Novell Access Manager

3.0 SP3

www.novell.com

QUICK STARTS

April 18, 2008

Novell®

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/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
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).

Novell Trademarks

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

Third-Party Materials

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

Contents

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 13

For an explanation of the options, please see the following manuals:

- *Novell Access Manager 3.0 SP3 Installation Guide*
- *Novell Access Manager 3.0 SP3 Setup Guide*

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 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/novellaccessmanager).

Additional Documentation

- *Novell Access Manager 3.0 SP3 Installation Guide*
- *Novell Access Manager 3.0 SP3 Setup Guide*
- *Novell Access Manager 3.0 SP3 Administration Guide*
- *Novell Access Manager 3.0 SP3 J2EE Agent Guide*

Documentation Conventions

In Novell® documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

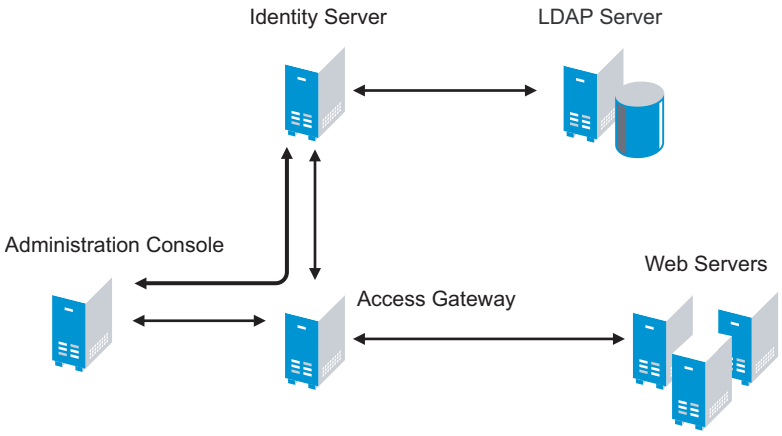
When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux* or UNIX*, should use forward slashes as required by your software.

Installation Quick Start

1

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 configuration where these components are installed on separate machines.

Figure 1-1 *Basic Installation*



The Administration Console and the Identity Server can be installed together on the same machine.

The Administration Console must be installed first. The other components can then be installed in any order.

IMPORTANT: Please provide feedback on this document by using the *Add Comment* link at the bottom of each page. We need to know whether it provides the right amount of information (too much? too little?) to get the components installed.

1.1 System Requirements

Review the following sections in the *Novell Access Manager 3.0 SP3 Installation Guide* to ensure that your machines or virtual images meet the installation prerequisites:

- “Administration Console Requirements”
- “Identity Server Requirements”
- “Access Gateway Requirements”

1.2 Administration Console

What you need to know	◆ The username and password you want to use for the Access Manager administrator. ◆ This is your first installation of an Administration Console, so when prompted, answer Yes for a primary installation. You can create a failover environment by installing more than one Administration Console. For more information, see "Clustering and Fault Tolerance" in the *Novell Access Manager 3.0 SP3 Setup Guide*.
For more information	See "Installing the Access Manager Administration Console" in the *Novell Access Manager 3.0 SP3 Installation Guide*.

1. Use `install.sh` to start the installation.
2. At the Installation menu, select 1, then follow the prompts.
3. Answer yes to the primary installation prompt.

1.3 Identity Server

What you need to know	◆ Username and password of the Access Manager administrator. ◆ (Conditional) IP address of the Administration Console if it is installed on a separate machine
For more information	See "Installing the Novell Identity Server" in the *Novell Access Manager 3.0 SP3 Installation Guide*.

1. Use `install.sh` to start the installation.
2. At the Installation menu, select 2, then follow the prompts.

1.4 Linux Access Gateway

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.
Security follow-up	Change the password of the `config` and `root` users on the Linux Access Gateway machine.
For more information	See "Installing the Linux Access Gateway" in the *Novell Access Manager 3.0 SP3 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 network information. For the IP address, specify the IP address you have selected for the Access Gateway.

7 Click *Next*, then specify the hostname and domain name for the Access Gateway and the IP address of at least one DNS server.

8 Click *Next*, then specify the Administration Console information.

Do not select to install other components at this time.

9 Click *Next* and review the summary installation page.

10 If everything looks correct, select to install.

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

11 Log in as `root` with a password of `novell`.

12 Change the password of the `root` user and the `config` user.

1.5 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, use the following command to restart Tomcat:

```
/etc/init.d/novell-tomcat4 start
```

If you still receive an error, see "Unable to Log In to the Administration Console" in the *Novell Access Manager 3.0 SP3 Administration 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" in the *Novell Access Manager 3.0 SP3 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.

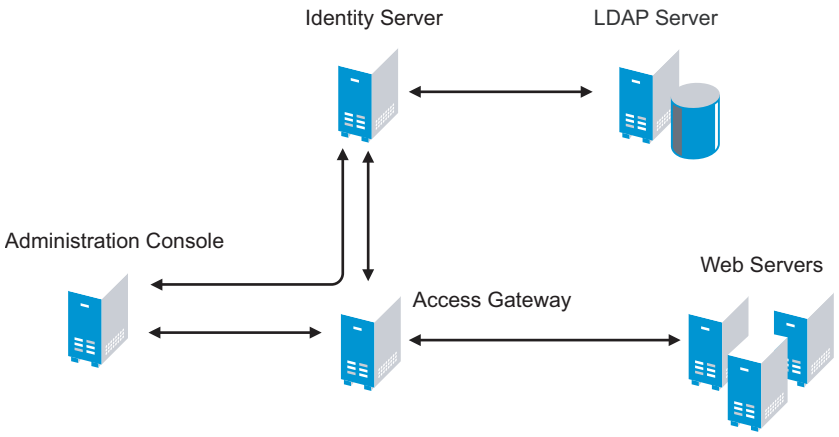
IMPORTANT: Please provide feedback on this document by using the *Add Comment* link at the bottom of each page. We need to know whether it provides the right amount of information (too much? too little?) to get the components installed.

Configuration Quick Start

2

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, although the Administration Console and the Identity Server can be installed together on the same machine.

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



This section explains how to configure your system so that user in your LDAP server can log in and access a protected resource on a Web server.

- Section 2.1, "New Identity Server Cluster Configuration," on page 13
- Section 2.2, "First Reverse Proxy Configuration," on page 15
- Section 2.3, "Configuring the Protected Resource for Authentication," on page 17

IMPORTANT: Please provide feedback on this document by using the *Add Comment* link at the bottom of each page. We need to know whether it provides the right amount of information (too much? too little?) to get the components configured.

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.

What you need to know	◆ The LDAP server information: The DN of the administrator, such as `cn=admin,o=novell` Administrator's password, such as `novell` The IP address of the LDAP server, such as `10.10.10.16` The DN of the user container, such as `o=novell` ◆ The DNS name of the Identity Server, such as `ipda.test.novell.com` ◆ Names you need to create: Identity Server cluster name, such as `idpa` User store name, such as `User Store` Replica name, such as `User Store Replica` Alias certificate name, such as `UserStoreRoot` ◆ Organization information for the Identity Server cluster: Name, such as `Access Manager` Display name, such as `Access Manager 3` URL, such as `ipda.am3sp3.com`
For more information	See "Creating a Basic Identity Server Configuration" in the *Novell Access Manager 3.0 SP3 Setup Guide*.

1. In the Administration Console, click the *Identity Servers* task.
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: `http://idpa.test.novell.com:8080/nidp`
5. Click *Next*, then configure the organization information.

   Name: `Access Manager`

   Display name: `Access Manager 3`

   URL: `ipda.am3sp3.com`
6. 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.
7. 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.

8 Click *OK*, then make sure the Validation Status of the replica displays a green check mark. If it 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: `o=novell`

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.

IMPORTANT: Please provide feedback on this document by using the *Add Comment* link at the bottom of each page. We need to know whether it provides the right amount of information (too much? too little?) to get the Identity Server configured.

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 17 builds on this configuration and explains how to require authentication to gain access to the Web server.

What you need to know	◆ Name of the Identity Server cluster, such as `idpa` ◆ DNS name of the Access Gateway, such as `lag.test.novell.com` ◆ Web server information IP address, such as `10.10.16.16` DNS name, such as `digital.test.novell.com` ◆ Names you need to create: Reverse proxy name, such as `DigitalAirlines` Proxy service name, such as `DA` Protected resource name, such as `everything`
For more information	See "Configuring the Access Gateway" in the *Novell Access Manager 3.0 SP3 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 Click *OK*, then configure a protected resource.

- Click the *Protected Resource* tab.
- In the *Protected Resource* section, click *New*, then specify `everything`.
- In the *URL Path* section, examine the path. It should be set to /* which matches 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 3.0 SP3 Administration 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.nowll.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.

IMPORTANT: Please provide feedback on this document by using the *Add Comment* link at the bottom of each page. We need to know whether it provides the right amount of information (too much? too little?) to get the Access Gateway configured.

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 *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 16.

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.nowll.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 3.0 SP3 Administration Guide*.

IMPORTANT: Please provide feedback on this document by using the *Add Comment* link at the bottom of each page. We need to know whether it provides the right amount of information (too much? too little?) to get the authentication configured.
