

## Quick Start

# Novell® Access Manager

### 3.1 SP3

June 29, 2010

[www.novell.com](http://www.novell.com)



## Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2008-2010 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.  
404 Wyman Street, Suite 500  
Waltham, MA 02451  
U.S.A.  
[www.novell.com](http://www.novell.com)

*Online Documentation:* To access the latest online documentation for this and other Novell products, see the [Novell Documentation Web page \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

## **Novell Trademarks**

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

## **Third-Party Materials**

All third-party trademarks are the property of their respective owners.



# Contents

<b>About This Guide</b>	<b>7</b>
<b>1 Installation Quick Start</b>	<b>9</b>
1.1 System Requirements	9
1.2 Administration Console	10
1.2.1 Linux Administration Console	10
1.2.2 Windows Administration Console	10
1.3 Identity Server	10
1.3.1 Linux Identity Server	11
1.3.2 Windows Identity Server	11
1.4 Access Gateway Appliance	11
1.5 Access Gateway Service	12
1.6 SSL VPN Server	12
1.7 Verifying the Installation	13
<b>2 Configuration Quick Start</b>	<b>15</b>
2.1 New Identity Server Cluster Configuration	15
2.2 First Reverse Proxy Configuration	18
2.3 Configuring the Protected Resource for Authentication	19
2.4 Basic Configuration for SSL VPN	20
2.4.1 Configuring Authentication for ESP-Enabled SSL VPN	20
2.4.2 Accelerating the Traditional SSL VPN Server	21
<b>3 SSL Configuration Quick Start</b>	<b>23</b>
3.1 Configuring a New Identity Server Cluster with SSL	23
3.2 Configuring a New Access Gateway for SSL	26



# About This Guide

This guide is designed to help you get a basic Access Manager system installed and configured. It contains the following:

- ♦ [Chapter 1, “Installation Quick Start,” on page 9](#)
- ♦ [Chapter 2, “Configuration Quick Start,” on page 15](#)
- ♦ [Chapter 3, “SSL Configuration Quick Start,” on page 23](#)

## Audience

This guide is intended for Access Manager administrators who are new to the product.

## Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to [www.novell.com/documentation/feedback.html](http://www.novell.com/documentation/feedback.html) and enter your comments there.

## Documentation Updates

For the most recent version of the *Access Manager Quick Start Guide*, visit the [Novell Access Manager Documentation Web site](http://www.novell.com/documentation/novellaccessmanager31) (<http://www.novell.com/documentation/novellaccessmanager31>).

## Additional Documentation

- ♦ [Novell Access Manager 3.1 SP2 Installation Guide](#)
- ♦ [Novell Access Manager 3.1 SP2 Setup Guide](#)
- ♦ [Novell Access Manager 3.1 SP2 Administration Console Guide](#)
- ♦ [Novell Access Manager 3.1 SP2 Policy Guide](#)
- ♦ [Novell Access Manager 3.1 SP2 Identity Server Guide](#)
- ♦ [Novell Access Manager 3.1 SP2 Access Gateway Guide](#)
- ♦ [Novell Access Manager 3.1 SP2 SSL VPN Server Guide](#)
- ♦ [Novell Access Manager 3.1 SP2 J2EE Agent Guide](#)

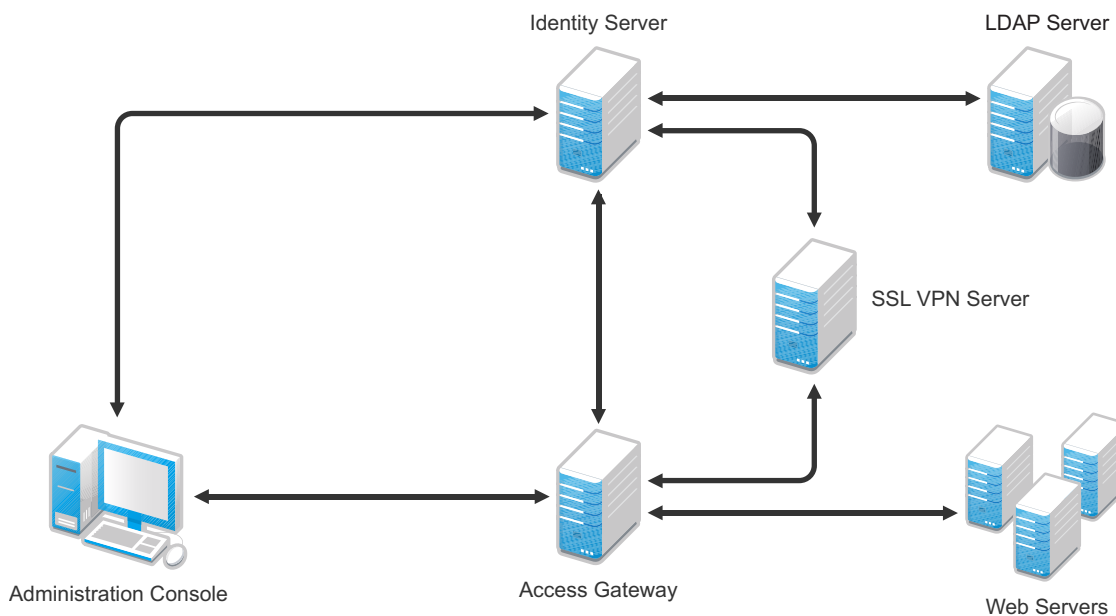




# Installation Quick Start

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. [Figure 1-1](#) illustrates a setup where these components are installed on separate machines.

**Figure 1-1** Basic Installation



The Administration Console must be installed first. The other components can then be installed in any order. The SSL VPN server can be installed so that it communicates with the Identity Server or with the Access Gateway for authentication credentials.

- ♦ [Section 1.1, “System Requirements,” on page 9](#)
- ♦ [Section 1.2, “Administration Console,” on page 10](#)
- ♦ [Section 1.3, “Identity Server,” on page 10](#)
- ♦ [Section 1.4, “Access Gateway Appliance,” on page 11](#)
- ♦ [Section 1.5, “Access Gateway Service,” on page 12](#)
- ♦ [Section 1.6, “SSL VPN Server,” on page 12](#)
- ♦ [Section 1.7, “Verifying the Installation,” on page 13](#)

## 1.1 System Requirements

Review the following sections to ensure that your machines or virtual images meet the installation prerequisites:

- ♦ [“Administration Console Requirements”](#) in the *Novell Access Manager 3.1 SP2 Installation Guide*

- ♦ “Identity Server Requirements” in the *Novell Access Manager 3.1 SP2 Installation Guide*
- ♦ “Access Gateway Requirements” in the *Novell Access Manager 3.1 SP2 Installation Guide*
- ♦ “SSL VPN Requirements” in the *Novell Access Manager 3.1 SP2 Installation Guide*

## 1.2 Administration Console

---

What you need to know	<ul style="list-style-type: none"> <li>♦ The username and password you want to use for the Access Manager administrator.</li> <li>♦ This is your first installation of an Administration Console, so answer Yes for a primary installation, when prompted.</li> <li>♦ You can create a failover environment by installing more than one Administration Console. For more information, see “Clustering and Fault Tolerance” in the <i>Novell Access Manager 3.1 SP2 Setup Guide</i>.</li> </ul>
For more information	See “Installing the Access Manager Administration Console” in the <i>Novell Access Manager 3.1 SP2 Installation Guide</i> .

---

### 1.2.1 Linux Administration Console

- 1 Download the `tar.gz` file, extract it, and use `install.sh` to start the installation.

For software download instructions, see the “Novell Access Manager Readme” ([http://www.novell.com/documentation/novellaccessmanager31/accessmanager\\_readme/data/accessmanager\\_readme.html](http://www.novell.com/documentation/novellaccessmanager31/accessmanager_readme/data/accessmanager_readme.html)).

- 2 At the Installation menu, select 1, then follow the prompts.
- 3 Answer Yes to the primary installation prompt.

### 1.2.2 Windows Administration Console

- 1 Download the Windows file and execute it.

For software download instructions, see the “Novell Access Manager Readme” ([http://www.novell.com/documentation/novellaccessmanager31/accessmanager\\_readme/data/accessmanager\\_readme.html](http://www.novell.com/documentation/novellaccessmanager31/accessmanager_readme/data/accessmanager_readme.html)).

- 2 Select to install the *Novell Access Manager Administration* component.
- 3 Answer Yes to the primary installation prompt.

## 1.3 Identity Server

The Identity Server can be installed on its own machine or with the Administration Console.

---

What you need to know	<ul style="list-style-type: none"> <li>♦ Username and password of the Access Manager administrator.</li> <li>♦ (Conditional) IP address of the Administration Console if it is installed on a separate machine</li> </ul>
For more information	See “Installing the Novell Identity Server” in the <i>Novell Access Manager 3.1 SP2 Installation Guide</i> .

---

### 1.3.1 Linux Identity Server

- 1 Download the `tar.gz` file, extract it, and use `install.sh` to start the installation.

For software download instructions, see the “Novell Access Manager Readme” ([http://www.novell.com/documentation/novellaccessmanager31/accessmanager\\_readme/data/accessmanager\\_readme.html](http://www.novell.com/documentation/novellaccessmanager31/accessmanager_readme/data/accessmanager_readme.html)).

- 2 At the Installation menu, select 2, then follow the prompts.

### 1.3.2 Windows Identity Server

- 1 Download the Windows file and execute it.

For software download instructions, see the “Novell Access Manager Readme” ([http://www.novell.com/documentation/novellaccessmanager31/accessmanager\\_readme/data/accessmanager\\_readme.html](http://www.novell.com/documentation/novellaccessmanager31/accessmanager_readme/data/accessmanager_readme.html)).

- 2 Select to install the *Novell Identity Server* component.

## 1.4 Access Gateway Appliance

---

What you need to know

- ♦ Username and password of the Access Manager administrator.
- ♦ IP address of the Administration Console.
- ♦ Static IP address, hostname, and domain name to use for the Linux Access Gateway.
- ♦ Network settings: IP address of default gateway and the subnet mask for your network.
- ♦ DNS settings: the IP address of one or two DNS servers.

For more information

See “Installing the Linux Access Gateway Appliance” in the *Novell Access Manager 3.1 SP2 Installation Guide*.

---

- 1 Insert the CD.
- 2 At the installation options page, select *Standard Installation*.
- 3 Accept the license agreement.
- 4 Select an appropriate keyboard and time zone.
- 5 Change the date and time to match the Identity Server.
- 6 Specify the following information:
  - ♦ The Network Configuration information. Specify the IP address you have selected for the Access Gateway.
  - ♦ A password for the `root` user.
  - ♦ The hostname and domain name for the Access Gateway and the IP address of at least one DNS server.
  - ♦ The IP address, username, and password of the Administration Console.
  - ♦ (Optional) If you want to install SSL VPN along with Linux Access Gateway, select *Install and enable SSL VPN Service*.
- 7 Click *Next* and review the installation settings page.

- 8 Click *Install* to continue with installation.

During installation, the machine reboots. During the reboot, some error messages are displayed. Let them scroll by and wait for the login prompt.

## 1.5 Access Gateway Service

---

What you need to know	<ul style="list-style-type: none"> <li>♦ Username and password of the Access Manager administrator.</li> <li>♦ IP address of the Administration Console.</li> </ul>
For more information	See “ <a href="#">Installing the Access Gateway Service</a> ” in the <a href="#">Novell Access Manager 3.1 SP2 Installation Guide</a> .

---

- 1 Download the file to the Linux or Windows machine.

For software download instructions, see the “[Novell Access Manager Readme](http://www.novell.com/documentation/novellaccessmanager31/accessmanager_readme/data/accessmanager_readme.html)” ([http://www.novell.com/documentation/novellaccessmanager31/accessmanager\\_readme/data/accessmanager\\_readme.html](http://www.novell.com/documentation/novellaccessmanager31/accessmanager_readme/data/accessmanager_readme.html)).

- 2 (Linux) Grant execute rights to the installation program.

- 3 Start the installation program:

**Linux:** Enter the following command:

```
./<filename>
```

**Windows:** Double-click the executable file.

- 4 Accept the license agreement.
- 5 Specify the Administration Console information.
- 6 Configure the disk cache.
- 7 Review the installation summary.
- 8 If everything looks correct, select to install.

## 1.6 SSL VPN Server

---

What you need to know	<ul style="list-style-type: none"> <li>♦ Username and password of the Access Manager administrator.</li> <li>♦ IP address of the Administration Console.</li> </ul>
For more information	See “ <a href="#">Installing the SSL VPN Server</a> ” in the <a href="#">Novell Access Manager 3.1 SP2 Installation Guide</a> .

---

You can install the SSL VPN server either as a traditional SSL VPN server (which communicates with the Access Gateway for authentication credentials) or as an ESP enabled server (which communicates with the Identity Server for authentication credentials). You can install the SSL VPN server on a separate machine, with the Identity Server, with the Administration Console, or with the Access Gateway Appliance.

- ♦ To install the SSL VPN on a separate machine, continue with this section.
- ♦ To install the SSL VPN with the Identity server, see [Section 1.3, “Identity Server,” on page 10](#).

- ♦ To install the SSL VPN with the Administration Console, see [Section 1.2, “Administration Console,” on page 10](#).
- ♦ To install the SSL VPN with the Access Gateway Appliance, see [Section 1.4, “Access Gateway Appliance,” on page 11](#)

To install SSL VPN on a separate machine:

- 1 Download the `tar.gz` file, extract it, and use `install.sh` to start the installation.  
For software download instructions, see the “[Novell Access Manager Readme](http://www.novell.com/documentation/novellaccessmanager31/accessmanager_readme/data/accessmanager_readme.html)” ([http://www.novell.com/documentation/novellaccessmanager31/accessmanager\\_readme/data/accessmanager\\_readme.html](http://www.novell.com/documentation/novellaccessmanager31/accessmanager_readme/data/accessmanager_readme.html)).
- 2 Do one of the following:
  - ♦ Type 3 to install the ESP-Enabled SSL VPN.
  - ♦ Type 4 to install the traditional SSL VPN.
- 3 Press Enter, then follow the prompts.

## 1.7 Verifying the Installation

To verify the installation of the components:

- 1 Open a browser and enable browser pop-ups.
- 2 Log in to the Administration Console. The URL is the IP address of the Administration Console followed by `:8080/nps` for the port and the application. For example:  
`http://10.10.15.10:8080/nps`  
If you get an error message, restart Tomcat on the Administration Console:  
**Linux:** Enter the following command:  
`/etc/init.d/novell-tomcat5 restart`  
**Windows:** Enter the following commands:  
`net stop Tomcat5`  
`net start Tomcat5`  
If you still receive an error, see “[Unable to Log In to the Administration Console](#)” in the *Novell Access Manager 3.1 SP2 Administration Console Guide*.
- 3 Click *Access Manager > Overview*.  
Each icon should contain the number one, if your component successfully imported into the Administration Console.  
If a component has not imported, click the link to the device. If a repair import option is available, click this link. If it is not available, see “[Troubleshooting Installation and Upgrade](#)” in the *Novell Access Manager 3.1 SP2 Installation Guide*.
- 4 Before continuing with configuration, verify the following:
  - ♦ Use the `ping` command to verify that the DNS names for the Identity Server and the Access Gateway are resolvable.
  - ♦ Make sure time is synchronized among your components.

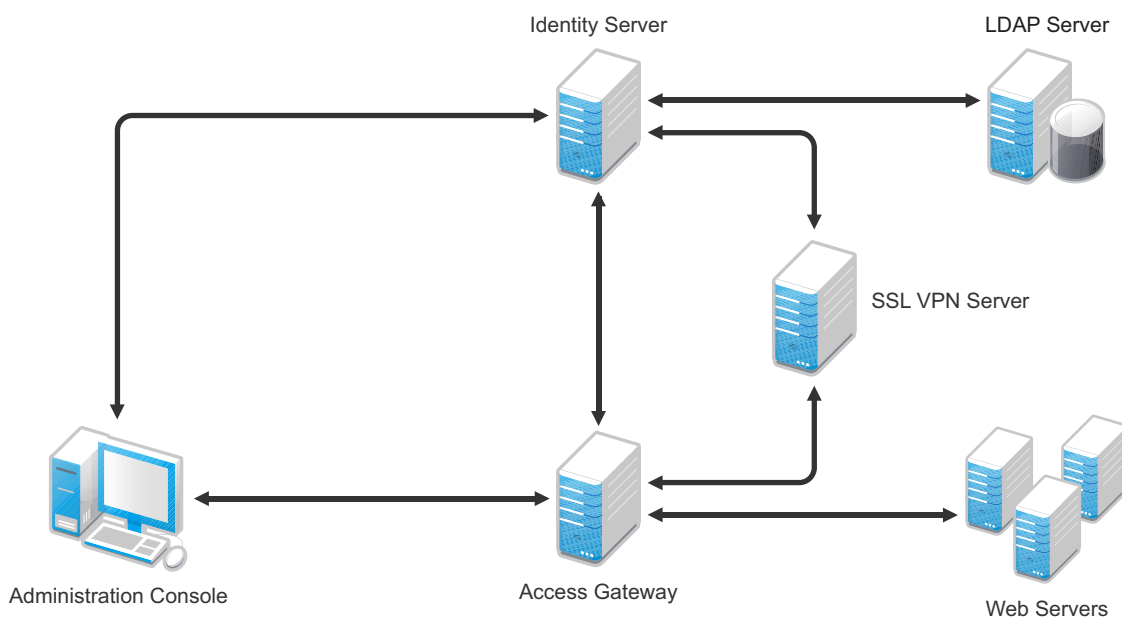


## 2

# Configuration Quick Start

A basic configuration 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. [Figure 2-1](#) illustrates a configuration where these components are installed on separate machines.

**Figure 2-1** Modules Required for a Basic Configuration



This section explains how to configure your system so that users in your LDAP server can log in and access a protected resource on a Web server and also access an SSL VPN application.

- ♦ [Section 2.1, “New Identity Server Cluster Configuration,” on page 15](#)
- ♦ [Section 2.2, “First Reverse Proxy Configuration,” on page 18](#)
- ♦ [Section 2.3, “Configuring the Protected Resource for Authentication,” on page 19](#)
- ♦ [Section 2.4, “Basic Configuration for SSL VPN,” on page 20](#)

## 2.1 New Identity Server Cluster Configuration

This section explains how to add your Identity Server to a cluster and how to configure the cluster to communicate with the LDAP server and use its authentication credentials.

**Table 2-1** Identity Server Configuration Information

What you need to know	Example	Your Value
LDAP server information:		
DN of the administrator	cn=admin,o=novell	_____
Password of the administrator	novell	_____
IP address of the LDAP server	10.10.10.16	_____
DN of the user container	ou=users,o=novell	_____
DNS name of the Identity Server	idpa.test.novell.com	_____
Names you need to create:		
Identity Server cluster name	idpa	_____
User store name	User Store	_____
Replica name	User Store Replica	_____
Alias certificate name	UserStoreRoot	_____
Organization information for the Identity Server cluster:		
Name	Access Manager	_____
Display name	Access Manager 3	_____
URL	idpa.am.novell.com	_____
For more information, see “ <a href="#">Creating a Basic Identity Server Configuration</a> ” in the <a href="#">Novell Access Manager 3.1 SP2 Setup Guide</a> .		

- 1 In the Administration Console, click *Devices > Identity Servers*.
- 2 Click *New Cluster*.
- 3 Specify a name such as `idpa`, select your Identity Server, then click *OK*.  
In [Table 2-1](#), `idpa` is the Identity Server cluster name you created.
- 4 Configure the Base URL of the Identity Server, using the DNS name of the Identity Server:  
`http://idpa.test.novell.com:8080/nidp`  
In [Table 2-1](#), this is the DNS name of the Identity Server with a port and `/nidp`.
- 5 Click *Next*, then configure the organization information.  
**Name:** Access Manager  
**Display name:** Access Manager 3  
**URL:** idpa.am.novell.com  
In [Table 2-1](#), these three fields are the organization information you created for the Identity Server cluster.
- 6 Click *Next*, then configure the user store:



**Name:** User Store

In [Table 2-1](#), User Store is the sample name for the user store.

**Admin name:** cn=admin,o=novell

In [Table 2-1](#), this is the sample DN of the administrator for the LDAP server.

**Admin password:** novell

**Confirm password:** novell

In [Table 2-1](#), these fields are the sample password for the administrator of the LDAP server.

**Directory Type:** Select a type from the drop-down menu.

- 7 In the *Server replicas* section, click *New*, then fill in the following fields:

**Name:** User Store Replica

In [Table 2-1](#), User Store Replica is the sample name for the replica

**IP Address:** 10.10.10.16

In [Table 2-1](#), this is the sample IP address of the LDAP server.

**Use secure LDAP connections:** Select this option.

**Auto import trusted root:** Click this link, follow the prompts, and specify `UserStoreRoot` for the alias.

In [Table 2-1](#), `UserStoreRoot` is the sample alias certificate name.

- 8 Click *OK*, then make sure the Validation Status of the replica displays a green check mark. If the check mark is red, you have a configuration error:
  - ♦ Check the distinguished name of the admin user, the password, and the IP address of the replica.
  - ♦ Check for network communication problems between the Identity Server and the LDAP server.

- 9 In the *Search Contexts* section, click *New*, then specify the following:

**Search context:** ou=users,o=novell

In [Table 2-1](#), this is the sample DN of the user container.

**Scope:** Subtree

- 10 Click *OK > Finish*, then restart Tomcat as prompted.
- 11 Wait for the health status of the Identity Server to turn green, then verify the configuration:
  - 11a Enter the Base URL of the Identity Server in a browser.  
`http://idpa.test.novell.com:8080/nidp`
  - 11b Log in using the credentials of a user in the LDAP server.

The user portal appears.

If the URL returns an error rather than displaying a login page, verify the following:

- ♦ The browser machine can resolve the DNS name of the Identity Server.
- ♦ The browser machine can access to the port.

## 2.2 First Reverse Proxy Configuration

This section explains how to create a reverse proxy to protect the name and IP address of your Web server from being exposed to users. [Section 2.3, “Configuring the Protected Resource for Authentication,” on page 19](#) builds on this configuration and explains how to require authentication to gain access to the Web server.

**Table 2-2** Access Gateway Configuration Information

What You Need To Know	Example	Your Value
Name of the Identity Server cluster	idpa	_____
DNS name of the Access Gateway	lag.test.novell.com	_____
Web server information		
IP address	10.10.16.16	_____
DNS name	digital.test.novell.com	_____
Names you need to create		
Reverse proxy name	DigitalAirlines	_____
Proxy service name	DA	_____
Protected resource name	everything	_____

For more information, see “[Configuring the Access Gateway](#)” in the *Novell Access Manager 3.1 SP2 Setup Guide*.

- 1 In the Administration Console, click *Devices > Access Gateways*.
- 2 Click *Edit*, then click *Reverse Proxy/Authentication*.
- 3 Configure a reverse proxy:
  - ♦ In the *Authentication Settings* section, select `idpa` from the drop-down list.  
In [Table 2-2](#), this is the sample name of the Identity Server cluster.
  - ♦ In the *Reverse Proxy* section, click *New*, specify `DigitalAirlines`, then click *OK*.  
In [Table 2-2](#), `DigitalAirlines` is the sample reverse proxy name.
- 4 To configure a proxy service, click *New* in the Proxy Service section, then fill in the following fields:
 

**Proxy Service Name:** `DA`  
In [Table 2-2](#), `DA` is the sample proxy service name.

**Published DNS Name:** `lag.test.novell.com`  
In [Table 2-2](#), this is the sample DNS name of the Access Gateway.

**Web Server IP Address:** `10.10.16.16`  
In [Table 2-2](#), this is the sample IP address of the Web server.

**Host Header:** Select the *Web Server Host Name* from the drop-down list.

**Web Server Host Name:** `digital.test.novell.com`

In [Table 2-2](#), this is the sample DNS name of the Web server.

**5** Click *OK*, then configure a protected resource.

- ♦ Click the *Protected Resource* tab.
- ♦ In the *Protected Resource* section, click *New*, then specify *everything*.  
In [Table 2-2](#), *everything* is the sample protected resource name.
- ♦ In the *URL Path* section, examine the path. It should be set to */\** to match everything on the Web server.

**6** Click *OK* to save the configuration.

**7** Click the *Access Gateways* task, then click *Update*.

Wait for the health status to turn green. If it doesn't turn green, click the *Health* icon to discover the cause.

- ♦ If the Access Gateway cannot connect to the Web server, verify the IP address of the Web server.
- ♦ Use the `ping` command to verify that the Access Gateway can communicate with the Web server and the Identity Server.
- ♦ Verify that the Access Gateway can resolve the DNS name of the Identity Server.
- ♦ For other problems, see “[Monitoring the Health of an Access Gateway](#)” in the *Novell Access Manager 3.1 SP2 Access Gateway Guide*.

**8** Click the *Identity Servers* task, then click *Update*.

**9** To test that the Access Gateway is protecting the Web server, open a browser and enter the following URL:

```
http://lag.test.novell.com:80/
```

The first page of the Web server is displayed. If you get an error, verify the following:

- ♦ Check the times on the Access Gateway and the Identity Server. Their times need to be synchronized.
- ♦ Verify that the browser machine can resolve the DNS name of the Access Gateway.

## 2.3 Configuring the Protected Resource for Authentication

This section explains how to configure the Access Gateway so that users are prompted to log in when accessing the protected resource.

**1** To return to the protected resource, click *Devices > Access Gateways > Edit > DigitalAirlines > DA > Protected Resources > everything*.

**2** For the *Contract* option, select *Name/Password Form* from the drop-down list.

If the list is empty, you have not selected an Identity Server cluster configuration for the Access Gateway. See [Step 3 on page 18](#).

**3** Click *OK* to save the configuration.

**4** Click the *Access Gateways* task, then click *Update*.

**5** To test that accessing the resource now requires authentication, open a browser, then enter the URL to your protected resource:

```
http://lag.test.novell.com:80/
```

When you are prompted for login credentials, use a name and a password from a user on the LDAP server.

If you receive an error, verify the following:

- ♦ The Identity Server can resolve the DNS name of the Access Gateway.
- ♦ The Access Gateway can resolve the DNS name of the Identity Server.
- ♦ Time is synchronized between the Identity Server and the Access Gateway.

For other problems, see “[General Authentication Troubleshooting Tips](#)” in the *Novell Access Manager 3.1 SP2 Identity Server Guide*.

## 2.4 Basic Configuration for SSL VPN

This section explains how to create a basic configuration for the SSL VPN server.

- ♦ If you have installed the ESP-enabled SSL VPN, continue with [Section 2.4.1, “Configuring Authentication for ESP-Enabled SSL VPN,”](#) on page 20.
- ♦ If you have installed the traditional SSL VPN, continue with [Section 2.4.2, “Accelerating the Traditional SSL VPN Server,”](#) on page 21.

### 2.4.1 Configuring Authentication for ESP-Enabled SSL VPN

This section explains how to establish a trust relationship between the Identity Server and the Embedded Service Provider of the SSL VPN server.

**Table 2-3** *ESP-Enabled SSL VPN Configuration Information*

What You Need To Know	Example	Your Value
Name of the Identity Server cluster	idpa	_____
DNS name of the SSL VPN machine	sslvpn.test.novell.com	_____
A certificate where the subject name matches the DNS name of the SSL VPN machine	For information on how to create such a certificate, see “ <a href="#">Creating a Locally Signed Certificate</a> ” in the <i>Novell Access Manager 3.1 SP2 Administration Console Guide</i> .	

For more information, see “[Configuring Authentication for the ESP-Enabled Novell SSL VPN](#)” in the *Novell Access Manager 3.1 SP2 Setup Guide*.

- 1 In the Administration Console, click *Devices > SSL VPNs > Edit*.
- 2 Select *Authentication Configuration* from the *Gateway Configuration* section.
- 3 Fill in the following fields:

**Identity Server Cluster:** idpa

In [Table 2-3](#), this is the sample name of the Identity Server cluster.

**Authentication Contract:** Select *Any Contract*.

**Embedded Service Provider Base URL:** https:sslvpn.test:8443/sslvpn

In [Table 2-3](#), this is the DNS name for the SSL VPN server. It assumes you want to use HTTPS. If you want to use HTTP, select http and make sure the port is 8080.

**Redirect Requests from Non-Secure Port to Secure Port:** Select this option if you are using HTTPS.

**SSL VPN Certificate:** Click the icon and select the certificate that has a subject name that matches the DNS name of the SSL VPN server.

**Embedded Service Provider Certificate:** Click the icon and select the certificate that has a subject name that matches the DNS name of the SSL VPN server.

- 4 Restart the Tomcat server when prompted.
- 5 Click *OK*, then click *Update* on the Configuration page.
- 6 Click *Update* on the Identity Server Configuration page.

## 2.4.2 Accelerating the Traditional SSL VPN Server

This section explains how to accelerate the traditional SSL VPN server in a path-based multi-homing configuration.

- 1 In the Administration Console, click *Devices > Access Gateways*, then click *Edit > [Name of Reverse Proxy]*.
- 2 In the *Proxy Service List*, click *New*, then provide the following values:
 

**Proxy Service Name:** Specify *sslvpn*.

**Multi-Homing Type:** Select *Path-Based*.

**Path:** Specify */sslvpn*.

**Web Server IP Address:** Specify the IP address of SSL VPN server.

**Host Header:** If your SSL VPN server has a DNS name, select *Web Server Host Name*. Otherwise, select *Forward Received Host Name*.

**Web Server Host Name:** Specify the DNS name of the SSL VPN server if you selected *Web Server Host Name* for the *Host Header* option.
- 3 Click *OK*.
- 4 In the *Proxy Service List*, click *sslvpn > Web Servers*.
- 5 Change the *Connect Port* from 80 to 8080, then click *OK*.
- 6 In the *Proxy Service List*, select the *sslvpn*.
- 7 In the *Path List*, select the *sslvpn* path, then click *Enable SSL VPN*.
- 8 Fill in the following fields:
 

**Policy Container:** Select *Master\_Container*.

**Policy:** Select *Create SSL VPN Default Policy*. In the Policy List window, click *Apply Changes*, then click *Close*.

**Name:** Select *Create SSL VPN Default Protected Resource*.
- 9 Click *OK* twice, then update the Access Gateway and the SSL VPN server.

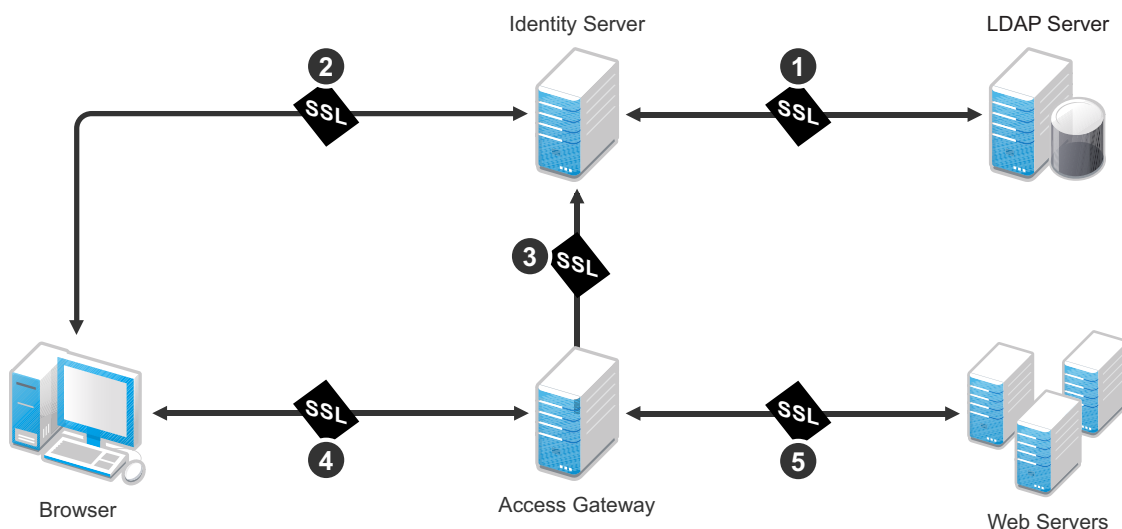


## 3

# SSL Configuration Quick Start

Access Manager has five communication channels that can be configured for SSL. [Figure 3-1](#) illustrates these channels.

**Figure 3-1** Potential SSL Communication Channels



The channels need to be configured according to their numeric values. You need to configure SSL between the Identity Server and the LDAP server before you configure SSL between the Identity Server and the browsers. The Identity Server must be configured for SSL before you configure the channel between the Access Gateway and the Identity Server for SSL.

The following procedures assume that you want to set up a new system using certificates created by the Access Manager Certificate Authority. To modify an existing system to use SSL, see [“Enabling SSL Communication”](#) in the *Novell Access Manager 3.1 SP2 Setup Guide*. To use certificates signed by an external CA, see [“Using Externally Signed Certificates”](#) in the *Novell Access Manager 3.1 SP2 Setup Guide*.

This section describes the following tasks:

- ♦ [Section 3.1, “Configuring a New Identity Server Cluster with SSL,” on page 23](#)
- ♦ [Section 3.2, “Configuring a New Access Gateway for SSL,” on page 26](#)

## 3.1 Configuring a New Identity Server Cluster with SSL

This section explains how to add your Identity Server to a cluster, how to configure the cluster to use SSL, and how to configure the cluster to communicate with the LDAP server so users can access their authentication credentials.

What You Need to Know	Example	Your Value
LDAP server information:		
DN of the administrator	cn=admin,o=novell	_____
Password of the administrator	novell	_____
IP address of the LDAP server	10.10.10.16	_____
DN of the user container	ou=users,o=novell	_____
DNS name of the Identity Server	idpa.test.novell.com	_____
Certificate name	idpa_test	_____
Certificate subject fields:		
Common name	idpa.test.novell.com	_____
Organizational unit	o=novell	_____
Organization	test	_____
City or town	Provo	_____
State or province	Utah	_____
Country	US	_____
Names you need to create:		
Identity Server cluster name	idpa	_____
User store name	User Store	_____
Replica name	User Store Replica	_____
Alias certificate name	UserStoreRoot	_____
Organization information for the Identity Server cluster:		
Name	Access Manager	_____
Display name	Access Manager 3	_____
URL	idpa.am.novell.com	_____
For more information, see “ <a href="#">Creating a Basic Identity Server Configuration</a> ” in the <a href="#">Novell Access Manager 3.1 SP2 Setup Guide</a> .		

- 1 In the Administration Console, click *Devices > Identity Servers*.
- 2 Click *New Cluster*.
- 3 Specify a name such as *idpa*, select your Identity Server, then click *OK*.
- 4 Configure the Base URL of the Identity Server, using the DNS name of the Identity Server:  
https://idpa.test.novell.com:8443/nidp
- 5 On the *SSL Certificate* line, click the *Select Certificate* icon, then click *Replace*.
- 6 In the *Replace* box, click the *Select Certificate* icon.



- 7 On the Certificates page, click *New*.
- 8 Select *Use local certificate authority*.
- 9 Fill in the following fields:
  - Certificate name:** `idpa_test`
  - Signature algorithm:** Accept the default.
  - Valid from:** Accept the default.
  - Months valid:** Accept the default.
  - Key size:** Accept the default.
- 10 Click the *Edit* icon on the *Subject* line.
- 11 Fill in the following fields:
  - Common name:** `idpa.test.novell.com`
  - Organizational unit:** `o=novell`
  - Organization:** `test`
  - City or town:** `Provo`
  - State or province:** `Utah`
  - Country:** `US`
- 12 Click *OK* twice.
- 13 Verify that the new certificate is selected, then click *OK*.
- 14 In the *Replace* box, click *OK*, then click *Close*.
- 15 To configure the organization information, click *Next*, then fill in the following fields:
  - Name:** `Access Manager`
  - Display name:** `Access Manager 3`
  - URL:** `idpa.am.novell.com`
- 16 Click *Next*, then configure the user store:
  - Name:** `User Store`
  - Admin name:** `cn=admin,o=novell`
  - Admin password:** `novell`
  - Confirm password:** `novell`
  - Directory Type:** Select a type from the drop-down menu.
- 17 In the *Server replicas* section, click *New*, then fill in the following fields:
  - Name:** `User Store Replica`
  - IP Address:** `10.10.10.16`
  - Use secure LDAP connections:** Select this option.
  - Auto import trusted root:** Click this link, follow the prompts, and specify `UserStoreRoot` for the alias.

- 18 Click *OK*, then make sure the Validation Status of the replica displays a green check mark. If the check mark is red, you have a configuration error:
- ♦ Check the distinguished name of the admin user, the password, and the IP address of the replica.
  - ♦ Check for network communication problems between the Identity Server and the LDAP server.
- 19 In the *Search Contexts* section, click *New*, then specify the following:
- Search context:** `ou=users,o=novell`
- Scope:** `Subtree`
- 20 Click *OK*, click *Finish*, then restart Tomcat as prompted.
- 21 Wait for the health status of the Identity Server to turn green, then verify the configuration:
- 21a** Enter the Base URL of the Identity Server in a browser.
- `https://idpa.test.novell.com:8443/nidp`
- 21b** Log in using the credentials of a user in the LDAP server.
- The user portal appears.
- If the URL returns an error rather than displaying a login page, verify the following:
- ♦ The browser machine can resolve the DNS name of the Identity Server.
  - ♦ The browser machine can access port 8443.

## 3.2 Configuring a New Access Gateway for SSL

This section explains how to create a reverse proxy to protect the name and IP address of your Web server from being exposed to users, how to require SSL between the browsers and the reverse proxy, and how to require authentication to gain access to the Web server.

What You Need to Know	Example	Your Value
Name of the Identity Server cluster	<code>idpa</code>	<input type="text"/>
DNS name of the Access Gateway	<code>lag.test.novell.com</code>	<input type="text"/>
Web server information		
IP address	<code>10.10.16.16</code>	<input type="text"/>
DNS name	<code>digital.test.novell.com</code>	<input type="text"/>
Names you need to create		
Reverse proxy name	<code>DigitalAirlines</code>	<input type="text"/>
Proxy service name	<code>DA</code>	<input type="text"/>
Protected resource name	<code>everything</code>	<input type="text"/>

For more information, see “[Configuring the Access Gateway](#)” in the [Novell Access Manager 3.1 SP2 Setup Guide](#).

- 1 In the Administration Console, click the *Access Gateways* task.
- 2 Click *Edit*, then click *Reverse Proxy/Authentication*.

**3** Configure a reverse proxy:

- ♦ In the *Authentication Settings* section, select *idpa* from the drop-down list.
- ♦ In the *Reverse Proxy* section, click *New*, specify *DigitalAirlines*, then click *OK*.

**4** To configure a proxy service, click *New* in the *Proxy Service* section, then fill in the following fields:

**Proxy Service Name:** DA

**Published DNS Name:** lag.test.novell.com

**Web Server IP Address:** 10.10.16.16

**Host Header:** Select the *Web Server Host Name* from the drop-down list.

**Web Server Host Name:** digital.test.novell.com

**5** On the Reverse Proxy page, configure a protected resource.

**5a** In the *Proxy Service List* section, click the name of proxy service (DA), then click the *Protected Resources* tab.

**5b** In the *Protected Resource List* section, click *New*, specify *everything*, then click *OK*.

**5c** For the contract, select *Secure Name/Password - Form*.

**5d** In the *URL Path* section, examine the path. It should be set to */\** to match everything on the Web server.

**5e** Click *OK* twice.

**6** On the Reverse Proxy page, enable SSL:

**6a** Select *Enable SSL with Embedded Service Provider*.

**6b** Select *Enable SSL between Browser and Access Gateway*.

**6c** Select *Redirect Requests from Non-Secure Port to Secure Port*.

**6d** Select *Auto-generate Key*, then click *OK*.

**6e** Ensure that the certificate is selected, then click *OK*.

**7** Click *OK* until you return to the Access Gateway page.

**8** On the Access Gateways page, click *Update*.

Wait for the health status to turn green. If it doesn't turn green, click the *Health* icon to discover the cause.

- ♦ If the Access Gateway cannot connect to the Web server, verify the IP address of the Web server.
- ♦ Use the `ping` command to verify that the Access Gateway can communicate with the Web server and the Identity Server.
- ♦ Verify that the Access Gateway can resolve the DNS name of the Identity Server.
- ♦ For other problems, see “[General Authentication Troubleshooting Tips](#)” in the *Novell Access Manager 3.1 SP2 Identity Server Guide*.

**9** Click the *Identity Servers* task, then click *Update*.

**10** To test that the Access Gateway is protecting the Web server, open a browser and enter the following URL:

`https://lag.test.novell.com:443/`

The first page of the Web server is displayed. If you get an error, verify the following:

- ♦ Check the times on the Access Gateway and the Identity Server. Their times need to be synchronized.
- ♦ Verify that the browser machine can resolve the DNS name of the Access Gateway.