AUTHORIZED DOCUMENTATION

Quick Starts

Novell® Access Manager

3.1 SP1

November 20, 2009

www.novell.com

Legal Notices

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

Third-Party Materials

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 3.1 SP1 Installation Guide*
- *Novell Access Manager 3.1 SP1 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 3.1 SP1 Installation Guide*
- *Novell Access Manager 3.1 SP1 Setup Guide*
- *Novell Access Manager 3.1 SP1 Administration Console Guide*
- *Novell Access Manager 3.1 SP1 Policy Management Guide*
- *Novell Access Manager 3.1 SP1 Identity Server Guide*
- *Novell Access Manager 3.1 SP1 Access Gateway Guide*
- *Novell Access Manager 3.1 SP1 SSL VPN Server Guide*
- *Novell Access Manager 3.1 SP1 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.

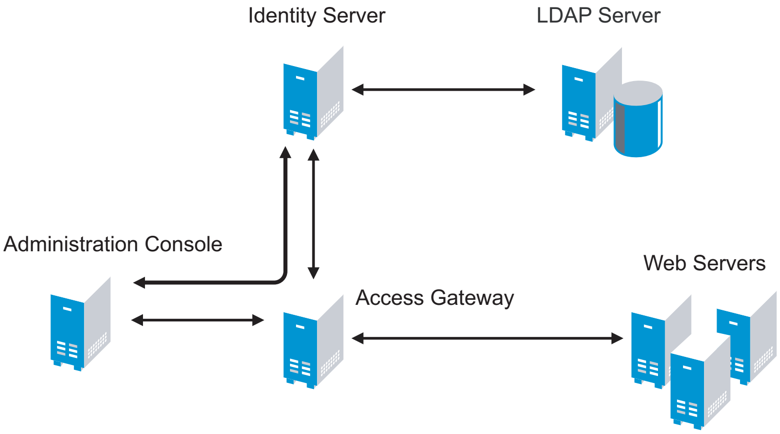
When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux* or UNIX*, should use forward slashes as required by your software.

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

- 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, "Linux Access Gateway," on page 11
- Section 1.5, "Verifying the Installation," on page 11

1.1 System Requirements

Review the following sections in the *Novell Access Manager 3.1 SP1 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 3.1 SP1 Setup Guide*.
For more information	See "Installing the Access Manager Administration Console" in the *Novell Access Manager 3.1 SP1 Installation Guide*.

1.2.1 Linux Administration Console

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.

1.2.2 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/readme/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

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 3.1 SP1 Installation Guide*.

1.3.1 Linux Identity Server

1. Use `install.sh` to start the installation.
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/readme/accessmanager_readme.html).

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

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 Appliance" in the *Novell Access Manager 3.1 SP1 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. Specify a password for the root user.
8. Click *Next*, then specify the hostname and domain name for the Access Gateway and the IP address of at least one DNS server.
9. Click *Next*, then specify the Administration Console information.

   Do not select to install other components at this time.
10. Click *Next* and review the summary installation page.
11. 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.

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, 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 SP1 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" in the *Novell Access Manager 3.1 SP1 Installation Guide*.

4. Before continuing with configuration, verify the following:

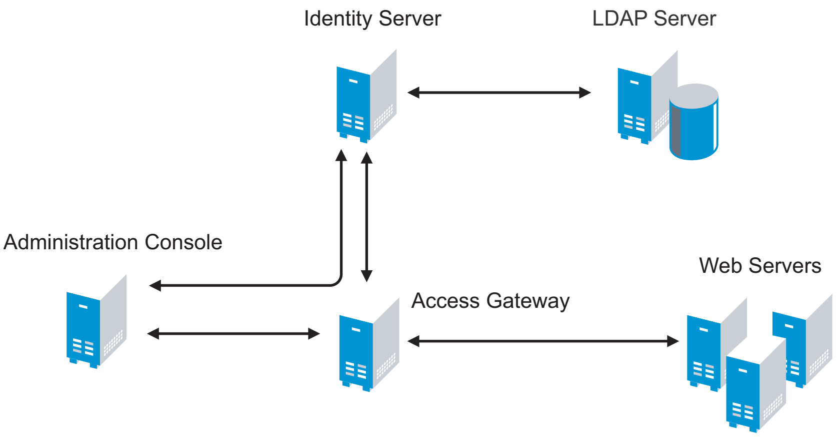
   - Use the `ping` command to verify that the DNS names for the Identity Server and the Access Gateway are resolvable.
   - Make sure time is synchronized among your components.

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.

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 16
- Section 2.3, "Configuring the Protected Resource for Authentication," on page 17

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	o=novell	
DNS name of the Identity Server	ipda.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	ipda.am3sp3.com	
For more information, see "Creating a Basic Identity Server Configuration" in the *Novell Access Manager 3.1 SP1 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*.

   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 `/nipd`.
5. Click *Next*, then configure the organization information.

   Name: `Access Manager`

   Display name: `Access Manager 3`

   URL: `ipda.am3sp3.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 user store name you created.

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

In Table 2-1, this is the DN of the administrator for the LDAP server.

Admin password: `novell`

Confirm password: `novell`

In Table 2-1, these fields are the 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 name you created for the replica

IP Address: `10.10.10.16`

In Table 2-1, this is the 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 alias certificate name you created.

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`

In Table 2-1, this is the 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 17 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 SP1 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 Table 2-2, this is the 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 reverse proxy name you created.
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 proxy service name you created.

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

   In Table 2-2, this is the DNS name of the Access Gateway.

   Web Server IP Address: `10.10.16.16`

   In Table 2-2, this is the 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`

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 protected resource name you created.
   - 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 3.1 SP1 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 *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.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.

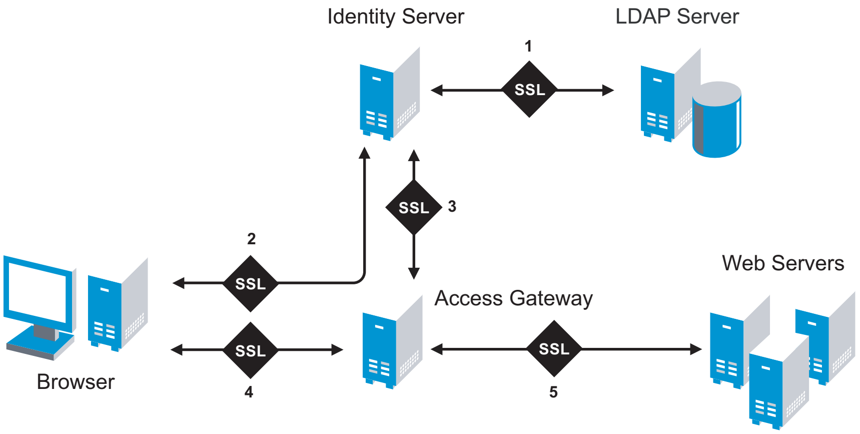
For other problems, see “General Authentication Troubleshooting Tips” in the *Novell Access Manager 3.1 SP1 Identity Server Guide*.

SSL Configuration Quick Start

3

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 SP1 Setup Guide*. To use certificates signed by an external CA, see "Using Externally Signed Certificates" in the *Novell Access Manager 3.1 SP1 Setup Guide*.

This section describes the following tasks:

- Section 3.1, "Configuring a New Identity Server Cluster with SSL," on page 19
- Section 3.2, "Configuring a New Access Gateway for SSL," on page 22

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	o=novell	
DNS name of the Identity Server	ipda.test.novell.com	
Certificate name	ipda_test	
Certificate subject fields:		
Common name	ipda.test.novell.com	
Organizational unit	o=novell	
Organization	test	
City or town	Provo	
State or province	UT	
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	ipda.am3sp3.com	
For more information, see “Creating a Basic Identity Server Configuration” in the *Novell Access Manager 3.1 SP1 Setup Guide*.		

1. In the Administration Console, click *Access Manager* > *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: `UT`

    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: `ipda.am3sp3.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 `UserStoreRoo`t for the alias.

18 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.

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

Search context: `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	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 SP1 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 SP1 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.