurations. The newly added SSL VPN servers inherit these configurations.

- 4 Repeat [Step 2](#) until all the 3.1 SP4 or 3.1 SP5 SSL VPN Servers are replaced with 4.0 SSL VPN servers.
- 5 On the newly added SSL VPN servers, restart Tomcat by using the /etc/init.d/novell-sslvpn restart or rcnovell-sslvpn restart command.

## Migrating ESP-enabled SSL VPN or Traditional SSL VPN Server

You can migrate the ESP-enabled SSL VPN or traditional SSL VPN server in the following cases:

- ♦ SSL VPN server is installed independently.
- ♦ SSL VPN server is installed with the Administration Console.
- ♦ SSL VPN is installed with the Identity Server.

### Migrating ESP-enabled SSL VPN or traditional SSL VPN when SSL VPN is installed independently:

---

**IMPORTANT:** Before you proceed with the steps for migration, ensure that you have followed the instructions in the [“Prerequisites for the SSL VPN Migration” on page 40](#)

---

- 1 If the operating system is 64-bit SLES 11 SP2 or SP3, uninstall version 3.1 SP4 or 3.1 SP5 and install version 4.0 SSL VPN Server. Continue with [Step 8](#)
- 2 Perform a new installation of 64-bit SLES 11 SP2 or SP3 operating system. For more information, see SLES 11 [Installation Quick Start](#).
- 3 Ensure the following packages are installed:
  - ♦ **perl-gettext, gettext-runtime** The required library and tools to create and maintain message catalogs.
  - ♦ **python:** The Python library.
  - ♦ **compat:** Libraries to address compatibility issues. On SLES 11 SP2 or SP3 platform, the `compat-32bit` package is available in the SLES11-Extras repository. For information on enabling this repository, see [TID 7004701](#).
- 3a Use YaST to install the packages that have not yet been installed.
- 3b Use the `rpm -qa | grep <package name>` command to verify the installation.  
Replace `<package name>` with the name of the package you want to verify. For example:  

```
rpm -qa | grep compat
```
- 4 Ensure you have downloaded the software or you have the CD available.
- 5 Do one of the following:
  - ♦ Insert the CD into the drive and navigate to the device. Enter the following:  

```
cd /media
```

  
Browse to your CD-ROM drive.
  - ♦ If you have downloaded the `AM_32_AccessManagerService_Linux.tar.gz` file, unpack the file using the `tar -xzf AM_32_AccessManagerService_Linux.tar.gz` command.
- 6 Browse to the `novell-access-manager` directory. All the files are extracted to the `novell-access-manager` folder.
- 7 Run the `install.sh` script from the `novell-access-manager` folder on a 64-bit SLES 11 SP2 or SP3 and choose the option to install the ESP-enabled SSL VPN or Traditional SSL VPN.
- 8 Review and accept the License Agreement.
- 9 If the SSL VPN machine has been configured with multiple IP addresses, select an IP address for the SSL VPN server at the prompt.
- 10 Specify the name of the administrator for the Administration Console.
- 11 Specify and confirm the administration password.

Wait while the SSL VPN server is installed on your system and imported into the Administration Console.

- 12 The installation ends with the following message: `Installation complete.`
- 13 If you are using an existing IP address, the device will be available in existing cluster. If it is installed with a new IP address, a new device will be found in the SSL VPN of the Administration Console.
- 14 If the existing IP address is used then wait until the health status of the device status turns green. If it is installed with a new IP address and is ESP-enabled, the health status will be in Yellow state.
- 15 If you are installing with a new IP address, add the device to the existing cluster and update the cluster.
- 16 If the export law permits and you want to install the high bandwidth version of SSL VPN, see [“Traditional SSL VPN server installed with 3.1 SP4 or 3.1 SP5 Access Gateway Appliance” on page 47.](#)
- 17 Check the SSL VPN functionality. Repeat [Step 1](#) to [Step 17](#) (except step 16) for the other devices in the cluster.
- 18 Restore any customized files from the backup taken earlier as part of steps in [“Prerequisites for the SSL VPN Migration” on page 40.](#)

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

Old Location	New Location
<code>/var/opt/novell/tomcat5/webapps/sslvpn/WEB-INF/web.xml</code>	<code>/opt/novell/nam/sslvpn/webapps/sslvpn/WEB-INF/web.xml</code>
<code>/var/opt/novell/tomcat5/webapps/sslvpn/WEB-INF/conf</code>	<code>/opt/novell/nam/sslvpn/webapps/sslvpn/WEB-INF/conf</code>
<code>/var/opt/novell/tomcat5/webapps/sslvpn/*.jsp</code>	<code>/opt/novell/nam/sslvpn/webapps/sslvpn/*.jsp</code>
<code>/var/opt/novell/tomcat5/webapps/sslvpn/pages*</code>	<code>/opt/novell/nam/sslvpn/webapps/sslvpn/pages*</code>
<code>/var/opt/novell/tomcat5/webapps/sslvpn/html</code>	<code>/opt/novell/nam/sslvpn/webapps/sslvpn/html</code>
<code>/var/opt/novell/tomcat5/webapps/sslvpn/images</code>	<code>/opt/novell/nam/sslvpn/webapps/sslvpn/images</code>
<code>/var/opt/novell/tomcat5/webapps/sslvpn/common</code>	<code>/opt/novell/nam/sslvpn/webapps/sslvpn/common</code>
<code>/var/opt/novell/tomcat5/webapps/sslvpn/SSLVPNClientHelp</code>	<code>/opt/novell/nam/sslvpn/webapps/sslvpn/SSLVPNClientHelp</code>

**server.xml:** If you have modified any elements or attributes in the 3.1 SP4 or 3.1 SP5 environment the corresponding changes will need to be applied to the 4.0 `/opt/novell/nam/sslvpn/conf/server.xml` file.

Typical changes done to the `server.xml` in 3.1 SP4 or 3.1 SP5 include modifying the `'Address='` to restrict the IP address the application will listen on, or `'maxThreads='` attributes to modify the number of threads.

In the following example, the 3.1 SP4 server has customized `maxThreads` value.

```
<Connector port="9029" enableLookups="false" protocol="AJP/1.3"
address="127.0.0.1" minSpareThreads="25" maxThreads="300" backlog="0"
connectionTimeout="20000", ... ../>
```

Make a note of the customizations and copy paste the changed values in the 4.0 `server.xml` file.

**tomcat5.conf:** Copy any elements or attributes that you have customized in the 3.1 SP4 or 3.1 SP5 `tomcat5.conf` file to the 4.0 `tomcat7.conf` file.

For example, if you have included the environment variable in the 3.1 SP4 `tomcat5.conf` file to increase the heap size by using `-Xmx/Xms/Xss` settings, the variables should be copied to the 4.0 `/opt/novell/nam/idp/conf/tomcat7.conf` file.

## Traditional SSL VPN server installed with 3.1 SP4 or 3.1 SP5 Access Gateway Appliance

---

**IMPORTANT:** Before you proceed with the steps for migration, ensure that you have followed the instructions in the [“Prerequisites for the SSL VPN Migration” on page 40](#)

---

- 1 Follow the steps to migrate from 3.1 SP4 or 3.1 SP5 Access Gateway Appliance to Access Gateway Appliance. For more information, see [Section 2.1.3, “Migrating 3.1 SP4 or 3.1 SP5 Access Gateway Appliance to 4.0 Access Gateway Appliance,” on page 31](#).
- 2 Start the installation and in the Appliance configuration screen, select the *Install and enable SSL VPN Service* check box.
- 3 If you have used an existing IP address, the existing SSL VPN within the cluster will be migrated to Access Manager 4.0. If it is installed with a new IP address, a new SSL VPN server will be displayed in the Administration Console.
- 4 The import/re-import process will take some time. Wait until the Access Gateway Appliance and the SSL VPN health status becomes green.
- 5 If it is not part of the SSL VPN cluster, add it to the existing cluster and update.
- 6 Repeat the steps for other devices in the cluster.
- 7 If the export law permits and you want to install the high bandwidth version of SSL VPN, see, [“Traditional SSL VPN server installed with 3.1 SP4 or 3.1 SP5 Access Gateway Appliance” on page 47](#).
- 8 Restore any customized files from the backup taken earlier as part of steps in [“Prerequisites for the SSL VPN Migration” on page 40](#).

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

Old Location	New Location
<code>/var/opt/novell/tomcat5/webapps/sslvpn/WEB-INF/web.xml</code>	<code>/opt/novell/nam/sslvpn/webapps/sslvpn/WEB-INF/web.xml</code>
<code>/var/opt/novell/tomcat5/webapps/sslvpn/WEB-INF/conf</code>	<code>/opt/novell/nam/sslvpn/webapps/sslvpn/WEB-INF/conf</code>
<code>/var/opt/novell/tomcat5/webapps/sslvpn/*.jsp</code>	<code>/opt/novell/nam/sslvpn/webapps/sslvpn/*.jsp</code>
<code>/var/opt/novell/tomcat5/webapps/sslvpn/pages*</code>	<code>/opt/novell/nam/sslvpn/webapps/sslvpn/pages*</code>

Old Location	New Location
/var/opt/novell/tomcat5/webapps/sslvpn/html	/opt/novell/nam/sslvpn/webapps/sslvpn/html
/var/opt/novell/tomcat5/webapps/sslvpn/images	/opt/novell/nam/sslvpn/webapps/sslvpn/images
/var/opt/novell/tomcat5/webapps/sslvpn/common	/opt/novell/nam/sslvpn/webapps/sslvpn/common
/var/opt/novell/tomcat5/webapps/sslvpn/SSLVPNClientHelp	/opt/novell/nam/sslvpn/webapps/sslvpn/SSLVPNClientHelp
/chroot/lag/opt/novell/bin/preapply.sh	/opt/novell/devman/jcc/scripts/presysconfig.sh
/chroot/lag/opt/novell/bin/postapply.sh	/opt/novell/devman/jcc/scripts/postsysconfig.sh

**server.xml:** If you have modified any elements or attributes in the 3.1 SP4 or 3.1 SP5 environment the corresponding changes will need to be applied to the 4.0 /opt/novell/nam/sslvpn/conf/server.xml file.

Typical changes done to the server.xml in 3.1 SP4 or 3.1 SP5 include modifying the 'Address=' to restrict the IP address the application will listen on, or 'maxThreads=' attributes to modify the number of threads.

In the following example, the 3.1 SP4 server has customized maxThreads value.

```
<Connector port="9029" enableLookups="false" protocol="AJP/1.3"
address="127.0.0.1" minSpareThreads="25" maxThreads="300" backlog="0"
connectionTimeout="20000", ... ..>
```

Make a note of the customizations and copy paste the changed values in the 4.0 server.xml file.

**tomcat5.conf:** Copy any elements or attributes that you have customized in the 3.1 SP4 or 3.1 SP5 tomcat5.conf file to the 4.0 tomcat7.conf file

For example, if you have included the environment variable in the 3.1 SP4 tomcat5.conf file to increase the heap size by using -Xmx/Xms/Xss settings, the variables should be copied to the 4.0 /opt/novell/nam/idp/conf/tomcat7.conf file.

## Installing the Key for the High-Bandwidth SSL VPN

You must install the high bandwidth SSL VPN if you want to add the SSL VPN servers to the cluster. Customers who are eligible to install the high bandwidth SSL VPN can install the key for the high bandwidth SSL VPN after they get the clearance to export. This key is installed only once.

In this release you do not have to upgrade the RPM every time the servlet and the server RPMs for SSL VPN are upgraded.

With Access Manager 3.1 or later, you can install the key once and upgrade it to new versions without installing the key again.

- 1 After you have ordered the high bandwidth version, log in to the NetIQ Customer Center and click on the link that allows you to download the RPM containing key for the high bandwidth version.
- 2 Download the novl-sslvpn-hb-key-3.1.0-0.noarch.rpm high bandwidth RPM.



- 3 Log in as root.
- 4 Enter the `/etc/init.d/novell-sslvpn stop` or `rcnovell-sslvpn stop` command to stop all services.
- 5 Enter the `rpm -ivh novl-sslvpn-hb-key-3.1.0-0.noarch.rpm` command to install the RPM for the high bandwidth version of SSL VPN.
- 6 Enter the `/etc/init.d/novell-sslvpn start` or `rcnovell-sslvpn start` command to restart all SSL VPN services.
- 7 Enter the `/etc/init.d/novell-sslvpn status` or `rcnovell-sslvpn status` command to check the status.

## 2.2 Migrating Access Manager on Red Hat From Windows

- ♦ [Section 2.2.1, “Migrating Administration Consoles,” on page 49](#)
- ♦ [Section 2.2.2, “Migrating Identity Server,” on page 56](#)
- ♦ [Section 2.2.3, “Migrating 3.1 SP4 or 3.1 SP5 Access Gateway Appliance to 4.0 Access Gateway Appliance,” on page 62](#)

### 2.2.1 Migrating Administration Consoles

- ♦ [“Prerequisites for the Administration Console Migration” on page 49](#)
- ♦ [“Migration Scenarios for the Administration Console” on page 50](#)
- ♦ [“Migrating the Primary Administration Console” on page 51](#)
- ♦ [“Migrating the Secondary Administration Console” on page 54](#)

### Prerequisites for the Administration Console Migration

In addition to the following prerequisites, ensure that you also meet the hardware and software requirements for the Administration Console. For details, see [“Installation Requirements on Linux”](#) in the *NetIQ Access Manager 4.0 SP2 Installation Guide*.

- ☐ A new IP address, that will be temporarily used during the Primary Administration Console migration.
- ☐ Timeout Per Protected Resource (TOPPR) is enabled and applied in the Access Gateway. In the Administration Console, click **Devices > Access Gateways > Edit**, then click **Enable Timeout Per Protected Resource**.  
If the **Enable Timeout Per Protected Resource** option has already been applied, it will not be displayed on the screen.
- ☐ The primary and secondary 3.1 SP4 or 3.1 SP5 Administration Console time is synchronized.
- ☐ The new 4.0 Administration Console that you want to install should be on the same subnet as the existing 3.1 SP4 or 3.1 SP5 primary console.
- ☐ The health statuses for all devices in the Administration Console are green in color.  
For more information, see [“Viewing Device Health”](#) in the *NetIQ Access Manager 4.0 SP1 Administration Console Guide*.

- ☐ You have physical access to the server or server console (in case of VMWare setups) as a root user and you are familiar with iptables.  
The required ports are opened in the firewall. For more information about ports, see [Section 1.1.4, “Port Details,” on page 12](#).
- ☐ Note down the contracts selected under the **Satisfies contract** list of SAML2.0 and Liberty identity providers. These are under **Devices > Identity Servers > Edit > [Protocol] > [IdentityProvider] > Authentication Card**.  
The application interface for this feature has changed in version 4.0. You must manually configure these contracts after migration. This configuration will be effective after the Identity Server migration is done.  
(Optional) If federation is configured, see the contracts configured for 3.1 SP4 or 3.1 SP5, and navigate to **Administration Console > Devices > Identity Servers > Edit > [Protocol] > [Identity Provider] > Authentication Card**. The **Satisfies Contract** field lists all the configured contracts.
- ☐ The host name of the new 4.0 Administration Console should be different from the existing 3.1 SP4 or 3.1 SP5 primary and secondary Administration Consoles.
- ☐ Ensure that the `\etc\hosts` file of the system where you are installing Access Manager 4.0 has the host name and IP address for the new 4.0 Administration Console server. If the hostname of the Administration Console is not listed in DNS, the `hosts` file is used to resolve the hostname of the machine to a valid IP address.
- ☐ Ensure that `nc-1.84-22.el6.x86_64.rpm` is installed on the Access Manager 4.0 setup.

---

**WARNING:** If three Administration Consoles are already installed and configured in the 3.1 SP4 or 3.1 SP5 setup, uninstall one secondary Administration Console before running the `install_and_migrate.sh` script.

For more information about deconfiguring and uninstalling the Administration Console, see [Step 12 on page 20](#) and “[Uninstalling the Linux Administration Console](#)” in the [NetIQ Access Manager 4.0 SP2 Installation Guide](#).

---

## Migration Scenarios for the Administration Console

The following scenarios are supported for migrating NetIQ Access Manager from 3.1 SP4 or 3.1 SP5 to 4.0 on Red Hat.

---

**IMPORTANT:** Ensure you identify the scenario that best describes your migration environment and review the appropriate steps before you begin the process of migration.

---

- ♦ “[Administration Console, Identity Server and 3.1 SP4 or 3.1 SP5 Access Gateway Appliance Are Installed on Different Servers](#)” on page 51
- ♦ “[Administration Console and Identity Server Are on the Same Server, and 3.1 SP4 or 3.1 SP5 Access Gateway Appliance Is on a Different Server](#)” on page 51
- ♦ “[Secondary Administration Console and Identity Server are on the Same Server](#)” on page 51
- ♦ “[The Administration Console and Identity Server Are on the Same Server](#)” on page 51

## Administration Console, Identity Server and 3.1 SP4 or 3.1 SP5 Access Gateway Appliance Are Installed on Different Servers

Workflow:

- 1 Migrate the Administration Consoles.
- 2 Migrate the Identity Server.
- 3 Migrate the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance to the 4.0 Access Gateway Appliance.

## Administration Console and Identity Server Are on the Same Server, and 3.1 SP4 or 3.1 SP5 Access Gateway Appliance Is on a Different Server

Workflow:

- 1 Migrate the primary Administration Console.
- 2 Migrate the Identity Server.
- 3 Migrate the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance to the 4.0 Access Gateway Appliance.

## Secondary Administration Console and Identity Server are on the Same Server

Workflow:

- 1 Migrate the primary Administration Console.
- 2 Migrate the secondary Administration Console.
- 3 Migrate the Identity Server.

## The Administration Console and Identity Server Are on the Same Server

Workflow:

- 1 Migrate the Administration Consoles.
- 2 Migrate the Identity Server.

---

**NOTE:** If the device has multiple interfaces, manually configure the primary IP address on each NIC.

To do this, from the terminal run the `system-config-network` command. Use the **Device Configuration** option to configure the interfaces.

---

## Migrating the Primary Administration Console

---

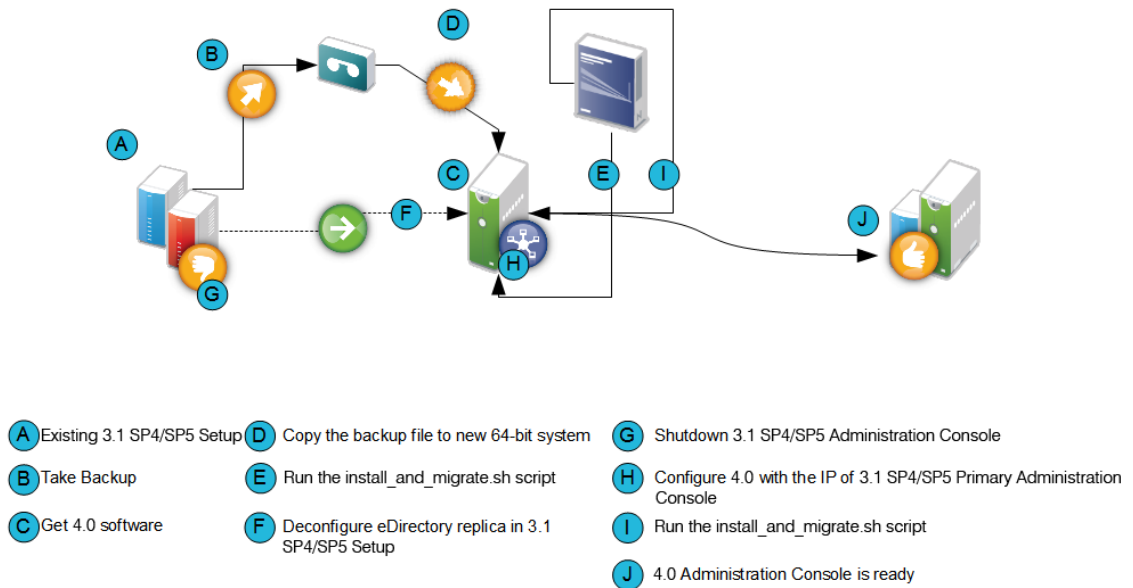
**IMPORTANT:** Before you proceed with the steps for migration, ensure that you have followed the instructions in the [Prerequisites for the Administration Console Migration](#).

If you have multiple components installed on the same system, before starting migration of any component, ensure that you read the migration prerequisites of all the components.

---

## Migration Process

Figure 2-3 Process of Migration of the Primary Administration Console



- 1 Back up the 3.1 SP4 or 3.1 SP5 primary Administration Console configuration by using `C:\Program Files(x86)\Novell\bin\ambkup.bat`.
- 2 Copy the backup zip file to `/tmp` or any other folder on the new 64-bit server where you plan to install the 4.0 Administration Console.  
 Make a note of the location and file name in absolute format. You need to provide this information in the installation and migration script (for example, `/tmp/idpq_20120111_1314.zip`).
- 3 Ensure that you have downloaded the software or you have the CD available.
- 4 Do one of the following:
  - ♦ Insert the CD into the drive, then navigate to the device. Enter the following:  
`cd /media`  
 Browse to your CD-ROM drive.
  - ♦ If you downloaded the `AM_40_AccessManagerService_Linux64.tar.gz` file, unpack the file using the following command:  
`tar -xzvf AM_40_AccessManagerService_Linux64.tar.gz`
- 5 Browse to the `novell-access-manager` folder.  
 All the files are extracted to the `novell-access-manager` folder.
- 6 Run the `install_and_migrate.sh` script from the folder to migrate the primary Administration Console from 3.1 SP4 or 3.1 SP5 to 4.0.
- 7 Accept the license agreement by entering `y` when the system prompts you.
- 8 Type `y` and press Enter when the installation confirmation message is displayed.
- 9 Provide the following details:
 

**3.1 Primary Administration Console IP address:** Enter the 3.1 SP4 or 3.1 SP5 primary IP address. Ensure that the IP address is static.

**Access Manager Administration user ID:** Enter the administrator user ID.

**Access Manager Administration password:** Enter the administrator password. Re-enter the password for verification.

**Location of the backup file with absolute path:** Enter the absolute path of the backup file that you created in [Step 1](#).

**Password for decrypting the data:** Enter the private key encryption password of the backup file. Re-enter the password for verification.

---

**NOTE:** To view installation progress, refer to the log files in `/tmp/novell_access_manager`.

---

- 10** Verify if the 4.0 Access Manager server is functional. Perform one of the following steps from the 4.0 terminal:

**10a** Run `/opt/novell/eDirectory/bin/ndsstat -r` command. This lists all the replicas available. Verify that the status of the 4.0 replica is `On`.

**10b** Run `/opt/novell/eDirectory/bin/ldapsearch -A -LLL -b "ou=accessManagerContainer,o=novell" -D "cn=<username>,o=novell" -w <password>` command. This lists all the objects in the NAM container. You can run the same command on the 3.1 SP4 or 3.1 SP5 terminal to verify if the object list is complete and accurate.

- 11** From the 3.1 SP4 or 3.1 SP5 Access Manager setup, uninstall eDirectory by using the **Add/Remove Programs** option.
- 12** Shut down the 3.1 SP4 or 3.1 SP5 Administration Console.
- 13** From the 4.0 Administration Console terminal, run the `system-config-network` command. Select the **Device Configuration** option to change the IP address to the old primary Administration Console IP address.

For more information about configuring or changing the IP address, see ([http://www.linuxtopia.org/online\\_books/rhel6/rhel\\_6\\_deployment/rhel\\_6\\_deployment\\_ch-Network\\_Interfaces.html](http://www.linuxtopia.org/online_books/rhel6/rhel_6_deployment/rhel_6_deployment_ch-Network_Interfaces.html))

- 14** Run the `install_and_migrate.sh` script from the `novell-access-manager` folder again to complete the installation.

A confirmation message is displayed.

- 14a** Enter `Y` and the following message is displayed:

```
Installation will continue to finish the rest of the 4.0 migration tasks
Would you like to continue this installation (y/n)?
```

- 14b** Enter `Y` and then provide the following details:

- ♦ Enter the Access Manager Administration user ID.
- ♦ Enter the Access Manager Administration password.
- ♦ Re-enter the password for verification.

After migration is complete, the system displays the following message:

```
4.0 Administration Console migration completed successfully.
```

- 14c** Log in to the 4.0 Administration Console and delete unused objects and certificates of the 3.1 SP4 or 3.1 SP5 Administration Console that you shutdown in [Step 12](#).

- 14c1** In Administration Console, select **View Objects**. Delete the following unused objects and certificates:

### Objects

- ♦ HTTP Server
- ♦ LDAP Server
- ♦ LDAP Group
- ♦ SNMP Group
- ♦ SAS Service
- ♦ PS object

### Certificates

- ♦ IP AG
- ♦ SSL Certificate IP
- ♦ DNS AG
- ♦ SSL Certificate DNS

## Migrating the Secondary Administration Console

To install the secondary Administration Console you can either use a new server that supports a 64-bit installer to install the secondary Administration Console or you can reuse the existing server for installation if it supports the 64-bit installer.

To migrate the secondary Administration Console to 4.0, use one of the following procedures:

- ♦ [“Using a New Server for the Secondary Administration Console” on page 22](#)
- ♦ [“Reusing the Existing Server or IP Address for the Secondary Administration Console” on page 23](#)

## Using a New Server for the Secondary Administration Console

---

**IMPORTANT:** Before you install the 4.0 secondary Administration Console on a 64-bit server, it is important to de-commission the 3.1 SP4 or 3.1 SP5 secondary Administration Console. This process helps ensure that the number of Administration Consoles do not exceed three instances.

---

- 1 Verify if the 4.0 Access Manager server is functional. Perform one of the following steps from the 4.0 terminal:
  - 1a Run `/opt/novell/eDirectory/bin/ndsstat -r` command. This lists all the replicas available. Verify that the status of the 4.0 replica is On.
  - 1b Run `/opt/novell/eDirectory/bin/ldapsearch -A -LLL -b "ou=accessManagerContainer,o=novell" -D "cn=<username>,o=novell" -w <password>` command. This lists all the objects in the NAM container. You can run the same command on the 3.1 SP4 or 3.1 SP5 terminal to verify if the object list is complete and accurate.
- 2 Log in to the 4.0 primary Administration Console.
- 3 Click **Auditing > Troubleshooting > Other Known Device Manager Servers**.
- 4 Click **Remove** for this server.

- 5 Install the 64-bit RHEL 6.4, 6.5 or 6.6 operating system on the new 64-bit server with a different host name.
  - 5a On the terminal, run `system-config-network` command.
  - 5b Select the **Device Configuration** option.
  - 5c Specify a different host name.

For more information, see ([http://www.linuxtopia.org/online\\_books/rhel6/rhel\\_6\\_deployment/rhel\\_6\\_deployment\\_ch-Network\\_Interfaces.html](http://www.linuxtopia.org/online_books/rhel6/rhel_6_deployment/rhel_6_deployment_ch-Network_Interfaces.html))
- 6 Ensure you have downloaded the software or you have the CD available.
- 7 Do one of the following:
  - ♦ Insert the CD into the drive, then navigate to the device. Enter the following:
 

```
cd /media
```

Browse to your CD-ROM drive.
  - ♦ If you downloaded the `AM_40_AccessManagerService_Linux64.tar.gz` file, unpack the file using the following command:
 

```
tar -xzf AM_40_AccessManagerService_Linux64.tar.gz
```
- 8 Browse to the `novell-access-manager` folder.
 

All the files are extracted to the `novell-access-manager` folder.

## Reusing the Existing Server or IP Address for the Secondary Administration Console

To use the existing server for installing the secondary Administration Console, ensure it is a 64-bit server.

- 1 Verify if the 4.0 Access Manager server is functional. Perform one of the following steps from the 4.0 terminal:
  - 1a Run `/opt/novell/eDirectory/bin/ndsstat -r` command. This lists all the replicas available. Verify that the status of the 4.0 replica is On.
  - 1b Run `/opt/novell/eDirectory/bin/ldapsearch -A -LLL -b "ou=accessManagerContainer,o=novell" -D "cn=<username>,o=novell" -w <password>` command. This lists all the objects in the NAM container. You can run the same command on the 3.1 SP4 or 3.1 SP5 terminal to verify if the object list is complete and accurate.
- 2 Enter the admin credentials in `admin.novell` format and proceed with deletion.
- 3 Log in to the 4.0 primary Administration Console.
- 4 Click **Auditing > Troubleshooting > Other Known Device Manager Servers**.
- 5 Click **Remove** for this server.
- 6 Format the server with the 64-bit Red Hat 6.4 or 6.5 and a different host name or configure the same IP address with a different host name.
  - 6a Run the `system-config-network` command.
  - 6b Select the **Device Configuration** option to make the changes.

For more information, see ([http://www.linuxtopia.org/online\\_books/rhel6/rhel\\_6\\_deployment/rhel\\_6\\_deployment\\_ch-Network\\_Interfaces.html](http://www.linuxtopia.org/online_books/rhel6/rhel_6_deployment/rhel_6_deployment_ch-Network_Interfaces.html))

---

**IMPORTANT:** Even after formatting the server, old certificates are not cleaned up from the user store. If you are using an existing host name during Access Manager installation, it may lead to a conflict with the existing certificates. It is recommended to use a different host name during IP address configuration.

---

7 Ensure you have downloaded the software or you have the CD available.

8 Do one of the following:

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

```
cd /media
```

Browse to your CD-ROM drive.

- ♦ If you downloaded the `AM_40_AccessManagerService_Linux64.tar.gz` file, unpack the file using the following command:

```
tar -xzf AM_40_AccessManagerService_Linux64.tar.gz
```

9 Browse to the `novell-access-manager` folder.

All the files are extracted to the `novell-access-manager` folder.

10 Install the secondary Administration Console by using the `install.sh` script.

For more information about how to install the secondary Administration Console, see “[Installing Secondary Versions of the Administration Console](#)” in the *NetIQ Access Manager 4.0 SP1 Setup Guide*.

11 From the 3.1 SP4 or 3.1 SP5 Access Manager setup, delete the objects of the unused eDirectory replica of the 3.1.4 Access Manager setup.

11a In Administration Console, select **View Objects**. Delete the following unused objects and certificates from the 3.1 SP4 or 3.1 SP5 Administration Console:

**Objects**

- ♦ HTTP Server
- ♦ LDAP Server
- ♦ LDAP Group
- ♦ SNMP Group
- ♦ SAS Service
- ♦ PS object

**Certificates**

- ♦ IP AG
- ♦ SSL Certificate IP
- ♦ DNS AG
- ♦ SSL Certificate DNS

---

**NOTE:** If the secondary Administration Console migration exits stating that the Server’s DIB does not contain replicas, see [Section 5.4, “Migration Exits Stating That the Server’s DIB Does Not Contain Replicas,”](#) on page 107.

---

## 2.2.2 Migrating Identity Server

- ♦ “[Prerequisites for the Identity Server Migration](#)” on page 57
- ♦ “[Reusing an Existing IP Address](#)” on page 58



- ♦ [“Using a New IP Address” on page 58](#)
- ♦ [“Process of Migration” on page 59](#)

It is recommended that you replace the Identity Servers individually. The 3.1 SP4 or 3.1 SP5 and 4.0 Identity Servers can coexist until the migration is complete.

## Prerequisites for the Identity Server Migration

In addition to the following prerequisites, ensure that you also meet the hardware and software requirements for the Identity Server. For details, see [“Installing the Identity Servers” in the \*NetIQ Access Manager 4.0 SP2 Installation Guide\*](#).

- ♦ The Identity Server can perform a DNS resolution with the ESP (Embedded Service Provider) host name of the Access Gateway.

For more information, see [“DNS Name Resolution” in the \*NetIQ Access Manager 4.0 SP1 Identity Server Guide\*](#).

- ♦ The Identity Server time is synchronized with the time of the Administration Console.
- ♦ You have physical access to the server or server console (in case of VMWare setups) as a root user and are familiar with firewall configurations. The required ports also must be opened in the firewall. For more information about the ports, see [Section 1.1.4, “Port Details,” on page 12](#).
- ♦ Determine if you want to reuse an existing IP address or use a new IP address for the migration process.
- ♦ If the services are managed by an L4 switch, remove the device that you are migrating from the L4 switch. Add the device back to the L4 switch once the migration is done successfully. This is required so that no user requests are sent by L4 switch to that device during migration.
- ♦ If you have customized any files use the `ambkup.bat` script to back up the files. This script is located in the `novell-access-manager` folder in the `AM_40_AccessManagerService_Linux64.tar.gz` file. Copy this script to the 3.1 SP4 or 3.1 SP5 server and run the script to do the back up. It is important to take the backup regardless of whether you are reusing the same machine or a new machine.

As part of the backup process, the files that get backed up are:

- ♦ `C:\Program Files (x86)\Novell\Tomcat\conf\server.xml`
- ♦ `C:\Program Files (x86)\Novell\Tomcat\conf\web.xml`
- ♦ `C:\Program Files (x86)\Novell\Tomcat\server\classes`
- ♦ `C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\config`
- ♦ `C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp`
- ♦ `C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\images`
- ♦ `C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\web.xml`
- ♦ `C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\images`
- ♦ `C:\Program Files (x86)\Novell\jre\lib\security\bcslogin.conf`
- ♦ `C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp`
- ♦ `C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\WEB-INF\classes`
- ♦ (Conditional) If the Identity Server cluster has been assigned to delegated administrators, remove them before migration and re-add them after the migration is complete.

If you do not perform this action, the delegated administrators will not be able to log in and configure devices assigned to them. You must manually re-create these administrators and assign the respective devices.

For more information about delegated users, “[Managing Delegated Administrators](#)” in the *NetIQ Access Manager 4.0 SP1 Administration Console Guide*.

- ♦ You have installed packages. For more information, see

## Reusing an Existing IP Address

- ♦ “[Identity Server Is the Only Component on the Server](#)” on page 58

### Identity Server Is the Only Component on the Server

Workflow:

1. Back up the files if they have been customized.
2. Stop and remove the 3.1 SP4 or 3.1 SP5 Identity Server.
3. Delete the 3.1 SP4 or 3.1 SP5 Identity Server which is removed from the Identity Servers cluster.
4. Uninstall the 3.1 SP4 or 3.1 SP5 Identity Server if you are going to use the current server to install 4.0 Identity Server.
5. Add the 4.0 Identity Server to the existing Identity Server cluster in the Administration Console.
6. Update the Identity Server and apply changes.
7. Restore any customized files from the backup taken earlier.

## Using a New IP Address

- ♦ “[Identity Server Is the Only Component on the Server](#)” on page 58

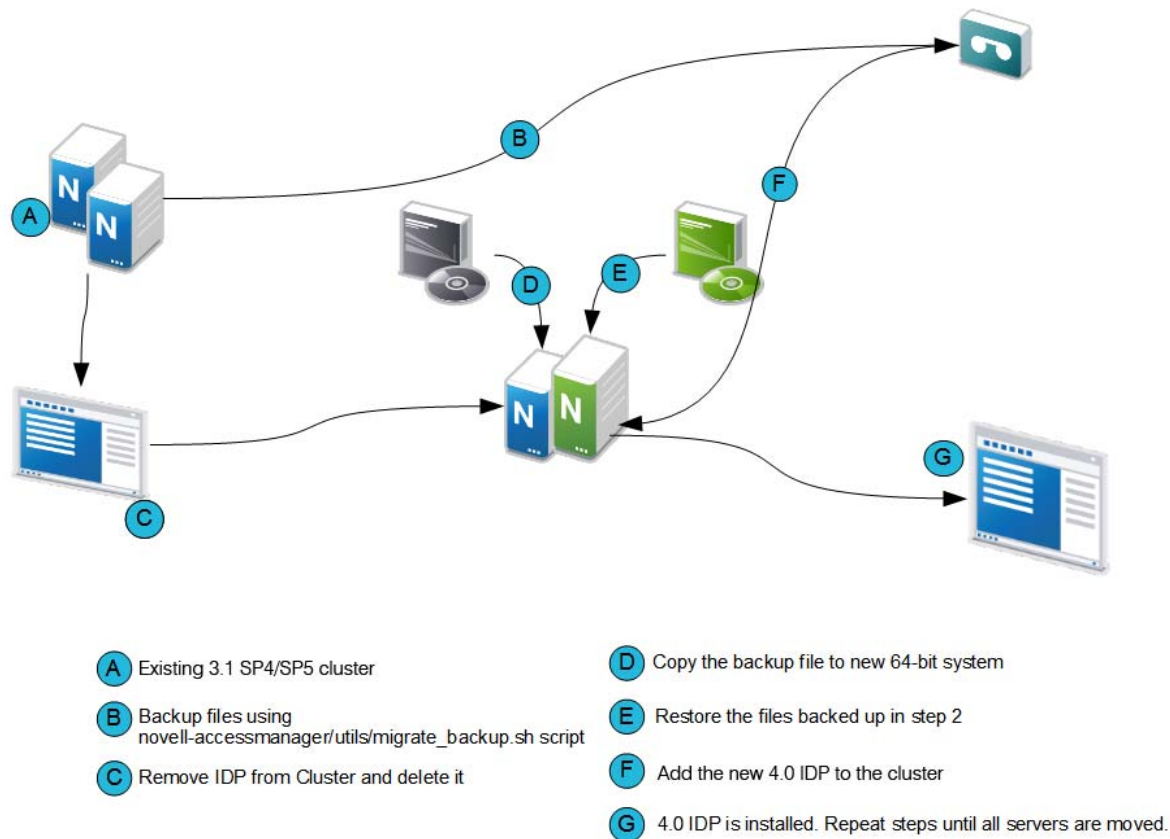
### Identity Server Is the Only Component on the Server

Workflow:

- 1 Back up the customized files.
- 2 Use the NetIQ Access Manager 4.0 installer to install the 4.0 Identity Server on a 64-bit Red Hat 6.4 or 6.5 operating system.
- 3 Add the 4.0 Identity Server to the existing Identity Server cluster in the Administration Console.
- 4 Update the Identity Server and apply changes.
- 5 Restore any customized files from the backup taken earlier.

## Process of Migration

Figure 2-4 Process of Migrating the Identity Server



**IMPORTANT:** Before you proceed with the steps for migration, ensure that you have followed the instructions in the [Prerequisites for the Identity Server Migration](#).

- 1 Stop the Identity Server and remove the Identity Server from the cluster configuration.
  - 1a In the Administration Console, click **Devices > Identity Servers**.
  - 1b Select the server, then click **Stop**.
  - 1c Select the server, then choose **Actions > Remove from cluster**.
  - 1d Update the cluster configuration.
- 2 If you are using an existing machine, delete the existing Identity Server from the Administration Console before installing the new Identity Server.
  - 2a In the Administration Console, click **Devices > Identity Servers**.
  - 2b Select the server, then click **Stop**.
  - 2c Click **Actions > Delete**.
- 3 If the operating system is already 64-bit Red Hat 6.4 or 6.5, uninstall the 3.1 SP4 or 3.1 SP5 version and install the 4.0 Identity Server.
- 4 Perform a new installation of 64-bit Red Hat 6.4 or 6.5 operating system.

For more information, see [Red Hat Enterprise Linux Installation Guide \(https://access.redhat.com/site/documentation/en-US/Red\\_Hat\\_Enterprise\\_Linux/6/pdf/Installation\\_Guide/Red\\_Hat\\_Enterprise\\_Linux-6-Installation\\_Guide-en-US.pdf\)](https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Installation_Guide/Red_Hat_Enterprise_Linux-6-Installation_Guide-en-US.pdf)..

- 5 Ensure you have downloaded the software or you have the CD available.

- 5a Insert the CD into the drive, then navigate to the device. Enter the following:

```
cd /media
```

Browse to your CD-ROM drive.

- 5b If you downloaded the `AM_40_AccessManagerService_Linux64.tar.gz` file, unpack the file using the following command:

```
tar -xzf AM_40_AccessManagerService_Linux64.tar.gz
```

- 6 Browse to the `novell-access-manager` folder.

All the files are extracted to the `novell-access-manager` folder.

- 7 Run the `install.sh` script from the `novell-access-manager` folder on a 64-bit Red Hat 6.4 or 6.5 server and choose the option to install the Identity Server.

- 8 Enter the following details:

- ♦ IP address of the 4.0 primary Administration Console as the primary Administration Console IP address
- ♦ Access Manager Administration User ID
- ♦ Access Manager Administration password
- ♦ Re-enter the password for verification

- 9 If local NAT is available for the Identity Server, enter the NAT IP address. For more information about configuring Network Address Translation, see “[Configuring Network Address Translation](#)” in the *NetIQ Access Manager 4.0 SP2 Installation Guide*.

- 10 Enter `y` to proceed with installation.

After installation, this Identity Server device is displayed in the Administration Console.

- 11 Restore any customized files from the backup taken earlier as part of steps in “[Prerequisites for the Identity Server Migration](#)” on page 24.

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

**Table 2-4** Restoring Files During IDP Migration

Old File Location	New File Location
C:\Program Files (x86)\Novell\Tomcat\conf\server.xml	/opt/novell/nam/idp/conf/server.xml
C:\Program Files (x86)\Novell\Tomcat\conf\web.xml	/opt/novell/nam/idp/webapps/nidp/WEBINF/ web.xml
C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\config	/opt/novell/nam/idp/webapps/nidp/config
C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\images	/opt/novell/nam/idp/webapps/nidp/images
C:\Program Files (x86)\Novell\jre\lib\security\bcslogin. conf	/opt/novell/java/jre/lib/security/ bcslogin.conf
C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp	/opt/novell/nam/idp/webapps/nidp/jsp
C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\WEB- INF\classes	/opt/novell/nam/idp/webapps/nidp/WEBINF/ classes

**server.xml:** If you have modified any elements or attributes in the 3.1 SP4 or 3.1 SP5 environment the corresponding changes will need to be applied to the 4.0 /opt/novell/nam/idp/conf/server.xml file.

Typical changes done to the server.xml in 3.1 SP4 or 3.1 SP5 include modifying the 'Address=' attribute to restrict the IP address the application will listen on, or 'maxThreads=' attribute to change the number of threads.

In the following example, 3.1 SP4 or 3.1 SP5 is customized to use the following ciphers.

```
<Connector NIDP_Name="connector" port="8443" address=""
ciphers="SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA,, ... ..>
```

When migrating to 4.0, copy the cipher list from your 3.1 SP4 or 3.1 SP5 server.xml and replace it in the SSL connector section of the 4.0 server.xml file.

**tomcat properties:** Go to C:\Program Files\Novell\Tomcat\bin\tomcat5w. Double-click the tomcat5w file and make a note of any elements or attributes customized in 3.1 SP4 or 3.1 SP5.

On the 4.0 server, go to C:\Program Files (x86)\Tomcat\bin\tomcat7w. Change the values and attributes as required.

For example, if you have modified the heap size in tomcat5w file, ensure you make the same changes in the tomcat7w file too

## 12 Add the newly installed Identity Server to the existing Identity Servers cluster.

For more information, see [“Clustering Identity Servers”](#) in the *NetIQ Access Manager 4.0 Setup Guide*.

The cluster object stores all the existing Identity Server configurations. The newly added Identity Servers inherit these configurations.

- 13 On the newly added Identity Server, restart Tomcat using the `/etc/init.d/novell-idp restart` or `rcnovell-idp restart` command.
- 14 Repeat [Step 1](#) through [Step 10](#) until all 3.1 SP4 or 3.1 SP5 Identity Servers are replaced with 4.0 Identity Servers.

## 2.2.3 Migrating 3.1 SP4 or 3.1 SP5 Access Gateway Appliance to 4.0 Access Gateway Appliance

- ♦ [“Prerequisites for the Access Gateway Appliance Migration”](#) on page 62
- ♦ [“Reusing an Existing IP Address”](#) on page 63
- ♦ [“Migration Process”](#) on page 64

### Prerequisites for the Access Gateway Appliance Migration

In addition to the following prerequisites, ensure that you also meet the hardware and software requirements for the Access Gateway. For details, see [“Linux Requirements”](#) in the *NetIQ Access Manager 4.0 SP2 Installation Guide*.

- ☐ Timeout Per Protected Resource (TOPPR) is enabled and applied in the Access Gateway. In the Administration Console, click **Devices > Access Gateways > Edit**, then click **Enable Timeout Per Protected Resource**.

If the **Enable Timeout Per Protected Resource** option has already been applied, it will not be displayed on the screen.

- ☐ Access Gateway should be in a cluster before migration. If the Access Gateway is on a single device, create an access gateway cluster with a single device before migration.

For more information, see [“Managing a Cluster of Access Gateways”](#) in the *NetIQ Access Manager 4.0 SP1 Access Gateway Guide*.

- ☐ You have physical access to the server or server console (in case of VMWare setups) as a root user and are familiar with firewall configurations. The required ports must be opened in the firewall. For more information about the ports, see [Section 1.1.4, “Port Details,”](#) on page 12.
- ☐ Ensure that you have migrated all the Administration Consoles and Identity Servers before migrating the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance to the 4.0 Access Gateway Appliance.
- ☐ Make a note of the IP addresses and host name of the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance before installing the Access Gateway Appliance. The IP address used by 3.1 SP4 or 3.1 SP5 Access Gateway Appliance to communicate with the Administration Console will be used for installing the Access Gateway Appliance.
- ☐ Determine if you want to reuse an existing IP address or use a new IP address for the migration process.
- ☐ Ensure that you have the same number of network interfaces on the new 4.0 Access Gateway as in the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance.
- ☐ If the services are managed by an L4 switch, remove the device that you are migrating from the L4 switch. Add the device back to the L4 switch once the migration is done successfully. This is required so that no user requests are sent by the L4 switch to that device during migration.
- ☐ If you have older versions prior to the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance, first upgrade to 3.1 SP4 or 3.1 SP5 by using the instructions at [Access Manager 3.1 Installation Guide](#).

- ❑ If you have customized any files back them up using the `migrate_backup.sh` script. This script is located in the `novell-access-manager` folder in the `AM_40_AccessManagerService_Linux64.tar.gz` file. Copy this script to the 3.1 SP4 or 3.1 SP5 server and run the script to back up.

It is important to take the backup regardless of whether you are reusing the same machine or a new server.

The files that get backed up are:

- ♦ `/var/opt/novell/tomcat5/conf/server.xml`
- ♦ `/var/opt/novell/tomcat5/conf/tomcat5.conf`
- ♦ `/var/opt/novell/tomcat5/conf/web.xml`
- ♦ `/var/opt/novell/tomcat5/webapps/nesp/WEB-INF/web.xml`
- ♦ `/var/opt/novell/tomcat5/webapps/nesp/jsp`
- ♦ `/var/opt/novell/tomcat5/webapps/nesp/html`
- ♦ `/var/opt/novell/tomcat5/webapps/nesp/images`
- ♦ `/var/opt/novell/tomcat5/webapps/nesp/config`
- ♦ `/chroot/lag/opt/novell/bin/preapply.sh`
- ♦ `/chroot/lag/opt/novell/bin/postapply.sh`
- ♦ `/var/novell/errorpagesconfig/current/ErrorMessage.xml`
- ♦ `/var/novell/ErrorPagesConfig.xml`

- ❑ If you have touch files configured in the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance, copy the touch file migration utility files `lag2mag_touchfiles.csv` and `migrate_touchfiles.sh` to the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance. These files are located in the `novell-access-manager/utils` folder in the `AM_AccessManagerService_Linux64.tar.gz` file.

Use the `sh migrate_touchfiles.sh > touchfile_list` command and back up the output file `touchfile_list`.

The `touchfile_list` file contains the options that needs to be mapped to the advanced options in Access Gateway Appliance.

Here is an example of sample output:

```
# Global Option example
NAGGlobalOptions InPlaceSilent=on

# Virtual Host/Server Option example
NAGGlobalOptions DebugHeaders=on
```

## Reusing an Existing IP Address

- ♦ [“3.1 SP4 or 3.1 SP5 Access Gateway Appliance Is the Only Component on the Server” on page 63](#)

### 3.1 SP4 or 3.1 SP5 Access Gateway Appliance Is the Only Component on the Server

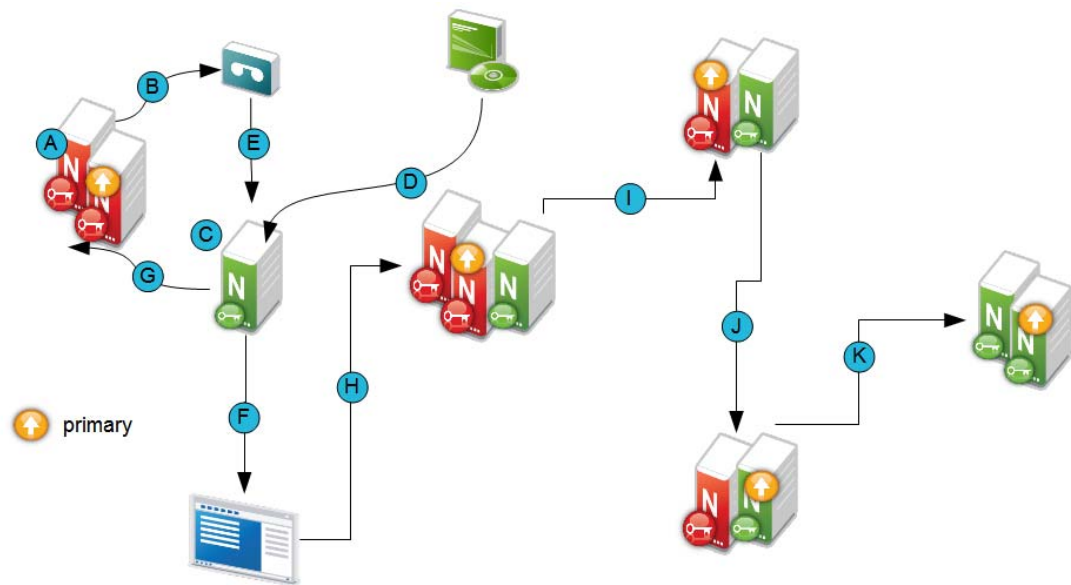
Workflow:

- 1 Back up any files that you have customized and note down the IP address and host name of 3.1 SP4 or 3.1 SP5 Access Gateway Appliance.
- 2 Shut down the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance.



- 3 Install the Access Gateway Appliance with the IP address and host name noted in [Step 1](#).
- 4 Restore any customized files from the backup taken earlier.

## Migration Process



- |   |  |   |
|---|--|---|
| <b>A</b> Existing 3.1 SP4/SP5 Access Gateway Appliances | <b>E</b> (Optional) Restore the files from the backup taken                                | <b>I</b> Remove one Linux Access Gateway from the cluster     |
| <b>B</b> (Optional) Take backup of customized files     | <b>F</b> Add the newly installed 4.0 Gateway Appliance to the existing 3.1 SP4/SP5 cluster | <b>J</b> Specify the Access Gateway as the Primary server     |
| <b>C</b> 64-bit Server                                  | <b>G</b> Copy the customized error message files   | <b>K</b> Convert all Linux Access Gateways to Access Gateways |
| <b>D</b> Install 4.0 Access Gateway Appliance           | <b>H</b> Mixed cluster setup   |   |

Migrating the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance to 4.0 Access Gateway Appliance will not cause any disruption to the existing setup. You can add new Access Gateway Appliance nodes into the existing 3.1 SP4 or 3.1 SP5 Access Gateway Appliance cluster. They can co-exist together.

If you are using a different server with a different IP address, see [“Use case scenario 1:” on page 34](#) and if you are reusing the same IP address, see [“Use case scenario 2:” on page 37](#).

### Use case scenario 1:

This scenario assumes that you have a new 64-bit server to install the 4.0 Access Gateway Appliance and explains how to migrate from 3.1 SP4 or 3.1 SP5 by using a different IP address.

Consider that the setup includes the following components:

- Administration Console (AC 1)
- Identity Server cluster (IDP 1 and IDP2)
- 3.1 SP4 or 3.1 SP5 Access Gateway Appliance cluster (LAG 1 and LAG 2).



## Migration Process

- 1 Determine which server in the 3.1 SP4 or 3.1 SP5 Access Gateway cluster is the primary server.

**1a** Login to Administration Console

**1b** Click **Devices > Access Gateways** > Select the device.

The list of servers are displayed. The primary server is indicated by a red mark beside the IP address.

### Access Gateways

Access Gateway Servers								
<a href="#">New Cluster...</a>   <a href="#">Restart</a>   <a href="#">Stop</a>   <a href="#">Refresh</a>   <a href="#">Actions</a> ▼								
<input type="checkbox"/> Name	Status	Health	Alerts	Commands	Statistics	Type	Configuration	
<a href="#">NAMAutomationLAG</a>	Current		0		<a href="#">View</a>		<a href="#">Edit</a>	
<input type="checkbox"/> <a href="#">172.16.0.0</a>	Current		0	<a href="#">Succeeded</a>	<a href="#">View</a>	Gateway Appliance		
<input type="checkbox"/> <a href="#">172.16.0.1</a>	Current		0	<a href="#">Succeeded</a>	<a href="#">View</a>	Gateway Appliance		
<input type="checkbox"/> <a href="#">172.16.0.2</a>	Current		0	<a href="#">Succeeded</a>	<a href="#">View</a>	Gateway Appliance		
<input type="checkbox"/> <a href="#">172.16.0.6</a>	Current		0	<a href="#">Succeeded</a>	<a href="#">View</a>	Gateway Appliance		

- 2 Install the Access Gateway Appliance (AG 1). For more information, see “[Installing the Access Gateway Appliance](#)” in the *NetIQ Access Manager 4.0 SP2 Installation Guide*. While installing the Access Gateway Appliance, specify the Administration Console's (AC 1) IP address, user name and password in the Administration Console Configuration field on the Appliance Configuration page.
- 3 Add the newly installed Access Gateway Appliance to the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance cluster. For more information, see “[Managing Access Gateways](#)”.
- 4 By default, all proxy services of newly added devices to the cluster are listening on the same IP address and port. To configure each reverse proxy service to a specific IP address and port, follow the steps below.
  - 4a** Configure a primary IP Address in YaST for the remaining interfaces.
    - 4a1** Go to YaST > Network Devices > Network Settings > Overview.
    - 4a2** Select the network card and click **Edit**.
    - 4a3** Specify the IP address.

Repeat the steps for all the interfaces.
  - 4b** Click **Devices > Access Gateways** > Select the device > **New IP** > click **OK**.
  - 4c** Add the secondary IP address if applicable to the interfaces from **Network Settings > Adapter List**.
  - 4d** Configure the DNS from **Network Settings > DNS**.
  - 4e** Add the Host entries (if any) from **Network Settings > Hosts**.
  - 4f** Set up the routing (if any) from **Network Settings > Gateways**.
  - 4g** Under Services, click on **Reverse Proxy/Authentication**. In the **Reverse Proxy List**, click the proxy service name. Select the newly added cluster member and select the **listening IP address** for that service.

(Optional) If you want to specify the outbound connection to the Web server, click **Web Servers**, then click **TCP Connect Options**. Select the **Cluster Member** and select the IP address from the drop down list against **Make Outbound Connection Using** if you want to select the outbound IP address to communicate with the Web server.

For more information about configuring the network settings, see “Configuring Network Settings” in the *NetIQ Access Manager 4.0 SP1 Access Gateway Guide*.

- 4h Restore any customized files backed up earlier as part of “Prerequisites for the Access Gateway Appliance Migration” on page 31.

Copy the content of the following files to the corresponding file in the new location.

**Table 2-5** Restoring Files during 4.0 Access Gateway Appliance Migration - Scenario 1

Old File Location	New File Location
/var/opt/novell/tomcat5/conf/web.xml	/opt/novell/nam/mag/conf/web.xml
/var/opt/novell/tomcat5/webapps/nesp/ WEB-INF/web.xml	/opt/novell/nam/mag/webapps/nesp/WEB- INF/web.xml
/var/opt/novell/tomcat5/webapps/nesp/jsp	/opt/novell/nam/mag/webapps/nesp/jsp
/var/opt/novell/tomcat5/webapps/nesp/ html	/opt/novell/nam/mag/webapps/nesp/html
/var/opt/novell/tomcat5/webapps/nesp/ images	/opt/novell/nam/mag/webapps/nesp/images
/var/novell/errorpagesconfig/current/ (Contains error messages and error pages configuration)	/opt/novell/nam/mag/webapps/agm/WEB-INF/ config/current
/var/opt/novell/tomcat5/webapps/nesp/ config	/opt/novell/nam/mag/webapps/nesp/config
/chroot/lag/opt/novell/bin/preapply.sh	/opt/novell/devman/jcc/scripts/ presysconfig.sh
/chroot/lag/opt/novell/bin/postapply.sh	/opt/novell/devman/jcc/scripts/ postsysconfig.sh

**NOTE:** The names of `preapply.sh` and `postapply.sh` files are different in the 4.0 environment. To restore these files, open the file and copy paste the entire content to the files in the 4.0 environment. Refer [Table 2-2 on page 36](#) for details of file locations.

**server.xml:** If you have modified any elements or attributes in the 3.1 SP4 or 3.1 SP5 environment the corresponding changes will need to be applied to the 4.0 `/opt/novell/nam/mag/conf/server.xml` file.

Typical changes done to the `server.xml` in 3.1 SP4 or 3.1 SP5 include modifying the 'Address=' attribute to restrict the IP address the application will listen on, or 'maxThreads=' attribute to modify the number of threads.

In the following example, 3.1 SP4 or 3.1 SP5 has customized `maxThreads` value.

```
<Connector port="9009" enableLookups="false" redirectPort="8443"
protocol="AJP/1.3" address="127.0.0.1" minSpareThreads="25"
maxThreads="300" backlog="0" connectionTimeout="20000", ... ..>
```

Make a note of the customizations and copy paste the changed values in the 4.0 `server.xml` file.

- 4i If you have customized the error pages for branding purposes, you will need to redo the changes in the 4.0 setup. For details on modifying messages and customizing pages, see [“Customizing the Error Pages”](#). The customized error messages can be restored by copying over the files as indicated in [Table 2-2 on page 36](#).

- 4j In the Administration Console, copy and paste the content of the previously referenced `touchfile_list` output file, under the following:

- ♦ Global Option files to **Access Gateways > Edit > Advanced Options**.

Example of Global Options in the `touchfile_list` file.

```
# Global Option example
NAGGlobalOptions InPlaceSilent=on
```

- ♦ Virtual Host/Server Option files to **Servers > Configuration > Reverse Proxy > Proxy Service > Advanced Options**.

Example of Virtual Host/Server Options in the `touchfile_list` file.

```
# Virtual Host/Server Option
NAGGlobalOptions DebugHeaders=on
```

- ♦ Files under the Administration Console are already available in the Access Gateway Appliance.

---

**NOTE:** Ensure that you do not have blank lines between each advanced option and also do not alter the content of `touchfile_list`.

For information about the migration utility files, `lag2mag_touchfiles.csv` and `migrate_touchfiles.sh` see, [“Utility Scripts” on page 113](#)

---

- 5 Test the Access Gateway Appliance functionality by accessing Access Gateway protected resources and making sure that the pages are rendered successfully.
- 6 Specify AG 1 as the primary server and click **Update**. For more information, see [“Changing the Primary Cluster Server”](#).
- 7 Remove the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance (LAG 1) from the cluster. For more information, see [“Viewing and Modifying Gateway Settings”](#).
- 8 Install 4.0 Access Gateway Appliance (AG 2) as in [Step 2](#) and add it to the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance cluster as in [Step 3](#).
- 9 After you confirm that all the services are up and running remove LAG2 from the cluster.
- 10 Remove the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance (LAG 2) from the cluster as in [Step 7](#).
- 11 Click **OK** and **Update all**.
- 12 Repeat [Step 2](#) to [Step 8](#) (except step 4j) until you have completely migrated all the existing 3.1 SP4 or 3.1 SP5 Access Gateway Appliance to 4.0 Access Gateway Appliance.  
After installing the Access Gateway Appliance, delete all the 3.1 SP4 or 3.1 SP5 Access Gateway Appliances from the Administration Console.
- 13 On the newly added Access Gateway server, restart Tomcat by using the `/etc/init.d/novell-mag restart` or `rcnovell-mag restart` command.

## Use case scenario 2:

This scenario assumes that you have a new/existing 64-bit server to install the 4.0 Access Gateway Appliance and explains how to migrate from 3.1 SP4 or 3.1 SP5 by using the existing IP address.

Consider that the setup includes the following components:

- ♦ Administration Console (AC 1)
- ♦ Identity Server cluster (IDP 1 and IDP 2)
- ♦ 3.1 SP4 or 3.1 SP5 Access Gateway Appliance cluster (LAG 1 and LAG 2)

## Migration Process

- 1 If you have a new 64-bit server to install 4.0 Access Gateway Appliance, ensure you do the following:
  - 1a Shut down LAG2 and
  - 1b Have the same number of Network Interface Cards as on LAG 2 and then proceed to step 2.

If you are reusing the existing LAG hardware, proceed to step 2.
- 2 Install the Access Gateway Appliance (AG 2) with the same IP address as of the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance (LAG 2). After the installation is complete, it will take some time to sync up the configuration. Ensure that you do not modify any configuration during this time.

When the configuration is synced up, the Access Gateway Appliance and the health of all the cluster members turns green.
- 3 Test the Access Gateway Appliance functionality by accessing Access Gateway protected resources and making sure pages are rendered successfully.
- 4 If you have customized the error pages for branding purposes, you will need to redo the changes in the 4.0 setup. For details on modifying messages and customizing pages, see [“Customizing the Error Pages”](#). The customized error messages can be restored by copying over the files as indicated in [Table 2-3 on page 39](#).
- 5 In the Administration Console, copy and paste the content of the previously referenced `touchfile_list` output file under the following:
  - ♦ Global Option files to **Access Gateways > Edit > Advanced Options**.

Example of Global Options in the `touchfile_list` file.

```
# Global Option example
NAGGlobalOptions InPlaceSilent=on
```
  - ♦ Virtual Host/Server Option files to **Servers > Configuration > Reverse Proxy > Proxy Service > Advanced Options**.

Example of Virtual Host/Server Options in the `touchfile_list` file.

```
# Virtual Host/Server Option
NAGGlobalOptions DebugHeaders=on
```
  - ♦ Files under the Administration Console are already available in the Access Gateway Appliance.

---

**NOTE:** Ensure that you do not have blank lines between each advanced option and also do not alter the content of the `touchfile_list` file.

For information about the migration utility files, `lag2mag_touchfiles.csv` and `migrate_touchfiles.sh` see, [“Utility Scripts” on page 113](#)

---

6 Click **OK** and **Update**.

7 Restore any customized files backed up earlier as part of “[Prerequisites for the Access Gateway Appliance Migration](#)” on page 31.

Copy the content of the following files to the corresponding file in the new location.

**Table 2-6** Restoring Files during 4.0 Access Gateway Appliance Migration -Scenario 2

Old File Location	New File Location
/var/opt/novell/tomcat5/conf/web.xml	/opt/novell/nam/mag/conf/web.xml
/var/opt/novell/tomcat5/webapps/nesp/ WEB-INF/web.xml	/opt/novell/nam/mag/webapps/nesp/WEB- INF/web.xml
/var/opt/novell/tomcat5/webapps/nesp/jsp	/opt/novell/nam/mag/webapps/nesp/jsp
/var/opt/novell/tomcat5/webapps/nesp/ html	/opt/novell/nam/mag/webapps/nesp/html
/var/opt/novell/tomcat5/webapps/nesp/ images	/opt/novell/nam/mag/webapps/nesp/images
/var/novell/errorpagesconfig/current/ (Contains error messages and error pages configuration)	/opt/novell/nam/mag/webapps/agm/WEB-INF/ config/current
/var/opt/novell/tomcat5/webapps/nesp/ config	/opt/novell/nam/mag/webapps/nesp/config
/chroot/lag/opt/novell/bin/preapply.sh	/opt/novell/devman/jcc/scripts/ presysconfig.sh
/chroot/lag/opt/novell/bin/postapply.sh	/opt/novell/devman/jcc/scripts/ postsysconfig.sh

**NOTE:** The names of `preapply.sh` and `postapply.sh` files are different in the 4.0 environment. To restore these files, open the file and copy paste the entire content to the files in the 4.0 environment. Refer [Table 2-2 on page 36](#) for details of file locations.

**server.xml:** If you have modified any elements or attributes in the 3.1 SP4 or 3.1 SP5 environment the corresponding changes will need to be applied to the 4.0 `/opt/novell/nam/mag/conf/server.xml` file.

Typical changes done to the `server.xml` in 3.1 SP4 or 3.1 SP5 include modifying the 'Address=' attribute to restrict the IP address the application will listen on, or 'maxThreads=' attribute to modify the number of threads.

In the following example, 3.1 SP4 or 3.1 SP5 has customized `maxThreads` value.

```
<Connector port="9029" enableLookups="false" protocol="AJP/1.3"
address="127.0.0.1" minSpareThreads="25" maxThreads="300" backlog="0"
connectionTimeout="20000", ... ..>
```

Make a note of the customizations and copy paste the changed values in the 4.0 `server.xml` file.

- 8 Repeat [Step 1](#) through [Step 6](#) except step 5 until you have completely migrated all the existing 3.1 SP4 or 3.1 SP5 Access Gateway Appliance to 4.0 Access Gateway Appliance.
- 9 On the newly added Access Gateway server, restart Tomcat by using the `/etc/init.d/novell-mag restart` or `rcnovell-mag restart` command.

---

**NOTE:** The Advanced options from the Administration Console are available only for the Access Gateway Appliance. For the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance, you should have touch files configured.

---

## 2.3 Migrating Access Manager on Windows

- ♦ [Section 2.3.1, “Prerequisites,” on page 70](#)
- ♦ [Section 2.3.2, “Migrating Administration Consoles From Windows 2003 to Windows 2008,” on page 71](#)
- ♦ [Section 2.3.3, “Migrating the Standalone Identity Servers from Windows 2003 to Windows 2008,” on page 73](#)

### 2.3.1 Prerequisites

- ♦ The 3.1 SP4 or 3.1 SP5 setup should be on Windows 2003.
- ♦ Back up your configuration. For instructions, see [Backing Up and Restoring](#) in the [Access Manager 3.1 SP5 Administration Console Guide](#).

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

- ♦ Back up the following files manually:
  - ♦ C:\Program Files\Novell\Tomcat\conf\server.xml
  - ♦ C:\Program Files\Novell\Tomcat\conf\web.xml
  - ♦ C:\Program Files\Novell\Tomcat\webapps\nidp\jsp
  - ♦ C:\Program Files\Novell\Tomcat\webapps\nidp\WEB-INF\lib\
  - ♦ C:\Program Files\Novell\jre\lib\security\bcslogin.conf
  - ♦ C:\Program Files\Novell\Tomcat\webapps\nidp\WEB-INF\classes
- ♦ For the Windows components (Identity Server, Administration Console, Access Gateway Appliance and Service), you should select a platform supported by Windows 2008 Server R2 Standard or Enterprise Edition.

## 2.3.2 Migrating Administration Consoles From Windows 2003 to Windows 2008

- 1 Before you proceed with the steps for migrating ensure you have followed the instructions in [Section 2.3.1, “Prerequisites,” on page 70](#).
- 2 Remove the Identity Server from the cluster configuration if the Identity Server is installed on the same machine as the Administration Console.
  - 2a In the Administration Console, click **Devices > Identity Servers**.
  - 2b Select the server, then click **Stop**. Wait for the Health indicator to turn red.
  - 2c Select the server, then choose **Actions > Remove from Cluster**.

---

**NOTE:** Shut down the old server to prevent duplicate IP address conflict. These IP addresses will be re-used in [Step 6](#).

---

- 3 Copy the files that are backed up to the new 64-bit server and shut down Windows 2003. The IP address and host name will be reused in [Step 6](#).
- 4 Perform a fresh installation of Windows 2008 R2 Server, 64-bit operating system on 64-bit hardware, in either Standard or Enterprise Edition with the latest patches applied.
- 5 If you have any secondary administration consoles, bring them down.
- 6 Install the 3.1 SP4 or 3.1 SP5 version of the Administration Console.

Use the same IP address and DNS name as that of Windows 2003.

For more information, see [Installing on Windows](#) in the [Access Manager 3.1 SP5 Installation Guide](#).

- 7 Restore any customized files from the backup taken earlier in [“Prerequisites” on page 70](#).

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

Old File Location	New File Location
C:\Program Files\Novell\Tomcat\conf\server.xml	C:\Program Files (x86)\Novell\Tomcat\conf\server.xml
C:\Program Files\Novell\Tomcat\conf\web.xml	C:\Program Files (x86)\Novell\Tomcat\conf\web.xml
C:\Program Files\Novell\Tomcat\webapps\nidp\jsp	C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp
C:\Program Files\Novell\Tomcat\webapps\nidp\WEB-INF\lib\	C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\WEB-INF\lib\
C:\Program Files\Novell\jre\lib\security\bcslogin.conf	C:\Program Files (x86)\Novell\jre\lib\security\bcslogin.conf
C:\Program Files\Novell\Tomcat\webapps\nidp\WEB-INF\classes	C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\WEB-INF\classes

**server.xml:** If you have modified any elements or attributes in the 3.1 SP4 or 3.1 SP5 environment on Windows 2003, the corresponding changes will need to be applied to the 3.1 SP4 or 3.1 SP5 C:\Program Files (x86)\Novell\Tomcat\conf\server.xml file on Windows 2008.

Typical changes done to the C:\Program Files\Novell\Tomcat\conf\server.xml in 3.1 SP4 or 3.1 SP5 include modifying the 'Address=' attribute to restrict the IP address the application will listen on, or 'Ciphers=' attribute to restrict ciphers used when communicating with application over SSL.

In the following example, 3.1 SP4 or 3.1 SP5 is customized to use the following ciphers:

```
<Connector NIDP_Name="connector" port="8443" address=""
ciphers="SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA, ... .."/>
```

When migrating to 3.1 SP4 or 3.1 SP5 to Windows 2008, copy this cipher list from your 3.1 SP4 or 3.1 SP5 server.xml on Windows 2003 and replace it in the SSL connector section of the 3.1 SP4 or 3.1 SP5 C:\Program Files (x86)\Novell\Tomcat\conf\server.xml on Windows 2008.

**Tomcat properties:** Go to C:\Program Files\Novell\Tomcat\bin\tomcat5w. Double-click the tomcat5w file and make a note of any elements or attributes customized in 3.1 SP4 or 3.1 SP5 on Windows 2003.

On Windows 2008 3.1 SP4 or 3.1 SP5 server, go to C:\Program Files (x86)\Novell\Tomcat\bin\tomcat5w. Change the values and attributes as required.

For example, if you have modified the heap size in tomcat5w file on Windows 2003, ensure you make the same changes in the tomcat5w file on Windows 2008 too.

**8** Modify the keystore locations in the server.xml file:

**8a** Log in to the Administration Console server as the administrator.

**8b** Open the server.xml file.

```
C:\Program Files (x86)\Novell\Tomcat\conf\server.xml
```

**8c** Search for the devman.keystore entry in the server.xml file

**8d** Change the path from

```
C:\Program Files\Novell\Tomcat\webapps\roma\WEB-INF\conf\devman.keystore
to
```

```
C:\Program Files (x86)\Novell\Tomcat\webapps\roma\WEB-INF\conf\
devman.keystore
```

**8e** Search for the tomcat.keystore entry in the server.xml file.

**8f** Change the path from

```
C:\Program Files\Novell\Tomcat\webapps\roma\WEB-INF\conf\tomcat.keystore
to
```

```
C:\Program Files (x86)\Novell\Tomcat\webapps\roma\WEB-
INF\conf\tomcat.keystore
```

**8g** Save the file.

**8h** Restart Tomcat.

```
net stop Tomcat5
net start Tomcat5
```

**9** Install the 3.1 SP4 or 3.1 SP5 version of the Identity Server.



For more information, see [Installing on Windows](#) in the [Access Manager 3.1 SP5 Installation Guide](#).

- 10 Restore any customized files from the backup taken earlier in “Prerequisites” on page 70 as in Step 7.
- 11 Add the Identity Server to the cluster configuration.  
For more information, see [Assigning an Identity Server to a Cluster Configuration](#) in the [Access Manager 3.1 SP5 Identity Server Guide](#).
- 12 Remove any secondary consoles from the configuration:
  - 12a In the Administration Console, click **Auditing > Troubleshooting**.
  - 12b In the **Other Known Device Manager Servers** section, click **Remove** to remove any secondary consoles.
- 13 Uninstall the secondary consoles.  
For more information, see [Uninstalling the Windows Administration Console](#) in the [Access Manager 3.1 SP5 Installation Guide](#).
- 14 Reinstall the secondary consoles as secondary consoles to the new primary console.  
For more information, see [Installing on Windows](#) in the [Access Manager 3.1 SP5 Installation Guide](#).

## 2.3.3 Migrating the Standalone Identity Servers from Windows 2003 to Windows 2008

- 1 Before you proceed with the steps for migrating ensure you have followed the instructions in [Section 2.3.1, “Prerequisites,” on page 70](#).
- 2 Remove the Identity Server from the cluster configuration.
  - 2a In the Administration Console, click **Devices > Identity Servers**.
  - 2b Select the server, then click **Stop**. Wait for the Health indicator to turn red.
  - 2c Select the server, then choose **Actions > Remove from Cluster**.
- 3 Perform a fresh installation of Windows 2008 R2 Server, 64-bit operating system on 64-bit hardware, in either Standard or Enterprise Edition with the latest patches applied.
- 4 Shut down the old server to prevent duplicate IP address conflict. These IP addresses will be re-used in the next step.
- 5 Install the 3.1 SP4 or 3.1 SP5 version of the Identity Server.  
Use the same IP address and DNS name for the Identity Server.
- 6 Restore any customized files from the backup taken earlier in “Prerequisites” on page 70.  
To restore the files, copy the content of the following files to the corresponding file in the new location.

Old File Location	New File Location
C:\Program Files\Novell\Tomcat\conf\web.xml	C:\Program Files (x86)\Novell\Tomcat\conf\web.xml
C:\Program Files\Novell\Tomcat\webapps\nidp\jsp	C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp

Old File Location	New File Location
C:\Program Files\Novell\Tomcat\webapps\nidp\WEB-INF\lib\	C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\WEB-INF\lib\
C:\Program Files\Novell\jre\lib\security\bcslogin.conf	C:\Program Files (x86)\Novell\jre\lib\security\bcslogin.conf
C:\Program Files\Novell\Tomcat\webapps\nidp\WEB-INF\classes	C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\WEB-INF\classes

## 7 Add the Identity Server to the cluster configuration.

For more information, see [Assigning an Identity Server to a Cluster Configuration](#) in the [Access Manager 3.1 SP5 Identity Server Guide](#).

---

# 3 Upgrading Access Manager

When you upgrade the Access Manager components, start the process by first backing up your configuration and then moving the Administration Console. You can then upgrade the various devices that you have imported into the Administration Console.

For instructions, see [“Backing Up the Access Manager Configuration”](#) in the *NetIQ Access Manager 4.0 SP1 Administration Console Guide*. This is useful when upgrade fails and you need to recover your previous configuration. For more information, see [“Restoring the Administration Console Configuration”](#).

We recommend that you upgrade all members of a cluster before moving to another type of device. You must upgrade the Access Manager components in the order of Administration Console, Identity Server, Access Gateway and then SSL VPN.

- ♦ [Section 3.1, “Upgrading on Linux,” on page 75](#)
- ♦ [Section 3.2, “Upgrading on Windows,” on page 89](#)

## 3.1 Upgrading on Linux

This section discusses how to upgrade Access Manager components to a higher version.

---

**NOTE:** (Access Manager 3.1 SP4 or 3.1 SP5) When using the Linux platform, only the 3.1 SP4 or 3.1 SP5 Access Gateway Service can be upgraded to Access Manager 4.0. Other Linux hosted 3.1 SP4 or 3.1 SP5 components such as the Administration Console, Identity Server, Access Gateway Appliance (also known as Linux Access Gateway), and SSL VPN must be migrated.

---

- ♦ [Section 3.1.1, “Upgrading from the Evaluation Version to the Purchased Version,” on page 75](#)
- ♦ [Section 3.1.2, “Upgrading the 3.1 SP4 or 3.1 SP5 Access Gateway Service,” on page 78](#)
- ♦ [Section 3.1.3, “Upgrading to Access Manager 4.0 SP1,” on page 80](#)
- ♦ [Section 3.1.4, “Applying Access Manager 4.0 Hotfix Patch for Linux,” on page 87](#)

### 3.1.1 Upgrading from the Evaluation Version to the Purchased Version

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

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

- ♦ [“Upgrading the Administration Console” on page 76](#)
- ♦ [“Upgrading the Identity Server” on page 76](#)

- ♦ “Upgrading the Access Gateway Appliance” on page 77
- ♦ “Upgrading the SSL VPN” on page 78

## Upgrading the Administration Console

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

- 1 Open a terminal window.
- 2 Log in as the `root` user.
- 3 Download the upgrade file from [dl.netiq.com \(https://dl.netiq.com/Download?buildid=XDUREId6sjA~\)](https://dl.netiq.com/Download?buildid=XDUREId6sjA~) and extract the `tar.gz` file using the following command:  
`tar -xzf <filename>.`
- 4 Change to the directory where you unpacked the file, then enter the following command in a terminal window:

```
./upgrade.sh
```

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

```
The following components were installed on this machine
```

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

- 6 Type **Y** and press Enter.
- 7 Enter the Access Manager Administration Console user ID.
- 8 Enter the Access Manager Administration Console password.
- 9 Re-enter the password for verification.
- 10 The system displays the following message when the upgrade is complete:

```
Successfully upgraded.
```

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

If you encounter an error, see [Section 5.11, “Troubleshooting a Linux Administration Console Upgrade,”](#) on page 109.

## Upgrading the Identity Server

Use the following procedure to upgrade the stand-alone Identity Server. If you have installed both the Identity Server and the Administration Console on the same machine, see [“Upgrading the Administration Console”](#) on page 81.

- 1 Open a terminal window.
- 2 Log in as the `root` user.
- 3 Download the upgrade file from [dl.netiq.com \(https://dl.netiq.com/Download?buildid=XDUREId6sjA~\)](https://dl.netiq.com/Download?buildid=XDUREId6sjA~) and extract the `tar.gz` file using the following command:  
`tar -xzf <filename>.`

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

```
./upgrade.sh
```

- 5 The system displays the following confirmation message:

```
The following components were installed on this machine
```

```
1. Identity Server
```

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

- 6 Type **Y** and press Enter.
- 7 Enter the Access Manager Administration Console user ID.
- 8 Enter the Access Manager Administration Console password
- 9 Re-enter the password for verification
- 10 The system displays the following message when the upgrade is complete:

```
Successfully upgraded.
```

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

## Upgrading the Access Gateway Appliance

**Prerequisite:** Before upgrading to 4.0 SP1, you must first upgrade the base operating system of the 4.0 Access Gateway appliance to the latest operating system that is included in the 4.0 SP1 Access Gateway appliance ISO. For more information about how to upgrade, see [Section 4.3, “Upgrading the Operating System for Access Gateway Appliance,” on page 104](#).

- 1 Open a terminal window.
- 2 Log in as the `root` user.
- 3 Download the upgrade file from [dl.netiq.com \(https://dl.netiq.com/Download?buildid=XDUREId6sjA~\)](https://dl.netiq.com/Download?buildid=XDUREId6sjA~) and extract the `tar.gz` file using the following command:  

```
tar -xzvf <filename>.
```
- 4 Change to the directory where you unpacked the file, then enter the following command in a terminal window:

```
./ma_upgrade.sh
```

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

---

**NOTE:** For upgrading the Access Gateway Service, see [Section 3.1.2, “Upgrading the 3.1 SP4 or 3.1 SP5 Access Gateway Service,” on page 78](#).

---

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

## Upgrading the SSL VPN

If you have installed both the SSL VPN and the Administration Console on the same machine, see [“Upgrading the Administration Console” on page 81](#).

- 1 Open a terminal window.
- 2 Log in as the `root` user.
- 3 Download the upgrade file from [dl.netiq.com \(https://dl.netiq.com/Download?buildid=XDUREId6sjA~\)](https://dl.netiq.com/Download?buildid=XDUREId6sjA~) and extract the `tar.gz` file using the following command:  
`tar -xzvf <filename>.`
- 4 Change to the directory where you unpacked the file, then enter the following command in a terminal window:

```
./upgrade.sh
```

- 5 The system displays the following confirmation message:

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

- 6 Type `Y` and press `Enter`.
- 7 Enter the Access Manager Administration Console user ID.
- 8 Enter the Access Manager Administration Console password
- 9 Re-enter the password for verification
- 10 The system displays the following message when the upgrade is complete:

```
Successfully upgraded.
```

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

### 3.1.2 Upgrading the 3.1 SP4 or 3.1 SP5 Access Gateway Service

- ♦ [“Prerequisites for Access Gateway Service” on page 78](#)
- ♦ [“Process” on page 78](#)

#### Prerequisites for Access Gateway Service

- ♦ Manually back up the `/var/opt/novell/tomcat5/conf/tomcat5.conf` and `/var/opt/novell/tomcat5/conf/server.xml` files.

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

#### Process

Before you proceed with the steps for upgrading ensure you have followed the instructions in the [“Prerequisites for Access Gateway Service” on page 78](#) section.

- 1 Download the `AM_40_AccessGatewayService_Linux_64.tar.gz` file from the NetIQ download site and extract it using the following command:  
`tar -xzvf <AM_40_AccessGatewayService_Linux_64.tar.gz>`
- 2 Run the `ag_upgrade.sh` script from the folder to start the upgrade.

The `ag_upgrade.sh` script upgrades the 3.1 SP4 or 3.1 SP5 Access Gateway Service to version 4.0.

**3** Specify the following information:

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

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

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

```
Starting Access Manager services...
Backup of customized files are available at /root/nambkup. Restore them if
required.
```

**4** View the log files. The install logs are located in the `/tmp/novell_access_manager/` directory.

**5** Restore any customized files from the backup taken earlier as part of steps in [“Prerequisites for Access Gateway Service” on page 78](#).

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

Old File Locations	New File Location
<code>/root/novell_access_manager/apache2/</code> (contains apache var files)	<code>/opt/novell/apache2/share/apache2/error</code>
<code>/root/novell_access_manager/nesp/</code> (contains modified error pages)	<code>/var/opt/novell/tomcat7/webapps/nesp/</code> <code>jsp/</code>

**server.xml:**

If you have modified any elements or attributes in the 3.1 SP4 or 3.1 SP5 environment the corresponding changes will need to be applied to the 4.0 `server.xml` file.

Typical changes done to the `server.xml` in 3.1 SP4 or 3.1 SP5 include modifying the `'Address='` to restrict the IP address the application will listen on, or `'maxThreads='` attributes to modify the number of threads.

In the following example, 3.1 SP4 or 3.1 SP5 has customized `maxThreads` value.

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

Make a note of the customizations and copy paste the changed values in the 4.0 `server.xml` file

**tomcat5.conf:**

Copy any elements or attributes that you have customized in the `tomcat5.conf` file to the `tomcat7.conf` file.

For example, if you have included the environment variable to increase the heap size by using `-Xmx/Xms/Xss` attributes in the `tomcat5.conf` file, copy this variable to the 4.0 `/opt/novell/nam/idp/conf/tomcat7.conf` file.

**6** Modify the required properties in `/opt/novell/nam/mag/webapps/agm/WEB-INF/agm.properties` using back up file `/root/novell_access_manager/agm/agm.properties`. If you have customized the `agm.properties` file from the backup taken in 3.1 SP4 or 3.1 SP5, ensure that you apply the same to the new 4.0 `/opt/novell/nam/mag/webapps/agm/WEB-INF/agm.properties` file. An example below shows the how to enable the backend webserver's webpage caching and the cache location.

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

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

```
chown -R novlwww:novlwww /var/opt/novell/tomcat7/webapps/nesp/jsp/
chown -R novlwww:novlwww /opt/novell/nam/mag/webapps/agm/WEB-INF/
agm.properties
```

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

### 3.1.3 Upgrading to Access Manager 4.0 SP1

For upgrading, you need to upgrade the components in the following order:

- ♦ [“Prerequisites” on page 80](#)
- ♦ [“Upgrading the Administration Console” on page 81](#)
- ♦ [“Upgrading the Identity Server” on page 82](#)
- ♦ [“Upgrading the Access Gateway Appliance” on page 84](#)
- ♦ [“Upgrading the SSL VPN” on page 85](#)
- ♦ [“Upgrading Access Gateway Appliance from 4.0 to 4.0 SP1” on page 87](#)

#### Prerequisites

Before upgrading the Access Manager components, ensure that you do the following:

- ♦ Ensure that you are either on Access Manager 3.2 Service Pack 2 or on Access Manager 4.0. Review the following table to understand the upgrade/ migrate paths for Access Manager 4.0 Service Pack 1 release.

Source	Migrate/Upgrade Paths to Access Manager 4.0 SP1
3.1.4/3.1.5	Migrate to 4.0 and then upgrade to 4.0 SP1
3.2.1/3.2.2	Upgrade to 4.0 and then upgrade to 4.0 SP1
3.2 Service Pack 2 or higher	Upgrade to 4.0 SP1
4.0 or 4.0 + Hotfixes	Upgrade to 4.0 SP1

- ♦ You must backup the files that you have customized.
- ♦ You will be able to upgrade to Access Manager 4.0 SP1, only if you have migrated all Linux Access Gateways (3.1.4/3.1.5) in the cluster to Access Gateway appliance (3.2.2 or 4.0) or removed all Linux Access Gateways (3.1.4/3.1.5) in the environment. If not, the Administration Console upgrade will detect the Linux Access Gateways in the configuration and terminates the upgrade.



- ♦ If you have custom partitioned your hard disk with partitions as in the table below, ensure that you have free disk space mentioned against each partition.

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

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

**NOTE:** If you do not upgrade the base operating system before upgrading to 4.0 SP1, upgrade will display an error message and terminates.

## Upgrading the Administration Console

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

- 1 Back up any customized JSP pages and related files.  
Even though the upgrade program backs up the JSP directory and its related files in the `/root/nambkup` folder, it is a good practice to backup these files.  
`/var/opt/novell/tomcat7/webapps/nidp/jsp`
- 2 Open a terminal window.
- 3 Log in as the `root` user.
- 4 Download the upgrade file from [dl.netiq.com](https://dl.netiq.com/Download?buildid=XDUREId6sjA~) (<https://dl.netiq.com/Download?buildid=XDUREId6sjA~>) and extract the `tar.gz` file using the following command:  
`tar -xzf <filename>`.
- 5 Change to the directory where you unpacked the file, then enter the following command in a terminal window:  
`./upgrade.sh`

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

The following components were installed on this machine

1. Access Manager Administration Console
2. Identity Server

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

- 7 Type **Y** to upgrade. A Warning message regarding backup and restore of JSP files is displayed.
- 8 Type **Y** to continue with the upgrade, then press Enter.
- 9 Type **Y** to restore the custom login pages.
- 10 Enter the Access Manager Administration Console user ID.
- 11 Enter the Access Manager Administration Console password.
- 12 Re-enter the password for verification.
- 13 The system displays the following message when the upgrade is complete:

Upgrade completed successfully.

- 14 (Optional) To view the upgrade files:

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

If you encounter an error, see [Section 5.11, “Troubleshooting a Linux Administration Console Upgrade,” on page 109](#).

## Upgrading the Identity Server

Use the following procedure to upgrade the stand-alone Identity Server. If you have installed both the Identity Server and the Administration Console on the same machine, see [“Upgrading the Administration Console” on page 81](#). For guidelines to upgrade from Access Manager 4.0 to 4.0 SP1, see [“Guidelines to Upgrade from Access Manager 4.0 to 4.0 SP1” on page 84](#).

---

**IMPORTANT:** Make sure to complete the following before you begin:

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

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

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

- 2 Open a terminal window.
- 3 Log in as the `root` user.

- 4 Download the upgrade file from [dl.netiq.com](http://dl.netiq.com) and extract the `tar.gz` file using the following command: `tar -xzf <filename>`.
- 5 Change to the directory where you unpacked the file, then enter the following command in a terminal window:

```
./upgrade.sh
```

- 6 The system displays the following confirmation message:

```
The following components were installed on this machine
```

```
1. Identity Server
```

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

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

- 8 Would you like to continue this upgrade? Type **Y** to upgrade.

- 9 The system displays the following message:

```
If old jsp pages need to be restored, ensure that you sanitize them to prevent possible Cross-site Scripting attacks. You can sanitize jsp pages after restoring them. Do you want to restore custom login pages? (y/n):
```

```
Type Y to restore.
```

- 10 Enter the Access Manager Administration Console user ID.

- 11 Enter the Access Manager Administration Console password

- 12 Re-enter the password for verification

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

```
Upgrade completed successfully.
```

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

- ♦ `/opt/novell/nam/idp/webapps/nidp/jsp`
- ♦ `/opt/novell/nam/idp/webapps/nidp/html`
- ♦ `/opt/novell/nam/idp/webapps/nidp/images`
- ♦ `/opt/novell/nam/idp/webapps/nidp/config`
- ♦ `/opt/novell/nam/idp/webapps/nidp/WEBINF/lib`
- ♦ `/opt/novell/nam/idp/webapps/nidp/WEBINF/web.xml`
- ♦ `/opt/novell/nam/idp/webapps/nidp/WEBINF/classes`
- ♦ `/opt/novell/nam/idp/webapps/nidp/WEBINF/conf`
- ♦ `/opt/novell/java/jre/lib/security/bcslogin.conf`
- ♦ `/opt/novell/java/jre/lib/security/nidpkey.keytab`
- ♦ `/opt/novell/nam/idp/webapps/nidp/`

- classUtils
- ♦ /opt/novell/nam/idp/conf/server.xml
- ♦ /opt/novell/nam/idp/conf/tomcat7.conf

---

**NOTE:** If you want to name the `.keytab` file to a name other than `nidpkey.keytab`, before upgrading, ensure that you modify the `upgrade_utility_functions.sh` script located under `novell-access-manager/scripts` folder.

---

## Guidelines to Upgrade from Access Manager 4.0 to 4.0 SP1

Starting from Access Manager 4.0 SP1 release, the default binding (WS-Trust) supported is SOAP 1.2. If you want to use SOAP 1.1 instead, perform the following steps on all instances of the Identity Server:

- 1 Traverse to the `/opt/novell/nam/idp/webapps/nidp/WEB-INF` folder and edit the `sun-jaxws.xml` file.
- 2 Remove all instances of bindings from the endpoints in the `sun-jaxws.xml` file and save the changes. A binding is represented by the following line in this file:

```
binding="http://java.sun.com/xml/ns/jaxws/2003/05/soap/bindings/HTTP/"
```

- 3 Restart the Identity Server using the `/etc/init.d/novell-idp restart` command.

---

**NOTE:** If you are upgrading the Identity Server from 4.0 to 4.0 SP1 and have configured the Google Authenticator custom class, all the existing (registered) users are moved to the new implementation seamlessly. But if you are a new user planning to register with the Google Authenticator, you must configure the contract using the TOTP class implementation available as part of 4.x.x.

---

## Upgrading the Access Gateway Appliance

**Prerequisite:** Before upgrading to 4.0 SP1, you must first upgrade the base operating system of the 4.0 Access Gateway appliance to the latest operating system that is included in the 4.0 SP1 Access Gateway appliance ISO. For more information about how to upgrade, see [Section 4.3, “Upgrading the Operating System for Access Gateway Appliance,”](#) on page 104.

- 1 Back up any customized JSP pages and related files.  
Even though the upgrade program backs up the JSP directory and its related files in the `/root/nambkup` folder, it is a good practice to backup these files.
- 2 Open a terminal window.
- 3 Log in as the `root` user.
- 4 Download the upgrade file from [dl.netiq.com](https://dl.netiq.com/Download?buildid=XDUREId6sjA~) (<https://dl.netiq.com/Download?buildid=XDUREId6sjA~>) and extract the `tar.gz` file using the following command:  

```
tar -xzvf <filename>.
```
- 5 Change to the directory where you unpacked the file, then enter the following command in a terminal window:  

```
./ma_upgrade.sh
```
- 6 A Warning message regarding backup and restore is displayed. If you have customized any files, take a backup and restore them after installation.
- 7 Would you like to continue this upgrade? Type **Y** to continue.
- 8 Do you want to restore custom login pages? Type **Y** to confirm.

- 9 Enter the Access Manager Administration Console user ID.
- 10 Enter the Access Manager Administration Console password
- 11 Re-enter the password for verification

---

**NOTE:** For upgrading the Access Gateway Service, see [Section 3.1.2, “Upgrading the 3.1 SP4 or 3.1 SP5 Access Gateway Service,” on page 78.](#)

---

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

Upgrade completed successfully.

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

- ♦ /opt/novell/nam/mag/tomcat7/conf/web.xml
- ♦ /opt/novell/nam/mag/tomcat7/webapps/  
nosp/WEB-INF/web.xml
- ♦ /opt/novell/nam/mag/tomcat7/webapps/  
nosp/jsp
- ♦ /opt/novell/nam/mag/tomcat7/webapps/  
nosp/html
- ♦ /opt/novell/nam/mag/tomcat7/webapps/  
nosp/images
- ♦ /opt/novell/nam/mag/webapps/agm/WEB-INF/  
config/current
- ♦ /opt/novell/nam/mag/tomcat7/webapps/  
nosp/config
- ♦ /opt/novell/devman/jcc/scripts/  
presysconfig.sh
- ♦ /opt/novell/devman/jcc/scripts/  
postsysconfig.sh

## Upgrading the SSL VPN

If you have installed both the SSL VPN and the Administration Console on the same machine, see [“Upgrading the Administration Console” on page 81.](#)

Make sure that you have done the following before you proceed with the upgrade:

- ♦ Upgrade the Administration Console, Identity Server, and Access Gateway Appliance before upgrading SSL VPN servers that are installed on separate machines.

If the SSL VPN server was installed with the other Access Manager components, the SSL VPN server is automatically upgraded along with the other components.

- ♦ If you have installed high bandwidth SSL VPN, make sure you download and install the high bandwidth SSL VPN RPM. SSL VPN has a high bandwidth RPM that needs to be installed once to get its capabilities. This RPM should be installed before upgrading the SSL VPN server. For information on how to install the high bandwidth SSL VPN RPM, see [“Installing the Key for High-Bandwidth SSL VPN” in the \*NetIQ Access Manager 4.0 SP2 Installation Guide\*](#)

- ♦ The Access Manager Administration Console must be up and running before you begin upgrading SSL VPN servers. Do not perform any configuration tasks in the Administration Console during an SSL VPN Server upgrade
- ♦ If you have customized the SSL VPN user interface, make a backup of the customized `sslvpnclient.jsp` file, then save it as `/var/opt/novell/tomcat7/webapps/sslvpnsslvpnclient.jsp.rpm` save file. If a file with that name already exists, then either delete or move the existing file to another location before saving the current `.jsp` file.

See “Customizing SSL VPN User Interface” in the *NetIQ Access Manager 4.0 SSL VPN Server Guide*.

- 1 Open a terminal window.
- 2 Log in as the `root` user.
- 3 Download the upgrade file from [dl.netiq.com](http://dl.netiq.com) and extract the `tar.gz` file using the following command: `tar -xzf <filename>`.
- 4 Change to the directory where you unpacked the file, then enter the following command in a terminal window:

```
./upgrade.sh
```

- 5 The system displays the following confirmation message:

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

- 6 A Warning message regarding backup and restore is displayed. If you have customized any files, take a backup and restore them after installation. For more information, see
- 7 Would you like to continue this upgrade? Type `Y` to continue.
- 8 Enter the Access Manager Administration Console user ID.
- 9 Enter the Access Manager Administration Console password
- 10 Re-enter the password for verification
- 11 The system displays the following message when the upgrade is complete:

```
Upgrade completed successfully.
```

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

- ♦ `/var/opt/novell/tomcat7/conf/server.xml`
- ♦ `/var/opt/novell/tomcat7/conf/tomcat7.conf`
- ♦ `/var/opt/novell/tomcat7/webapps/sslvpn/WEB-INF/web.xml`
- ♦ `/var/opt/novell/tomcat7/webapps/sslvpn/WEB-INF/conf`
- ♦ `/var/opt/novell/tomcat7/webapps/sslvpn/*.jsp`
- ♦ `/var/opt/novell/tomcat7/webapps/sslvpn/pages*`
- ♦ `/var/opt/novell/tomcat7/webapps/sslvpn/jsp`
- ♦ `/var/opt/novell/tomcat7/webapps/sslvpn/html`
- ♦ `/var/opt/novell/tomcat7/webapps/sslvpn/images`
- ♦ `/var/opt/novell/tomcat7/webapps/sslvpn/common`
- ♦ `/var/opt/novell/tomcat7/webapps/sslvpn/SSLVPNClientHelp`

## Upgrading Access Gateway Appliance from 4.0 to 4.0 SP1

**Prerequisite:** While upgrading Access Gateway appliance from 3.2x and 4.0 to 4.0 SP1, perform the following:

1. Before upgrading to 4.0 SP1, you must first upgrade the base operating system of the 4.0 Access Gateway appliance to the latest operating system that is included in the 4.0 SP1 Access Gateway appliance ISO. For more information about how to upgrade, see [Section 4.3, “Upgrading the Operating System for Access Gateway Appliance,”](#) on page 104.
2. Follow the procedure to upgrade the Access Gateway appliance. For more information about upgrading the Access Gateway appliance, see [“Upgrading the Access Gateway Appliance”](#) on page 84

### 3.1.4 Applying Access Manager 4.0 Hotfix Patch for Linux

You can upgrade Access Manager 4.0 to 4.0 Hotfix by applying the Hotfix patch.

---

**NOTE:** Hotfix\* is used to represent the hotfix number released for Access Manager 4.0.

Installing patches are not supported on the evaluation version. To install patches, upgrade to the licensed version using information at [Upgrading from the Evaluation Version to the Licensed Version \(https://www.netiq.com/documentation/netiqaccessmanager4/target\\_mig\\_upgrade/data/bzevr94.html#bzevtr2\)](https://www.netiq.com/documentation/netiqaccessmanager4/target_mig_upgrade/data/bzevr94.html#bzevtr2)

---

The patch helps you upgrade to the latest Access Manager with ease. Instead of downloading tar files that contain the entire set of binaries, you can download a `.zip` file that contains incremental changes in form of a patch file. You can use this patch file to update all components of your Access Manager.

If you have multiple components installed on the same system, the patch installation process will take care of updating all the binaries of these components. For example, if you have both Identity Server and Administration Console installed on a system, installing the patch takes care of updating the binaries of Identity Server and Administration Console.

---

**IMPORTANT:** In a cluster setup, ensure that you install the patch on each node of the Access Manager setup.

---

### Prerequisites

Ensure that you have installed the latest version of the product. Refer to the following readmes for verifying the version numbers of a specific Hotfix release:

- ♦ [Access Manager Appliance HF1 Readme](#)
- ♦ [Access Manager Appliance HF2 Readme](#)
- ♦ [Access Manager Appliance HF3 Readme](#)

## Installing the Patch

Perform the following steps before applying the patch.

- 1 Save the hotfix file to the server running Access Manager. If you have multiple servers in your set up, ensure that you copy this .zip file to all the servers.
- 2 Extract the patch file using the `unzip <patch name>.zip` command, where *<patch filename>* is the name of the patch file, for example, AM\_401\_HF1.

After extraction, the following files and folders are created in the *<patch name>* folder:

File/Folder Name	Description
rpm	Contains rpm files for the patch to run on a Linux server.
Patchtool	Contains logging properties file and files necessary for the patch to run on a Windows server.
installPtool.sh	Script to install the patch and the patch tool on a Linux server.
installPatch.sh	Script to install the HF* patch tool and the updated binaries on a Linux server.
installPtool.cmd	Script to install the patch on a Windows server.
<patch name>-xxx.patch	The patch file. The name of the patch file changes for each HF release.  <b>NOTE:</b> xxx represents the build number which is available in the respective release readme.

- 3 Log in as the root user.
- 4 Go to the location where you have extracted the patch files.
- 5 Run the `sh installPatch.sh` command.  
This command installs the patch and the bundled binaries.

**TIP:** To manage the Access Manager patch file, go to `/opt/novell/nam/patching/bin` folder.

If the patch is already installed, the installer exits with a message.

## Administering Patches

1. After the patch is installed, go to the `/opt/novell/nam/patching/bin` folder.
2. Use the following options to administer the Access Manager Appliance patch file.

**NOTE:** xxx represents the build number which is available in the respective release readme.

Option	Description	Command on Linux server
-qa	Lists all installed patches.	<code>./patch -qa</code>



Option	Description	Command on Linux server
-q	Lists details of an installed patch.	<pre>./patch -q</pre> <p>Example: If you have installed <i>&lt;latest release patch name&gt;</i>, use the following command: <code>./patch -q HF*-xxx</code></p>
-i	Installs a patch. During installation of a patch, all running services are stopped temporarily. After a patch is installed, all services are restarted and details of the operation are written to log files.	<pre>./patch -i &lt;location and patch name&gt;</pre> <p>Example: <code>./patch -i /tmp/AM_400_HF*-xxx.patch</code></p>
-e	Removes an installed patch. The patch maintains content relationship among patches. So, if you have installed patch 1 and patch 2, patch 1 cannot be removed without removing patch 2. This is because patch 2 contains details of patch 1 as well.	<pre>./patch -e &lt;patch name&gt;</pre> <p>Example: <code>./patch -e HF*-xxx</code></p>
	During the patch process, all the running services are stopped temporarily.	
-qpl	Lists details of a patch that is not installed. If you want to view the changes that are included in the patch file without installing it on your server, use this option	<pre>./patch -qpl &lt;location and patch name&gt;</pre> <p>Example: <code>./patch -qpl /tmp/AM_400_HF*-xxx.patch</code></p>
-v	Verifies integrity of a patch.	<pre>./patch -v &lt;location and patch name&gt;</pre> <p>Example: <code>./patch -v /tmp/AM_400_HF*-xxx.patch</code></p>
-t	Verifies if services can be restored by the installer.	<pre>./patch -t &lt;location and patch name&gt;</pre> <p>Example: <code>./patch -t /tmp/AM_400_HF*-xxx.patch</code></p>

## 3.2 Upgrading on Windows

- [Section 3.2.1, “Prerequisites,” on page 90](#)
- [Section 3.2.2, “Upgrading from Evaluation Version to the Purchased Version,” on page 90](#)
- [Section 3.2.3, “Upgrading Access Manager from 3.1 SP4 and 3.1 SP5 to 3.2.2 or 4.0,” on page 90](#)
- [Section 3.2.4, “Upgrading Access Manager from 3.2.2 to 4.0,” on page 95](#)
- [Section 3.2.5, “Applying Access Manager 4.0 Hotfix\\* Patch for Windows,” on page 98](#)

## 3.2.1 Prerequisites

In addition to the following prerequisites, ensure that you also meet the hardware requirements. For more information about hardware requirements, see the component-specific requirements in the [NetIQ Access Manager 4.0 SP2 Installation Guide](#).

- ❑ The 3.1 SP4 or 3.1 SP5 setup should be on Windows 2008 before upgrading to version 4.0. For more information, see the *Access Manager 3.1 SP5 Installation Guide* available in the [Novell Access Manager Documentation website](#).
- ❑ Before upgrading, back up your configuration using the `ambkup.bat` file. For instructions, see “[Backing Up the Access Manager Configuration](#)” in the *NetIQ Access Manager 4.0 SP1 Administration Console Guide*.

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

## 3.2.2 Upgrading from Evaluation Version to the Purchased Version

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

After you have purchased the product, log in to the [Novell Customer Center \(http://www.novell.com/center\)](http://www.novell.com/center) and follow the link that allows you to download the product. Then follow the instructions in [Section 3.2.4, “Upgrading Access Manager from 3.2.2 to 4.0,” on page 95](#) for upgrading components.

For verifying that Access Manager components have been upgraded, see [Access Manager HF3 Readme](#).

## 3.2.3 Upgrading Access Manager from 3.1 SP4 and 3.1 SP5 to 3.2.2 or 4.0

You can upgrade Access Manager from version 3.1 SP4 and 3.1 SP5 to 3.2 Service Pack 2 or 4.0.

Log in to the [NetIQ Downloads](#) page and follow the link that allows you to download the product.

- ♦ “[Upgrading the Administration Console](#)” on page 90
- ♦ “[Upgrading the Identity Server](#)” on page 92
- ♦ “[Upgrading the Access Gateway Service](#)” on page 94

### Upgrading the Administration Console

If you have installed the Administration Console and Identity Server on the same server, you must upgrade both of them at the same time. Upgrading 3.1 SP4 or 3.1 SP5 to 3.2.2 or 4.0 is supported only on Windows 2008.

---

**NOTE:** If your Access Manager 3.1 SP4 or 3.1 SP5 components are installed on Windows 2003, migrate them to 3.1 SP4 or 3.1 SP5 Windows 2008.

---

- 1 Manually back up your current Access Manager configuration using `ambkup.bat` file. For instructions, see “[Backing Up and Restoring](#)” in the *NetIQ Access Manager 4.0 SP1 Administration Console Guide*.
- 2 If the Identity Server is installed on the same server, manually back up the JSP pages and related files in the `C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp` directory.
- 3 If you have customized the `tomcat5.conf` file or the `server.xml` file, back up these files before upgrading. These files are overwritten during the upgrade process.

---

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

---

- 4 For upgrading to version 3.2.2: Download and run the Windows 64 `exe` file from NetIQ.  
For upgrading to version 4.0: Download and run `AM_40_AccessManagerService_Win64.exe` file from NetIQ.
- 5 Run the installation program. When the installation program detects an installed version of the Administration Console, it automatically prompts you to upgrade.
- 6 Read the Introduction, then click **Next**.
- 7 Accept the License Agreement, then click **Next**.
- 8 Select the component to upgrade that is currently installed, then click **Next**.
- 9 At the upgrade prompt, click **Continue**.
- 10 Specify the following information for the administrator account on the Administration Console:  
*Administration user ID:* Specify the name of the administration user for the Administration Console.  
*Password and Re-enter Password:* Specify and re-enter the password for the administration user account.
- 11 Decide whether you want the upgrade program to create a backup of your current configuration:
  - ♦ If you have a recent backup, click **Continue**. If you choose to not create a backup when you do not have a recent backup and you then encounter a problem during the upgrade, you may be forced to re-create your configuration.
  - ♦ If you do not have a recent backup, click **Run Config Backup**. The program creates a backup and stores it in the root of the operating system drive in the `nambkup` directory.
- 12 Review the summary, then click **Install**.
- 13 If the upgrade seems to hang and you have been performing other tasks on the desktop, click the installation screen and check for a warning message. Some subcomponents of Access Manager do not send warning messages to the Installation screen when the focus of the mouse is not on the installation window.
- 14 When you are prompted, reboot the server.
- 15 View the upgrade log file found in the following location:  
`C:\Program Files(x86)\Novell\log\AccessManagerServer_InstallLog.log`
- 16 If the Identity Server installed on the same server, copy any custom login pages to the `C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp` directory.
- 17 Restore any customized files from the backup taken earlier.  
To restore the files, copy the content of the following files to the corresponding file in the new location.

### server.xml:

If you have customized the `server.xml` file from the backup taken in 3.1 SP4 or 3.1 SP5, ensure that you apply the same to the new 3.2.2 or 4.0 `server.xml` located at `C:\Program Files (x86)\Novell\Tomcat\conf\` directory.

An example below shows that the IP address is removed and ciphers added.

```
<Connector
NIDP_Name="connector" port="8443" address=""
ciphers="SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA, ... .."/>
```

### Tomcat properties:

Go to `C:\Program Files\Novell\Tomcat\bin\tomcat5w`. Double-click the `tomcat5w` file and make a note of any elements or attributes customized in 3.1 SP4 or 3.1 SP5.

On the 3.2.2 or 4.0 server, go to `C:\Program Files (x86)\Tomcat\bin\tomcat7w`. Change the values and attributes as required.

For example, if you have modified the heap size in `tomcat5w` file, ensure you make the same changes in the `tomcat7w` file too.

---

**NOTE:** If you have installed the Identity Server with the Administration Console and you have customized login pages, decide whether you want your customized pages restored automatically. Be aware that any new features introduced in JSP files that have the same name as your files are lost, when your file overwrites the installed file with the automatic restore.

Wait until upgrade is complete. Compare your customized file with the newly installed file and then decide whether you need to modify your file before restoring it.

---

For more information about the Administration Console requirements, see [“Installation Requirements on Windows”](#) in the *NetIQ Access Manager 4.0 SP2 Installation Guide*.

## Upgrading the Identity Server

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

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

---

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

---

- 2 If you have customized the `tomcat5.conf` file or the `server.xml` file at `C:\Program Files (x86)\Novell\Tomcat\conf\`, back up these files before upgrading. The registries and the file are overwritten during the upgrade process.
- 3 For upgrading to version 3.2 x: Download and run `AM_32_AccessManagerService_Win64.exe` file from NetIQ.  
  
For upgrading to version 4.0: Download and run `AM_40_AccessManagerService_Win64.exe` file from NetIQ.  
  
This file starts the installation program. When the program detects an installed version of the Identity Server, it automatically prompts you to upgrade.
- 4 On the Introduction page, click **Next**.
- 5 Accept the License Agreement.
- 6 At the upgrade prompt, click **Continue**.
- 7 Specify the following information for the Administration Console:

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

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

- 8 If you have customized login pages, decide whether you want your customized pages restored automatically. Be aware that any new feature introduced in the JSP files that have the same name as your files are lost when your file overwrites the installed file with the automatic restore. You may want to wait until after the upgrade, then compare your customized file with the newly installed file. You can then decide whether you need to modify your file before restoring it.

---

**NOTE:** Ensure that you sanitize the restored customized JSP file to prevent XSS attacks. For more information about how to sanitize the JSP file, see [“Preventing Cross-site Scripting Attacks”](#) in the *NetIQ Access Manager 4.0 SP1 Identity Server Guide*.

---

- 9 Review the summary, then click **Install**.
- 10 View the upgrade log file found in the following location:

*Windows 2008:* C:\Program Files (x86)\Novell\log\AccessManagerServer\_InstallLog.log

- 11 Copy any custom login pages to the C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp directory.
- 12 Restore any customized files from the backup taken earlier.

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

**server.xml:**

If you have customized the `server.xml` file from the backup taken in 3.1 SP4 or 3.1 SP5, ensure that you apply the same to the new `server.xml` located at C:\Program Files (x86)\Novell\Tomcat\conf\ directory.

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

**Tomcat properties:** Go to C:\Program Files\Novell\Tomcat\bin\tomcat5w. Double-click the `tomcat5w` file and make a note of any elements or attributes customized in 3.1 SP4 or 3.1 SP5.

On the 3.2.2 or 4.0 server, go to C:\Program Files (x86)\Tomcat\bin\tomcat7w. Change the values and attributes as required.

For example, if you have modified the heap size in `tomcat5w` file, ensure you make the same changes in the `tomcat7w` file too.

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

---

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

---

## Upgrading the Access Gateway Service

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

- 1 Manually back up any customized tomcat files. If you have customized the `tomcat5.conf` file or the `server.xml` (`C:\Program Files\Novell\Tomcat\conf`) file, back up these files before upgrading. These files are overwritten during the upgrade process.
- 2 For upgrading to version 3.2 x: Download and run `AM_32_AccessGatewayService_Win64.exe` file from NetIQ.  
For upgrading to version 4.0: Download and run `AM_40_AccessGatewayService_Win64.exe` file from NetIQ.
- 3 Run the installation program. When the installation program detects an installed version of the Access Gateway, it automatically prompts you to upgrade.
- 4 Answer **Yes** to the prompt to upgrade.
- 5 Read the Introduction, then click **Next**.
- 6 Review the Readme information, then click **Next**.
- 7 Accept the License Agreement, then click **Next**.
- 8 Specify the following information:  
*User ID:* Specify the name of the administration user for the Administration Console.  
*Password and Re-enter Password:* Specify the password and re-enter the password for the administration user account.
- 9 Review the installation summary, then click **Install**.  
The Access Gateway Service is upgraded.
- 10 View the log files. The install logs are located in the `C:\Program Files\Novell\log` and `C:\agsinstall.log` directories.
- 11 Restore any customized files from the backup taken earlier.  
To restore the files, copy the content of the following files to the corresponding file in the new location.

### **server.xml:**

If you have customized the `server.xml` file from the backup taken in 3.1 SP4 or 3.1 SP5, ensure that you apply the same to the new `server.xml` located at `C:\Program Files\Novell\Tomcat\conf\` directory.

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

**Tomcat properties:** Go to `C:\Program Files\Novell\Tomcat\bin\tomcat5w`. Double-click the `tomcat5w` file and make a note of any elements or attributes customized in 3.1 SP4 or 3.1 SP5.

On the 3.2.2 or 4.0 server, go to `C:\Program Files\Novell\Tomcat\bin\tomcat7w`. Change the values and attributes as required.

For example, if you have modified the heap size in `tomcat5w` file, ensure you make the same changes in the `tomcat7w` file too.

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

## 3.2.4 Upgrading Access Manager from 3.2.2 to 4.0

Log in to the [NetIQ Downloads](#) page and follow the link that allows you to download the product.

- ♦ “Upgrading the Administration Console” on page 95
- ♦ “Upgrading the Identity Server” on page 96
- ♦ “Upgrading the Access Gateway Service” on page 97

### Upgrading the Administration Console

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

- 1 Manually back up your current Access Manager configuration using `ambkup.bat` file. For instructions, see “[Backing Up and Restoring](#)” in the *NetIQ Access Manager 4.0 SP1 Administration Console Guide*.
- 2 If the Identity Server is installed on the same server, manually back up the JSP pages and related files in the `C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp` directory.
- 3 If you have customized the `tomcat7.conf` file or the `server.xml` file, back up these files before upgrading. These files are overwritten during the upgrade process.

---

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

---

- 4 Run the installation program. When the installation program detects an installed version of the Administration Console, it automatically prompts you to upgrade.
- 5 Read the Introduction, then click **Next**.
- 6 Accept the License Agreement, then click **Next**.
- 7 Select the component to upgrade that is currently installed, then click **Next**.
- 8 At the upgrade prompt, click **Continue**.
- 9 Specify the following information for the administrator account on the Administration Console:  
**Administration user ID:** Specify the name of the administration user for the Administration Console.  
**Password and Re-enter Password:** Specify and re-enter the password for the administration user account.
- 10 Decide whether you want the upgrade program to create a backup of your current configuration:
  - ♦ If you have a recent backup, click **Continue**. If you choose to not create a backup when you do not have a recent backup and you then encounter a problem during the upgrade, you may be forced to re-create your configuration.
  - ♦ If you do not have a recent backup, click **Run Config Backup**. The program creates a backup and stores it in the root of the operating system drive in the `nambkup` directory.
- 11 Review the summary, then click **Install**.
- 12 If the upgrade seems to hang and you have been performing other tasks on the desktop, click the installation screen and check for a warning message. Some subcomponents of Access Manager do not send warning messages to the Installation screen when the focus of the mouse is not on the installation window.
- 13 When you are prompted, reboot the server.
- 14 View the upgrade log file found in the following location:

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

- 15 If the Identity Server installed on the same server, copy any custom login pages to the C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp directory.

- 16 Restore any customized files from the backup taken earlier.

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

#### **server.xml**

If you have customized the `server.xml` file from the backup taken in 3.2.2, ensure that you apply the same to the new 4.0 `server.xml` located at C:\Program Files (x86)\Novell\Tomcat\conf\ directory.

An example below shows that the IP address is removed and ciphers added.<Connector NIDP\_Name="connector" port="8443" address="" ciphers="SSL\_RSA\_WITH\_RC4\_128\_MD5, SSL\_RSA\_WITH\_RC4\_128\_SHA, ... .."/>

#### **Tomcat properties:**

Go to C:\Program Files\Novell\Tomcat\bin\tomcat7w. Double-click the `tomcat7w` file and make a note of any elements or attributes customized in 3.2.2.

On the 4.0 server, go to C:\Program Files (x86)\Tomcat\bin\tomcat7w. Change the values and attributes as required.

## Upgrading the Identity Server

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

---

**NOTE:** If you are upgrading the Identity Server from 4.0 to 4.0 SP1 and have configured the Google Authenticator custom class, all the existing (registered) users are moved to the new implementation seamlessly. But if you are a new user planning to register with the Google Authenticator, you must configure the contract using the TOTP class implementation available as part of 4.x.x.

---

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

---

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

---

- 2 If you have customized the `tomcat7.conf` file or the `server.xml` file at C:\Program Files (x86)\Novell\Tomcat\conf\, back up these files before upgrading. The registries and the file are overwritten during the upgrade process.
- 3 Download and run `AM_40_AccessManagerService_Win64.exe` file from NetIQ.

This file starts the installation program. When the program detects an installed version of the Identity Server, it automatically prompts you to upgrade.
- 4 On the Introduction page, click **Next**.
- 5 Accept the License Agreement.
- 6 At the upgrade prompt, click **Continue**.
- 7 Specify the following information for the Administration Console:

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

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



- 8 If you have customized login pages, decide whether you want your customized pages restored automatically. Be aware that any new feature introduced in the JSP files that have the same name as your files are lost when your file overwrites the installed file with the automatic restore. You may want to wait until after the upgrade, then compare your customized file with the newly installed file. You can then decide whether you need to modify your file before restoring it.

---

**NOTE:** Ensure that you sanitize the restored customized JSP file to prevent XSS attacks. For more information about how to sanitize the JSP file, see [“Preventing Cross-site Scripting Attacks”](#) in the *NetIQ Access Manager 4.0 SP1 Identity Server Guide*.

---

- 9 Review the summary, then click **Install**.

- 10 View the upgrade log file found in the following location:

C:\Program Files (x86)\Novell\log\AccessManagerServer\_ InstallLog.log

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

- 12 Restore any customized files from the backup taken earlier.

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

**server.xml**

If you have customized the `server.xml` file from the backup taken in 3.2.2, ensure that you apply the same to the new `server.xml` located at C:\Program Files (x86)\Novell\Tomcat\conf\ directory.

An example below shows that the IP address is removed and ciphers added.

```
<Connector
NIDP_Name="connector" port="8443" address=""
ciphers="SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA, ... .."/>
```

**Tomcat properties:**

Go to C:\Program Files\Novell\Tomcat\bin\tomcat7w. Double-click the `tomcat7w` file and make a note of any elements or attributes customized in 3.2.2.

On the 4.0 server, go to C:\Program Files (x86)\Tomcat\bin\tomcat7w. Change the values and attributes as required.

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

---

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

---

## Upgrading the Access Gateway Service

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

- 1 Manually back up any customized tomcat files. If you have customized the `tomcat7.conf` file or the `server.xml` (C:\Program Files\Novell\Tomcat\conf )file, back up these files before upgrading. These files are overwritten during the upgrade process.
- 2 Download and run `AM_40_AccessGatewayService_Win64.exe` file from NetIQ.

- 3 Run the installation program. When the installation program detects an installed version of the Access Gateway, it automatically prompts you to upgrade.
- 4 Answer **Yes** to the prompt to upgrade.
- 5 Read the Introduction, then click **Next**.
- 6 Review the Readme information, then click **Next**.
- 7 Accept the License Agreement, then click **Next**.
- 8 Specify the following information:
  - User ID:** Specify the name of the administration user for the Administration Console.
  - Password and Re-enter Password:** Specify the password and re-enter the password for the administration user account.
- 9 Review the installation summary, then click **Install**.  
The Access Gateway Service is upgraded.
- 10 View the log files. The install logs are located in the C:\Program Files\Novell\log and C:\agsinstall.log directories.
- 11 Restore any customized files from the backup taken earlier.  
To restore the files, copy the content of the following files to the corresponding file in the new location.
  - server.xml:**  
If you have customized the `server.xml` file from the backup taken in 3.2.2, ensure that you apply the same to the new `server.xml` located at C:\Program Files\Novell\Tomcat\conf\ directory.  
  
An example below shows that the IP address is removed and ciphers added.

```
<Connector
NIDP_Name="connector" port="8443" address=""
ciphers="SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA, ... .."/>
```
  - Tomcat properties:**  
Go to C:\Program Files\Novell\Tomcat\bin\tomcat7w. Double-click the `tomcat7w` file and make a note of any elements or attributes customized in 3.2.2  
  
On the 4.0 server, go to C:\Program Files\Novell\Tomcat\bin\tomcat7w. Change the values and attributes as required.
- 12 Restart the tomcat server by using the Windows service. Go to **Start > Control Panel > System and Security > Administrative Tools > Services**.

## 3.2.5 Applying Access Manager 4.0 Hotfix\* Patch for Windows

You can upgrade Access Manager 4.0 to 4.0 Hotfix by applying the Hotfix patch.

---

**NOTE:** Hotfix\* is used to represent the hotfix number released for Access Manager 4.0.

---

The patch helps you upgrade to the latest Access Manager with ease. Instead of downloading tar files that contain the entire set of binaries, you can download a .zip file that contains incremental changes in form of a patch file. You can use this patch file to update all components of your Access Manager

If you have multiple components installed on the same system, the patch installation process will take care of updating all the binaries of these components. For example, if you have both Identity Server and Administration Console installed on a system, installing the patch takes care of updating the binaries of Identity Server and Administration Console.

---

**IMPORTANT:** In a cluster setup, ensure that you install the patch on each node of the Access Manager setup.

---

## Prerequisites

Ensure that you have installed the latest version of the product. Refer to the following readmes for verifying the version numbers of a specific Hotfix release:

- ♦ [Access Manager Appliance HF1 Readme](#)
- ♦ [Access Manager Appliance HF2 Readme](#)
- ♦ [Access Manager Appliance HF3 Readme](#)

## Installing the Patch

Perform [Step 1 on page 88](#) and [Step 2 on page 88](#) to extract the files.

After extracting files from the `<patch name>.zip` file, install the patch by using the following command:

Log in as an administrator and from the command prompt, run the `installPtool.cmd` command. It will install the 4.0 HF\* binaries on the Windows system.

---

**TIP:** To manage your Access Manager patch file, go to the `C:\Program Files\Novell\patching\bin` folder.

---

## Installing and Administering Patches

1. After the patch is installed, go to the `C:\Program Files\Novell\patching\bin` folder.
2. Use the following options to administer the Access Manager patch file.

---

**NOTE:** xxx represents the build number which is available in the respective release readme.

---

Option	Description	Command on Windows server
-qa	Lists all installed patches.	<code>patch.cmd -qa</code>
-q	Lists details of an installed patch.	<code>patch.cmd -q</code>  Example: If you have installed <code>AM_400_HF*-xxx.patch</code> , use the following command: <code>patch.cmd -q HF*-xxx</code>
-i	Installs a patch. During installation of a patch, all running services are stopped temporarily. After a patch is installed, all services are restarted and details of the operation are written to log files.	<code>patch.cmd -i &lt;location and patch name&gt;</code>  Example: <code>patch.cmd -i C:/Patches/AM_400_HF*/AM_400_HF*-xxx.patch</code>

Option	Description	Command on Windows server
-e	Removes an installed patch. The patch maintains content relationship among patches. So, if you have installed patch 1 and patch 2, patch 1 cannot be removed without removing patch 2. This is because patch 2 contains details of patch 1 as well.  During the patch process, all the running services are stopped temporarily.	<code>patch.cmd -e &lt;patch name&gt;</code>  Example: <code>patch.cmd -e HF*-xxx</code>
-qpl	Lists details of a patch that is not installed. If you want to view the changes that are included in the patch file without installing it on your server, use this option	<code>patch.cmd -qpl &lt;location and patch name&gt;</code>  Example: <code>patch.cmd -qpl C:/Patches/AM_400_HF*/AM_400_HF*-xxx.patch</code>
-v	Verifies integrity of a patch.	<code>patch.cmd -v &lt;location and patch name&gt;</code>  Example: <code>patch.cmd -v C:/Patches/AM_400_HF*/AM_400_HF*-xxx.patch</code>
-t	Verifies if services can be restored by the installer. Use this option to stop/start all services after the installation of patch.	<code>patch.cmd -t &lt;location and patch name&gt;</code>  Example: <code>patch.cmd -t C:/Patches/AM_400_HF*/AM_400_HF*-xxx.patch</code>

---

# 4 Upgrading Kernel to the Latest Linux Security Patch

## Prerequisites

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

---

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

---

- ♦ [Section 4.1, “Installing or Updating Security Patches for the Access Gateway Appliance,” on page 101](#)
- ♦ [Section 4.2, “Configuring Subscription Management Tool for the Access Gateway Appliance,” on page 102](#)
- ♦ [Section 4.3, “Upgrading the Operating System for Access Gateway Appliance,” on page 104](#)

## 4.1 Installing or Updating Security Patches for the Access Gateway Appliance

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

- 1 Go to **YaST > Support > Novell Customer Center Configuration**.
- 2 Select **Configure Now (Recommended)**. In addition to the options that are selected by default, select **Registration Code**.
- 3 Click **Next**.  
The Manual Interaction Required screen appears. It might take a few minutes to connect to the server.  
This screen indicates that to activate the product, you must provide a valid e-mail ID associated with the Novell account and the activation code.
- 4 Click **Continue**.
- 5 To specify the e-mail address, activation code and system name in the relevant fields:
  - 5a Select the relevant option, then press **Enter**. A text field appears in the bottom left corner of the screen.
  - 5b Specify value for the selected option in this text field, then press **Enter** to return to the screen.
  - 5c Repeat these steps for each field.

6 Click **Submit** after you have specified all the relevant information to complete the registration.

7 Enter `q` to close the window.

8 Enter `y` at the prompt.

The Manual Interaction Required screen is displayed. It indicates that the software repositories are created. You will receive a message from the Novell Customer Center Configuration indicating that the configuration was successful.

9 Click **OK** to return to YaST Control Center.

10 Click **Quit** to exit YaST.

11 Open a shell prompt and specify the following command to verify if the repository named `NAM4x-APP-Updates` was created:

```
zypper lr
```

An output similar to the following appears

#	Alias	Enabled	Refresh	Name
1	NetIQAccessGatewayAppliance-4.x.x-x	Yes	No	NetIQAccessGatewayAppliance-4.x.x-x
2	nu_novell_com:NAM4x-APP-Updates	Yes	Yes	NAM4x-APP-Updates

12 Run the `zypper up` command to install the patches

13 After the patches are installed, restart the machine.

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

## 4.2 Configuring Subscription Management Tool for the Access Gateway Appliance

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

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

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

- [Section 4.2.1, “SMT Configuration,” on page 103](#)
- [Section 4.2.2, “Configuring the Access Gateway Appliance,” on page 103](#)
- [Section 4.2.3, “Troubleshooting,” on page 104](#)

## 4.2.1 SMT Configuration

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

- 1 Install the SMT server in a SLES 11 Server. For more information, see [Subscription Management Tool \(SMT\) for SUSE Linux Enterprise 11](#).
- 2 Log into your Novell Customer Center account.
- 3 Select **My Products > Mirroring Credentials**, then click **Generate Credentials**.
- 4 Copy the mirroring credentials before logging out of your Novell Customer Center account.
- 5 Run the *SMT Configuration* tool from YAST, then specify the mirroring credentials.
- 6 Run the **SMT Management** tool.  
The `NAM4x-APP-Updates`, `sle-11-x86_64` repository is displayed in the **Repositories** tab.
- 7 Select `sle-11-x86_64`, then click **Toggle Mirroring** to ensure mirroring is selected for this repository.
- 8 Click **Mirror Now**. This step ensures that the *NAM4x-APP-Updates* channel updates are mirrored from **nu.novell.com** to your local SMT server.
- 9 When mirroring is complete, click **OK** to close the tool.

## 4.2.2 Configuring the Access Gateway Appliance

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

You can use this script to configure a client machine to use the SMT server or to reconfigure it to use a different SMT server.

- 2 Specify the following command as `root` to execute the script on the client machine:

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

For example,

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

You can get the SMT server URL by running the SMT Configuration tool at the server. The URL is set by default.

- 3 Enter `y` to accept the CA certificate of the server.
- 4 Enter `y` to start the registration.
- 5 The script performs all necessary modifications on the client.
- 6 Execute the following command to perform registration:  

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

```
zypper up
```
- 8 Reboot the machine if prompted at the end of any patch install.
- 9 Confirm that all the patches are installed by running `zypper up` command once again.

## 4.2.3 Troubleshooting

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

## 4.3 Upgrading the Operating System for Access Gateway Appliance

The Access Gateway Appliance bundles the latest SUSE kernel. During fresh installation of Access Gateway appliance, the latest kernel will be installed automatically. During upgrade, you must upgrade the base operating system before upgrading the Access Gateway appliance. Perform the following steps to upgrade the base operating system.

- 1 Get the Access Gateway 4.0 SP1 appliance ISO and mount it in the Access Gateway server where you want to upgrade. For example if you want to mount on `/root/iso`, use the following command.

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

---

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

---

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

```
zypper ar /root/iso/ 40appiso
```

- 3 Refresh the repository using the following command.

```
zypper ref
```

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

```
zypper dup --from 40appiso
```

- 5 You will be prompted a dependency resolution for `usbutils`. Select **1** from the solutions.
- 6 Accept the license. The operating system will start upgrading.
- 7 After upgrade, view the notification.
- 8 Restart the Access Gateway appliance server.



---

# 5 Troubleshooting

- ♦ Section 5.1, "During Primary Administration Console Migration, ndsconfig rm Exits with "Error /opt/novell/eDirectory/bin/ndsconfig return value = 79"," on page 105
- ♦ Section 5.2, "While Migrating 3.1 SP4 Access Gateway with SSL VPN, ESP is in a Halted State After Rip and Replace," on page 106
- ♦ Section 5.3, "When Migration to 4.0 Access Manager Terminates Abruptly," on page 106
- ♦ Section 5.4, "Migration Exits Stating That the Server's DIB Does Not Contain Replicas," on page 107
- ♦ Section 5.5, "Exception During the Access Gateway Migration," on page 107
- ♦ Section 5.6, "Device Is Not Reachable After Migrating From the 3.1 SP4 Access Gateway Appliance to Access Gateway Appliance," on page 108
- ♦ Section 5.7, "Service Provider Does Not Start," on page 108
- ♦ Section 5.8, "The Access Gateway Throws a 403 Forbidden Page Error for a Resource Protected by a Form Fill Policy," on page 108
- ♦ Section 5.9, "Datastore Authentication Error, Bad Password or Certificate," on page 108
- ♦ Section 5.10, "DN Is Added as Provider ID While Installing NMAS SAML Method," on page 109
- ♦ Section 5.11, "Troubleshooting a Linux Administration Console Upgrade," on page 109
- ♦ Section 5.12, "WS-Trust Service Provider Attributes Sets Have to be Reconfigured After Upgrading Access Manager From 4.0 to 4.0 SP1," on page 110
- ♦ Section 5.13, "Unable to Access Identity Server Configuration Page After Upgrading from 3.2 SP3 to 4.0 SP1," on page 111

## 5.1 During Primary Administration Console Migration, ndsconfig rm Exits with "Error /opt/novell/eDirectory/bin/ndsconfig return value = 79"

To workaround this issue:

- 1 Open a terminal in the 4.0 Novell Administration Console.
  - 1a Run the `/opt/novell/eDirectory/bin/ndsrepair -N` command.
  - 1b Enter the server number.
  - 1c Enter the replica option 1 that is Repair all network addresses.
- 2 Open the terminal in the 3.1 SP4 or 3.1 SP5 Novell Administration Console.
  - 2a Run the following command and provide user name in the "admin.novell" format and password:

```
/opt/novell/eDirectory/bin/ndsconfig rm /etc/opt/novell/eDirectory/conf/nds.conf
```
  - 2b Provide the admin credentials and proceed with deletion.
- 3 Proceed with the migration steps.

## 5.2 While Migrating 3.1 SP4 Access Gateway with SSL VPN, ESP is in a Halted State After Rip and Replace

Keep the hostname and IP address same while migrating the 3.1 SP4 Access Gateway Appliance to 4.0 Access Gateway Appliance.

## 5.3 When Migration to 4.0 Access Manager Terminates Abruptly

The 4.0 migration may terminate due to any reason such as network issue. In such cases, re-run the migration after cleaning up partly installed components as in the following procedure:

To workaround this issue, perform the following steps to cleanup before re-running the `install_and_migrate` script:

- 1 Ensure that the 3.1 SP4 or 3.1 SP5 server remains as master replica
  - 1a In the 3.1 SP4 or 3.1 SP5 server, run the `ndsrepair -P -Ad` command.
  - 1b Enter 1 and press Enter.
  - 1c Enter 5 and press Enter.
- 2 Restore certificates back to 3.1 SP4 or 3.1 SP5.
  - 2a In the 3.1 SP4 or 3.1 SP5 server, go to `/opt/novell/devman/bin`, then run the `aminst-certs.sh` script.
  - 2b Enter the credentials and path for the backup file that was originally taken.
- 3 Remove the failed server.
  - 3a In the new 4.0 server, run the following command:

```
/opt/novell/eDirectory/bin/ndsconfig rm /etc/opt/novell/eDirectory/conf/nds.conf
```
  - 3b Enter the admin credentials in the admin.novell format and proceed with deletion.
- 4 In the new 4.0 machine, uninstall the Novell Access Manager binaries.
  - 4a From the `novell-access-manager` folder, run the `./uninstall.sh` script.
  - 4b Select the option **5** and proceed.
  - 4c Delete the `migrate_inputs.sh` script under `scripts` folder.
- 5 Delete objects from the eDirectory Configuration Store.
  - 5a Log in to the 3.1 SP4 or 3.1 SP5 Administration Console, then click **Auditing > Troubleshooting**.
  - 5b In the **Other Known Device Manager Servers** section, select the failed primary Administration Console.
  - 5c Click **Remove**.

Few objects in eDirectory require to be deleted. Sometime manual deletion could lead to errors. It is recommended to take a backup of entire eDirectory before you delete the objects.

Run the following command to back up the eDirectory objects:

```
ndsbackup cvf ndsbackupfile -a <user id like admin.novell> -p <password>
```

In case of any issue due to manual delete, you can restore the same by running the following command:

```
ndsbackup xvf ndsbackupfile
```

**5d** To delete the objects in eDirectory, select **View Objects** from the **iManager** menu bar.

**5e** In the Tree view, select **novell** and view the objects.

**5f** Delete all objects that refer to the failed primary console. You should find the following types of objects:

- ♦ SAS Service object with the host name of the failed primary console
- ♦ An object that starts with the last octet of the IP address of the failed primary console
- ♦ DNS AG object with the host name of the failed primary console
- ♦ DNS IP object with the host name of the failed primary console
- ♦ SSL CertificateDNS with the host name of the failed primary console
- ♦ SSL CertificateIP with the host name of the failed primary console

---

**NOTE:** You must follow the procedure irrespective of where the migration terminated to ensure that the machine is clean.

---

**6** On the 3.1 SP4 or 3.1 SP5 server, run the `/opt/novell/eDirectory/bin ndsstat -r` command to verify if there are any replicas in eDirectory caused due to failure while migrating. Ensure that you remove them.

**7** In the 4.0 server, run the `install_and_migate.sh` script the `novell-access-manager` folder and proceed with the installation steps.

## 5.4 Migration Exits Stating That the Server's DIB Does Not Contain Replicas

Some of the objects in the eDirectory store have invalid timestamps and the timestamps must be fixed before migrating.

To workaround this issue perform the following procedure:

- 1** Configure NTP server using YaST and synchronize the time.
- 2** Run the `ndsrepair -P -Ad` command, select option 1 and then option 12 which repairs the timestamps and declares a new epoch.
- 3** Run `ndsrepair -R`
- 4** Run the `nds restart` command at `/etc/init.d`.

## 5.5 Exception During the Access Gateway Migration

Exporting and importing policies from containers other than master containers will not automatically correct the existing policy references from the devices. You will have to re-reference to the imported policies.

To workaround this issue, perform the following steps:

- 1** In the Administration Console, click **Auditing > Troubleshooting > Policies**.
- 2** Click **Remove** under **Access Gateways with Protected Resources Referencing Nonexistent Policies**.

## 5.6 Device Is Not Reachable After Migrating From the 3.1 SP4 Access Gateway Appliance to Access Gateway Appliance

After migrating, Yast adds the default route through second interface if both the NIC interfaces are on the same subnet.

To workaround this issue, perform the following steps:

- 1 Go to **YaST > Network Devices > Network Settings > Routing** and remove the default gateway.
- 2 Select **Add** in the Routing Table and enter the following details:  
**Destination:** Enter the destination IP address 0.0.0.0.  
**Device:** Enter the device id eth0.  
**Gateway:** Enter the default gateway IP address.  
**Netmask:** Enter the netmask address 0.0.0.0.
- 3 Click **OK** and **Quit**. If the service provider does not start successfully perform the workaround provided in [Section 5.7, "Service Provider Does Not Start,"](#) on page 108.

## 5.7 Service Provider Does Not Start

After migrating and performing the workaround mentioned in [Device Is Not Reachable After Migrating From the 3.1 SP4 Access Gateway Appliance to Access Gateway Appliance](#), you may receive the following error message:

```
Start unsuccessful. Reason: Unable to read Truststore: /opt/novell/devman/jcc/certs/esp/6E781CF4892AB22D/truststore.keystore.
```

To workaround this issue, re-push the certificates from the **Administration Console > Troubleshooting > Certificates** and update the device. The service provider starts successfully.

## 5.8 The Access Gateway Throws a 403 Forbidden Page Error for a Resource Protected by a Form Fill Policy

This issue can happen if a Web server returns a form with a http 403 error code. The Access Gateway, by default, returns its own custom error pages. Hence, this prevents the Form Fill feature to work. To workaround, go to **Access Gateway > Advanced Options**, enter ProxyErrorOverride off > click **OK**.

## 5.9 Datastore Authentication Error, Bad Password or Certificate

After migrating to 4.0, when you log in to the Administration Console, the following alert is displayed:

```
Datastore authentication error, bad password or certificate.
```

This alert can be ignored because it does not have any impact on the functionality.

## 5.10 DN Is Added as Provider ID While Installing NMAS SAML Method

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

To resolve this issue, perform the following steps:

- 1 Log in to the 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>.

## 5.11 Troubleshooting a Linux Administration Console Upgrade

- [Section 5.11.1, “Upgrade Hangs,” on page 109](#)
- [Section 5.11.2, “Multiple IP Addresses,” on page 110](#)
- [Section 5.11.3, “Certificate Command Failure,” on page 110](#)

### 5.11.1 Upgrade Hangs

If the upgrade program encounters an error while installing a component or encounters an unexpected condition that requires user input, the installation appears to hang.

- 1 View the installation screen and determine which component is being upgraded.
- 2 Change to the `/tmp/novell_access_gateway` directory.
- 3 View the log file of the component that is being upgraded.

Solve the problem described in the log file before continuing with the upgrade.

For example, if the eDirectory health check fails, the `edir` log file indicates that the upgrade program is waiting for a response on whether the upgrade should continue. You should abort the upgrade, run `ndsrepair` to repair the configurations store, then restart with the upgrade process.

- 4 If the log file of the current component does not contain any errors, use the time stamps of the log files to determine which component just finished its upgrade and check it for errors.

If you cannot determine which component is causing the problem:

**4a** Abort the upgrade.

**4b** Enter the following command:

```
tail -f /tmp/novell_access_gateway
```

This command tails all the files created in the specified directory.

**4c** Restart the upgrade.

## 5.11.2 Multiple IP Addresses

If your server has multiple IP addresses, you might see the following error message during a Linux Administration Console upgrade:

```
Failed to load any MDB driver - Error: Could not load driver /usr/lib/mdb/mdbfile.so, error 9 - /usr/lib/mdb/mdbfile.so: cannot open shared object file: No such file or directory
```

The error occurs when running Novell Audit on servers with more than one IP address. It occurs when the system attempts to upgrade the audit server. Systems with more than one IP address have problems running Novell Audit because the multiple directory database (MDB) driver does not know which IP address to use with eDirectory. You can point Novell Audit to a specific IP address by creating an MDB configuration file.

The required filename and path for the MDB configuration file is as follows:

```
/etc/mdb.conf
```

To point Novell Audit to a specific IP address for eDirectory, the MDB configuration file must store the following parameters:

```
driver=mdbds referral=eDirectory_IP_ Address.
```

For example:

```
driver=mdbds referral=10.10.123.45.
```

You might only have one IP address, but your server might have two network adapters. If you create the `/etc/mdb.conf` file and specify your IP address, you do not encounter this error message when you upgrade.

## 5.11.3 Certificate Command Failure

Certificate commands are generated when you upgrade the Administration Console, and you should ensure that they have completed successfully. In the Administration Console, click **Security > Command Status**.

If a certificate command fails, note the store, then click **Auditing > Troubleshooting > Certificates**. Select the store, then click **Re-push certificates** to push the certificates to the store.

## 5.12 WS-Trust Service Provider Attributes Sets Have to be Reconfigured After Upgrading Access Manager From 4.0 to 4.0 SP1

While upgrading from 4.0 to 4.0 SP1, any attribute sets that are configured for WS-Trust service providers are no longer assigned.

Workaround: To resolve this issue, configure the Attribute Set and the Authentication Response. For more information, see [“Modifying Service Providers”](#) in the [“NetIQ Access Manager 4.0 SP1 Identity Server Guide”](#).

## 5.13 Unable to Access Identity Server Configuration Page After Upgrading from 3.2 SP3 to 4.0 SP1

After upgrading from 3.2 SP3 to 4.0 SP1, when you attempt to access the Identity Server an exception is displayed.

Workaround: To resolve this error, follow the details in [TID 7014856](#).





---

# A Utility Scripts

**Table A-1** *Utility Scripts*

Script Name	Description
ambkup.sh	Backs up the Access Manager configuration. This script is located in <code>/opt/novell/devman/bin/</code> .
install_and_migrate.sh	Migrates the Access Manager Administration Console from 3.1 SP4 or 3.1 SP5 to 4.0. This script is located in the <code>novell-access-manager</code> folder in the <code>AM_40_AccessManagerService_Linux64.tar.gz</code> file.
install.sh	Installs the fresh 4.0 Access Manager components. This script is located in the <code>novell-access-manager</code> folder in the <code>AM_40_AccessManagerService_Linux64.tar.gz</code> file.
migrate_backup.sh	Backs up any customized files of Identity Server, 3.1 SP4 or 3.1 SP5 Access Gateway and SSL VPN. This script is located in the <code>novell-access-manager</code> folder in the <code>AM_40_AccessManagerService_Linux64.tar.gz</code> file.
lag2mag_files.csv and migrate_files.sh	These files when copied and run on the 3.1 SP4 or 3.1 SP5 Access Gateway Appliance help in finding the equivalent Access Gateway advanced option. This file and script are located in the <code>novell-access-manager/utls</code> folder in the <code>AM_40_AccessManagerService_Linux64.tar.gz</code> file and also in <code>/opt/novell/ag/doc/</code> directory on the 4.0 Access Gateway Appliance.
appliance_backup.sh	Backs up customized files for all components of Access Manager. This script is available for Access Manager on Linux and Access Manager Appliance. It is located in the scripts folder of the install jar file.

