Novell Access Manager

3.0 SP3

www.novell.com

SETUP GUIDE

Interim Release 2

June 4, 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.

Copyright © 2006-2008 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., 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 9

1 Setting Up a Basic Access Manager Configuration 11

1.1 Understanding an Access Manager Configuration . . . 11
1.2 Prerequisites for Setup . . . 12
1.3 Creating a Basic Identity Server Configuration . . . 13
1.4 Configuring the Access Gateway . . . 18
1.4.1 Configuring a Reverse Proxy . . . 18
1.4.2 Configuring a Public Protected Resource . . . 20
1.5 Configuring the Access Gateway for Authentication . . . 22
1.5.1 Verifying Time Synchronization . . . 22
1.5.2 Enabling Trusted Authentication . . . 24
1.6 Setting Up an Identity Injection Policy . . . 25

2 Configuring SSL VPN to Protect an Application 29

2.1 Prerequisites . . . 29
2.2 Injecting the SSL VPN Header . . . 29

3 Enabling SSL Communication 33

3.1 Identifying the SSL Communication Channels . . . 33
3.2 Using Access Manager Certificates . . . 34
3.2.1 Configuring Secure Communication on the Identity Server . . . 34
3.2.2 Configuring the Access Gateway for SSL . . . 37
3.3 Using Externally Signed Certificates . . . 42
3.3.1 Obtaining Externally Signed Certificates . . . 42
3.3.2 Configuring the Identity Server to Use an Externally Signed Certificate . . . 44
3.3.3 Configuring the Access Gateway to Use an Externally Signed Certificate . . . 45

4 Clustering and Fault Tolerance 47

4.1 Installing Secondary Versions of the Administration Console . . . 47
4.1.1 Prerequisites . . . 48
4.1.2 Installing a Second Console . . . 49
4.1.3 Tasks Requiring the Primary Console . . . 49
4.2 Clustering Identity Servers . . . 49
4.2.1 Services of the Real Server . . . 50
4.2.2 Prerequisites . . . 50
4.2.3 Setting Up a Cluster . . . 51
4.3 Clustering Access Gateways . . . 53
4.3.1 Prerequisites . . . 54
4.3.2 Configuring a Cluster . . . 55
4.4 Configuration Tips for the L4 Switch . . . 56
4.4.1 Sticky Bit . . . 56
4.4.2 Network Configuration Requirements . . . 56
4.4.3 Health Checks . . . 57
4.4.4 Real Server Settings Example . . . 61
4.4.5 Virtual Server Settings Example . . . 62

5 Setting Up Firewalls 63

5.1 Required Ports . . . 63
5.2 Sample Configurations . . . 71
5.2.1 The Access Gateway and Identity Server in the DMZ . . . 71
5.2.2 A Firewall Separating Access Manager Components from the LDAP Servers . . . 72
5.2.3 Configuring the Firewall for the SSL VPN Server . . . 73
5.2.4 Configuring the Firewall for the J2EE Agent . . . 74

6 Setting Up Federation 77

6.1 Understanding a Simple Federation Scenario . . . 77
6.2 Configuring Federation . . . 78
6.2.1 Prerequisites . . . 80
6.2.2 Establishing Trust between Providers . . . 80
6.2.3 Configuring SAML 1.1 for Account Federation . . . 86
6.3 Sharing Roles . . . 89
6.3.1 Configuring Role Sharing . . . 91
6.3.2 Verifying the Configuration . . . 93
6.4 Setting Up Federation with Third-Party Providers . . . 96

7 Digital Airlines Example 97

7.1 Installation Overview and Prerequisites . . . 97
7.1.1 Installation Architecture . . . 98
7.1.2 Deployment Overview . . . 99
7.2 Setting Up the Web Server . . . 99
7.2.1 Installing the Apache Web Server and PHP Components . . . 100
7.2.2 Installing Digital Airlines Components . . . 101
7.2.3 Configuring Name Resolution . . . 102
7.3 Configuring Public Access to Digital Airlines . . . 102
7.4 Implementing Access Restrictions . . . 107
7.4.1 Enabling an Authentication Procedure . . . 107
7.4.2 Configuring a Role-Based Policy . . . 108
7.4.3 Assigning an Authorization Policy to Protect a Resource . . . 116
7.4.4 Configuring an Identity Injection Policy for Basic Authentication . . . 119
7.4.5 Initiating an SSL VPN Session . . . 125
7.5 Modifying the Digital Airlines Example . . . 131
7.5.1 Prerequisites . . . 132
7.5.2 Understanding the Example Files . . . 132
7.5.3 Updating Static Graphics . . . 132
7.5.4 Updating Mouse-Over Links . . . 135
7.5.5 Deploying Your Updated Example Web Service . . . 135

8 Creating Novell Audit Queries 137

8.1 Setting Up the MySQL Database . . . 137
8.1.1 Prerequisites . . . 137
8.1.2 Preparing MySQL for Novell Audit Connectivity . . . 137
8.1.3 Installing the JDBC Driver . . . 138
8.2 Logging Events to the MySQL Database . . . 138
8.2.1 Creating the MySQL Log Channel . . . 138
8.2.2 Configuring the Audit Server to Log Events to the MySQL Log Channel . . . 140
8.2.3 Configuring Access Manager Components to Log Audit Events . . . 142
8.3 Configuring Queries . . . 143
8.3.1 Enabling Queries to the MySQL Database . . . 144

8.3.2 Configuring the Query Event List and Display 144
8.3.3 Performing a Query 145

9 Protecting an Identity Server with an Access Gateway 147

About This Guide

This guide is intended to help you understand and set up a basic Access Manager 3.0 SP1 configuration.

IMPORTANT: In order to avoid configuration errors, it is strongly recommended that you closely follow the steps outlined in this document during your initial Access Manager setup.

- Chapter 1, “Setting Up a Basic Access Manager Configuration,” on page 11
- Chapter 2, “Configuring SSL VPN to Protect an Application,” on page 29
- Chapter 3, “Enabling SSL Communication,” on page 33
- Chapter 4, “Clustering and Fault Tolerance,” on page 47
- Chapter 5, “Setting Up Firewalls,” on page 63
- Chapter 6, “Setting Up Federation,” on page 77
- Chapter 7, “Digital Airlines Example,” on page 97
- Chapter 8, “Creating Novell Audit Queries,” on page 137
- Chapter 9, “Protecting an Identity Server with an Access Gateway,” on page 147

Not all Access Manager functionality and administrative tasks are discussed here. After you are familiar with Access Manager and the steps in this section, you can use the *Novell Access Manager 3.0 SP3 IR2 Administration Guide* as the source for additional or advance configuration.

Audience

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

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

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 Setup Guide*, visit the Novell Access Manager Documentation Web site (http://www.novell.com/documentation/novellaccessmanager).

Additional Documentation

- *Novell Access Manager 3.0 SP3 IR2 Administration Guide*
- *Novell Access Manager 3.0 SP3 IR2 Installation 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.

Setting Up a Basic Access Manager Configuration

1

The initial setup for Novell® Access Manager consists of installing the components and setting up the Identity Server and the Access Gateway to protect resources running on an HTTP Web server. Access Manager can also be configured to protect other resources such as applications on J2EE* servers and non-HTTP applications. These should be set up after you have created a basic setup. For J2EE server applications, see the *Novell Access Manager 3.0 SP3 J2EE Agent Guide*. For non-HTTP applications, see Chapter 2, "Configuring SSL VPN to Protect an Application," on page 29.

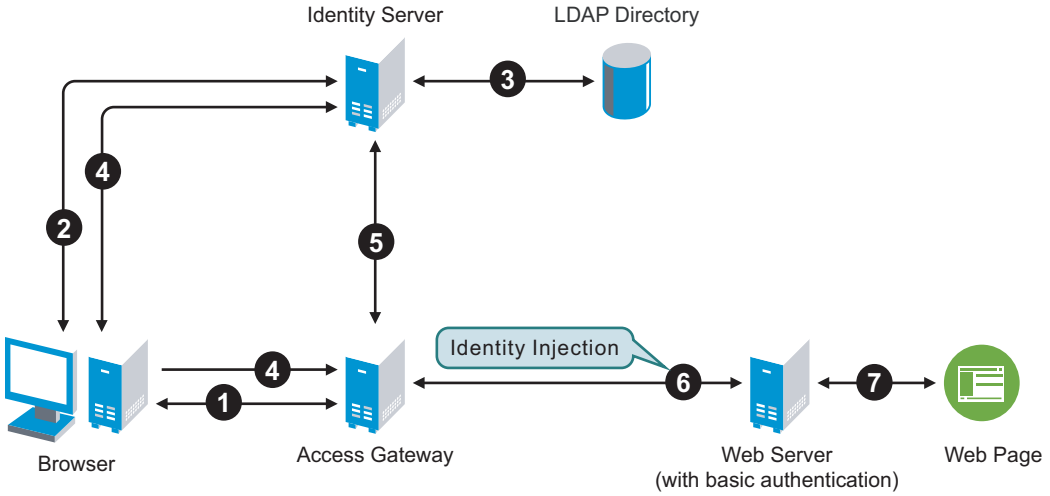
This tutorial describes the following topics and tasks:

- Section 1.1, "Understanding an Access Manager Configuration," on page 11
- Section 1.2, "Prerequisites for Setup," on page 12
- Section 1.3, "Creating a Basic Identity Server Configuration," on page 13
- Section 1.4, "Configuring the Access Gateway," on page 18
- Section 1.5, "Configuring the Access Gateway for Authentication," on page 22
- Section 1.6, "Setting Up an Identity Injection Policy," on page 25

1.1 Understanding an Access Manager Configuration

The following figure illustrates the components and process flow that make up a basic configuration.

Figure 1-1 *Basic Process Flow*

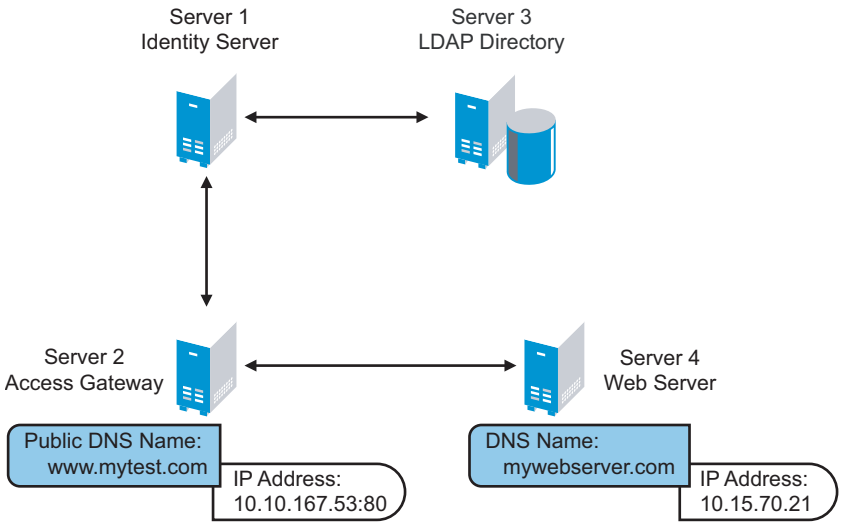


1. The user requests the Access Gateway for access to a protected resource.
2. The Access Gateway redirects the user to the Identity Server, which prompts the user for a username and password.

3. The Identity Server verifies the username and password against an LDAP directory user store (eDirectory™, Active Directory*, or Sun ONE*).
4. The Identity Server returns an authentication artifact to the Access Gateway.
5. The Access Gateway retrieves the user's credentials from the Identity Server.
6. The Access Gateway injects the basic authentication information into the HTTP header.
7. The Web server validates the authentication information and returns the requested Web page.

You configure the Access Manager so that a user can access a resource on a Web server whose name and address are hidden from the user. This basic configuration sets up communication between the following four servers.

Figure 1-2 *Basic Access Manager Configuration*



Although other configurations are possible, this section explains the configuration tasks for this basic Access Manager configuration. This section explains how to set up communication using HTTP. For HTTPS over SSL, see Chapter 3, "Enabling SSL Communication," on page 33.

1.2 Prerequisites for Setup

The following prerequisites are for setting up a basic Access Manager configuration:

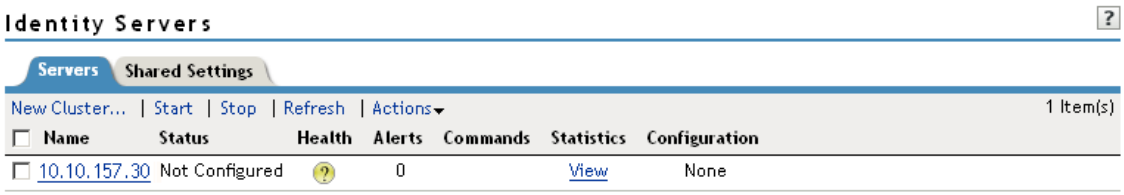
- ❑ An installed Access Manager version of iManager, called the Access Manager Administration Console. See "Installing the Access Manager Administration Console" in the *Novell Access Manager 3.0 SP3 IR2 Installation Guide*.
- ❑ An installed Identity Server. See "Installing the Novell Identity Server" in the *Novell Access Manager 3.0 SP3 IR2 Installation Guide*.
- ❑ An installed Access Gateway (either NetWare® or Linux). See "Installing the Linux Access Gateway" or "Installing the NetWare Access Gateway" in the *Novell Access Manager 3.0 SP3 IR2 Installation Guide*.
- ❑ An LDAP directory store with a test user added. This store can be eDirectory, Active Directory, or Sun ONE.

- ❑ A DNS server or modified `host` files to resolve DNS names and provide reverse lookups. For information on which host files need to be modified, see Section 7.2.3, "Configuring Name Resolution," on page 102.
- ❑ A Web server (IIS or Apache). The Web server should have three directories with three HTML pages. The first directory (`public`) should contain a page (such as index.html) for public access. This page needs to provide two links:
  - A link to a page in the `protected` directory. You will configure the Access Gateway to require authentication before allowing access to this page. You do not need to configure the Web server to protect this page.
  - A link to a page in the `basic` directory. You should already have configured your Web server to require basic authentication before allowing access to this page. See your Web Server documentation for instructions on setting up basic authentication. (This type of access is optional, but explained because it is fairly common.)

  If you do not have a Web server that you can use for this type of access, you might prefer to configure Access Manager for the sample Web pages we provide. See Chapter 7, "Digital Airlines Example," on page 97.
- ❑ A client workstation with a browser.
- ❑ Browser pop-ups enabled for the browser on the client workstation.

1.3 Creating a Basic Identity Server Configuration

After you log in to the Administration Console, click *Access Manager* > *Identity Servers*. The system displays the installed server, as shown in the following example:



At this point the Identity Server is in an unconfigured state and is halted. It remains in this state and cannot function until you create an Identity Server configuration, which defines how an Identity Server or Identity Server cluster operates.

NOTE: Before the Identity Server is configured, *"Complete"* might not display under the Command Status until Tomcat is restarted.

When creating the Identity Server configuration, you specify the following information:

- The DNS name for the Identity Server.
- The IP address of an LDAP directory (user store). The LDAP directory is used to authenticate users. The trusted root certificate of the user store is imported to provide secure communication between the Identity Server and the user store.
- The distinguished name and password of the administrator of the LDAP user store.

NOTE: This task is a basic setup to help you become familiar with Access Manager. It discusses only the required fields for creating a configuration. For information about all of the fields in the interface, see "Creating a Cluster Configuration" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

To create an Identity Server configuration:

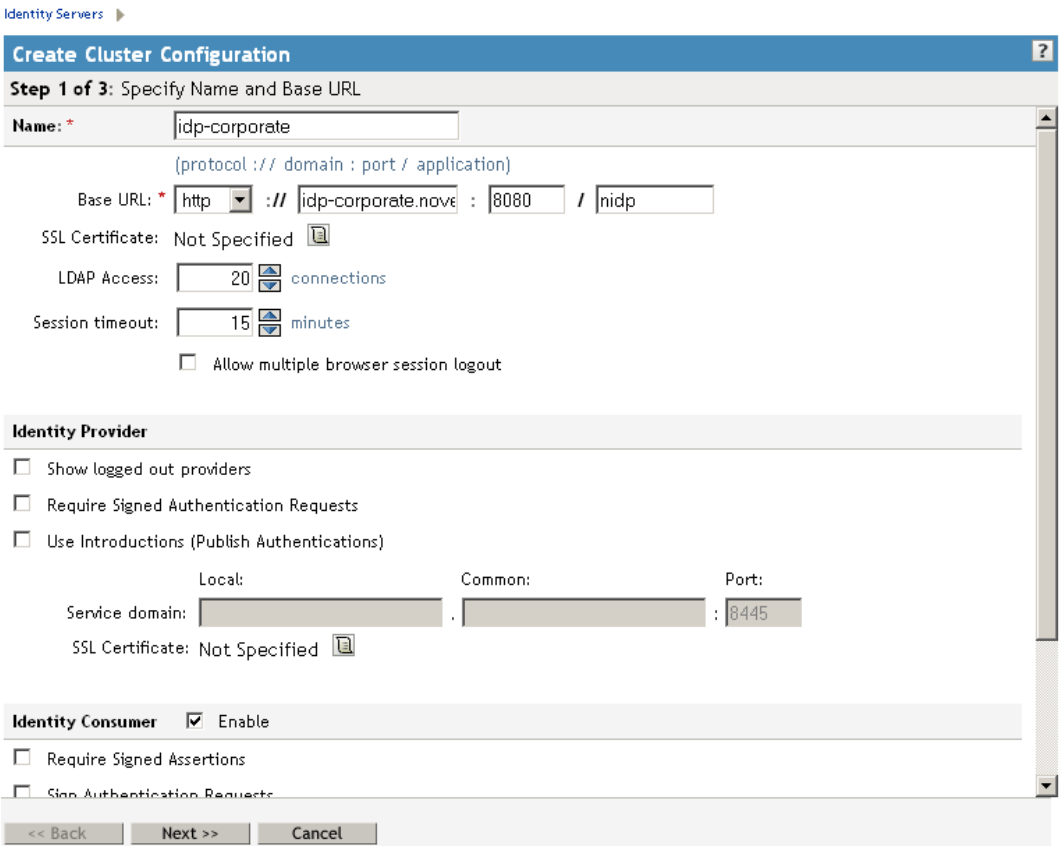
1. On a client workstation, enable browser pop-ups, then log in to the Administration Console.

   For login information, see "Logging In to the Administration Console" in the *Novell Access Manager 3.0 SP3 IR2 Installation Guide*.
2. In the Administration Console, click *Access Manager* > *Identity Servers* > *Servers*.
3. Select the check box by the Identity Server, then click *New Cluster*.

   Selecting the server is one way to assign it to the cluster configuration.
4. In the *New Cluster* dialog box, specify a name for the cluster configuration.

   If you did not select the server in the previous step, you can now select the server or servers that you want to assign to this configuration. For more information about assigning servers to a configuration, see "Assigning an Identity Server to a Cluster Configuration" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.
5. Click *OK*.

   The following example shows a new server configuration called *idp-corporate*:



6. Fill in the following fields to specify the properties for your Identity Server configuration:

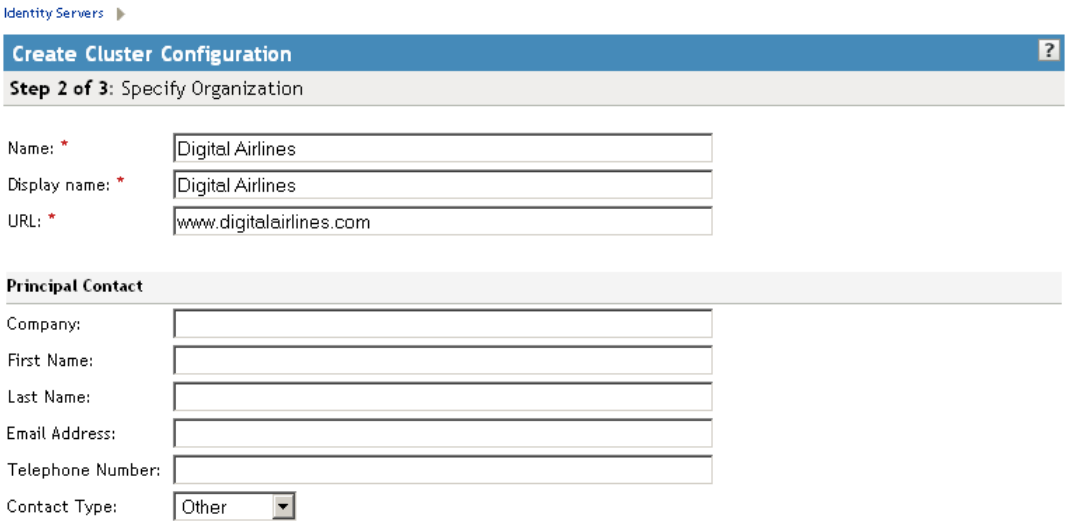
Name: The name by which you want to refer to the Identity Server configuration. This field is populated with the name you provided in the *New Cluster* dialog box. You can change this here, if necessary.

Base URL: The application path for the Identity Server. The Identity Server protocols (Liberty 1.2, SAML 1.1, and SAML 2.0) rely on this base URL to generate URL endpoints for each protocol.

- **Protocol:** The communication protocol. Select HTTP for a basic setup.
- **Domain:** The domain name used to access the Identity Server. For a basic setup, this is the DNS name of the machine on which you installed the Identity Server. Using an IP address is not recommended.
- **Port:** The port values for the protocol. For HTTP, this is 8080.
- **Application:** The Identity Server application path. Leave the default value as *nidp*.

7 Click *Next*.

The system displays the Organization page.



Use this page to specify organization information for the Identity Server configuration. The information you specify on this page is published in the metadata of the Liberty 1.2 and SAML protocols. The metadata is traded with federation partners and supplies various information regarding contact and organization information located at the Identity Server.

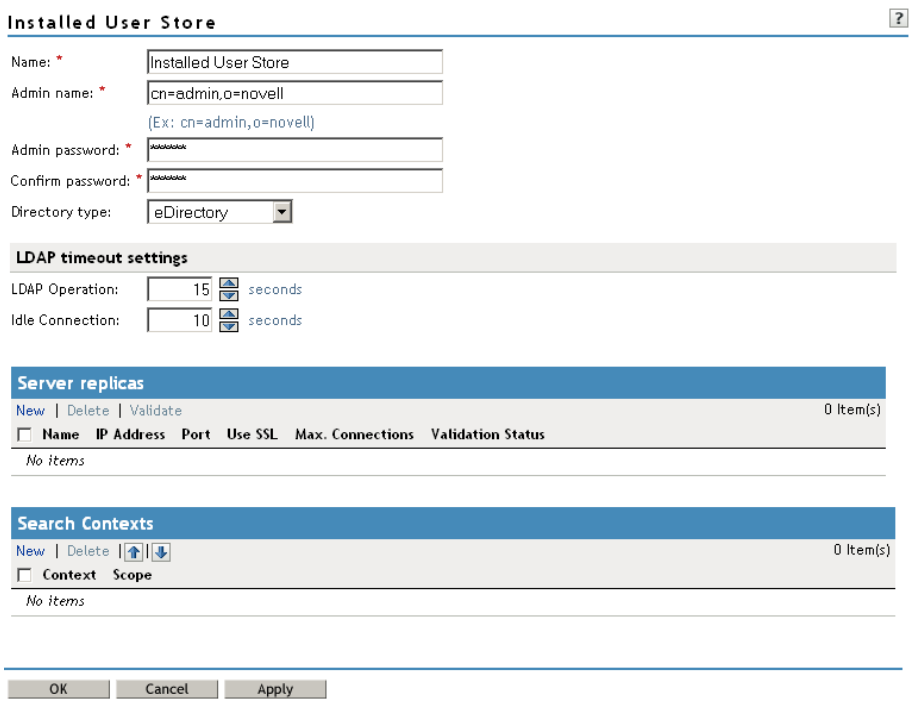
The following fields require information:

- **Name:** The name of the organization.
- **Display Name:** The display name for the organization. This can be the same as the name of the organization.
- **URL:** The organization's URL for contact purposes.

Optional fields include *Company*, *First Name*, *Last Name*, *Email*, *Telephone*, and *Contact Type*.

8 Click *Next*.

The system displays the User Store page.



Use this page to configure the user store that references users in your organization. User stores are LDAP directory servers to which end users authenticate. You can configure a user store to use more than one replica of the directory server, to provide load balancing and failover capability. You must reference an existing user store.

Name: A display name for the LDAP directory.

Admin Name: The distinguished name of the admin user of the LDAP directory. Administrator-level rights are required for setting up a user store.

Admin Password and Confirm Password: The password for the admin user and the confirmation for the password.

Directory Type: The type of LDAP directory. You can specify eDirectory, Active Directory, or Sun ONE.

If eDirectory has been configured to use Domain Services for Windows, eDirectory behaves like Active Directory. When you configure such a directory to be a user store, its Directory Type must be set to Active Directory for proper operation.

9 Under *Server Replicas*, click *New* to specify the user store replica information. It is recommended that you specify an LDAP server that contains a read/write replica.

Name: The display name for the LDAP directory server.

IP Address: The IP address of the LDAP directory server. The port is set automatically to the standard LDAP ports.

10 Click *Use secure LDAP connections*. You must enable SSL between the identity user store and the Identity Server. The port changes to 636, the secure LDAP port.

11 Click *Auto import trusted root*.

12 Click *OK* to confirm the import.

13 Select one of the certificates in the list.

You are prompted to choose either a server certificate or a root CA certificate. To trust one certificate, choose *Server Certificate*. Choose *Root CA Certificate* to trust any certificate signed by that certificate authority.

14 Specify an alias, then click *OK*.

An alias is a name you use to identify the certificate used by Access Manager.

15 Click *Close*, then click *OK*.

16 Under *Server Replicas*, verify the *Validation Status*.

The system displays a green check mark if the connection is valid. 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.

17 Add a search context. Click *New*, specify the DN of the context, select a scope, then click *OK*.

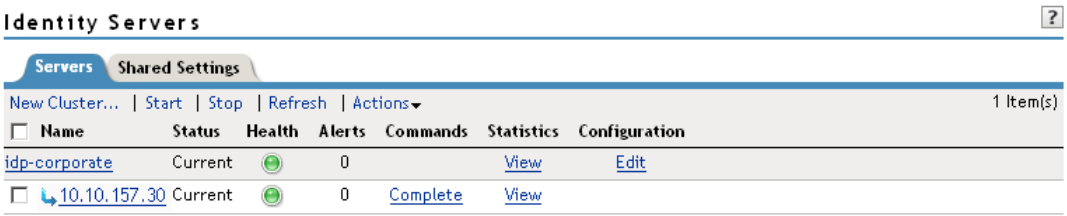
The search context is used to locate users in the directory. If a user exists outside of the specified search context and its scope (object, subtree, one level), the Identity Server cannot find the user, and the user cannot log in.

If the search context you specify finds more that one user with the same username, the Identity Server cannot authenticate these users. A username must be unique within a search context.

This is required for Active Directory or Sun ONE; it is optional for eDirectory, but recommended. If a search context is not specified for eDirectory, the entire tree is searched from the root.

18 Click *Finish* to save the server configuration.

19 Restart Tomcat as prompted.



The Health status icons for the configuration and the Identity Server should turn green. It might take several seconds for the Identity Server to start and for the system to display a green light. If the health does not turn green, see "Monitoring the Health of an Identity Server" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

20 (Optional) Verify the configuration by entering the Base URL of the Identity Server as the URL in a browser. Log in using the credentials of a user in the LDAP server.

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 the port.

21 If you have already installed an Access Gateway, continue with one of the following:

- To use your own Web server pages, continue with Section 1.4, "Configuring the Access Gateway," on page 18.

- To use the Digital Airlines sample Web pages, continue with Chapter 7, "Digital Airlines Example," on page 97.

To install an Access Gateway, see "Installing the Linux Access Gateway" or "Installing the NetWare Access Gateway" in the *Novell Access Manager 3.0 SP3 IR2 Installation Guide*.

1.4 Configuring the Access Gateway

The basic Access Gateway configuration procedures have been divided into the following tasks:

- Section 1.4.1, "Configuring a Reverse Proxy," on page 18
- Section 1.4.2, "Configuring a Public Protected Resource," on page 20

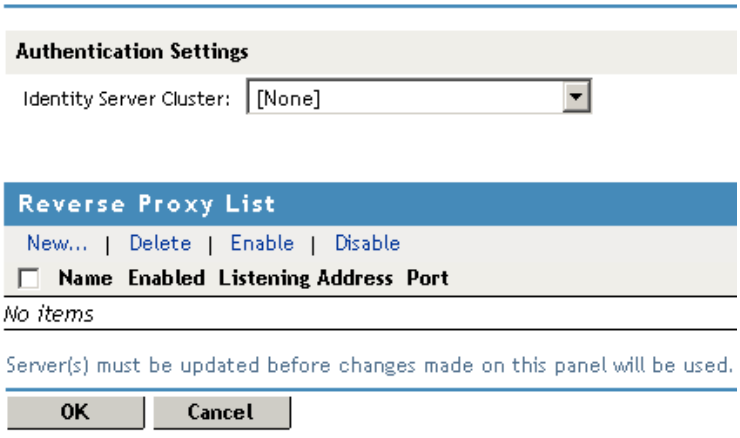
1.4.1 Configuring a Reverse Proxy

You protect your Web services by creating a reverse proxy. A reverse proxy acts as the front end to your Web servers in your DMZ or on your intranet, and off-loads frequent requests, thereby freeing up bandwidth and Web server connections. It also increases security because the IP addresses and DNS names of your Web servers are hidden from the Internet. A reverse proxy can be configured to protect one or more proxy services.

To create a reverse proxy, you must create at least one proxy service with a protected resource. You must supply a name for each of these components. Reverse proxy names and proxy service names must be unique to the Access Gateway because they are configured for global services such as IP addresses and TCP ports. For example, if you have a reverse proxy named `products` and another reverse proxy named `library`, only one of these reverse proxies can have a proxy service named `corporate`.

Protected resource names need to be unique to the proxy service, but they don't need to be unique to the Access Gateway because they are always accessed through their proxy service. For example, if you have a proxy service named `account` and a proxy service named `sales`, they both can have a protected resource named `public`.

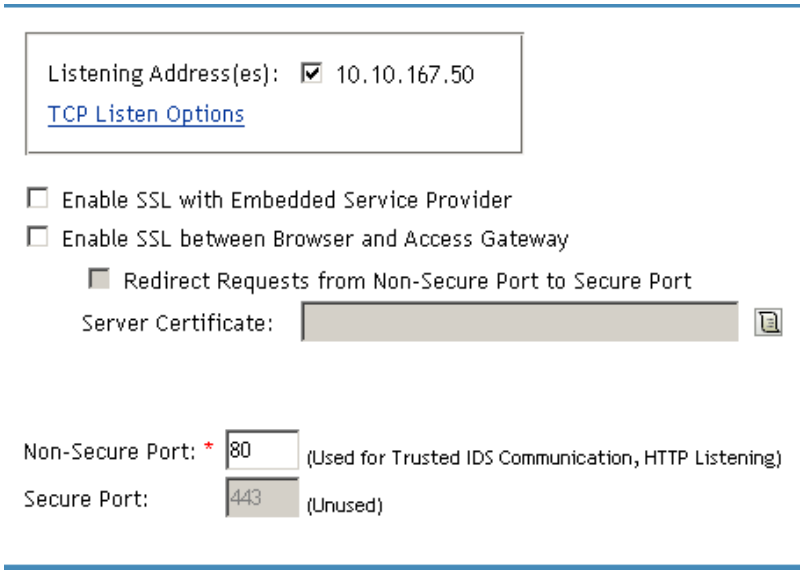
1 In the Administration Console, click *Access Manager* > *Access Gateways* > *Edit* > *Reverse Proxy / Authentication*.



2 In the *Identity Server Cluster* option, select the configuration you have assigned to the Identity Server.

This sets up the trust relationship between the Access Gateway and the Identity Server that is used for authentication.

3 In the *Reverse Proxy List*, click *New*, specify a display name for the reverse proxy, then click *OK*.



4 Enable a listening address.

Listening Address(es): A list of available IP addresses. If the server has only one IP address, only one is displayed and it is automatically selected. If the server has multiple addresses, you can select one or more IP addresses to enable. You must enable at least one address by selecting its check box.

TCP Listen Options: Options for configuring how requests are handled. You cannot set up the listening options until you create a proxy service.

5 Ignore the SSL configuration options.

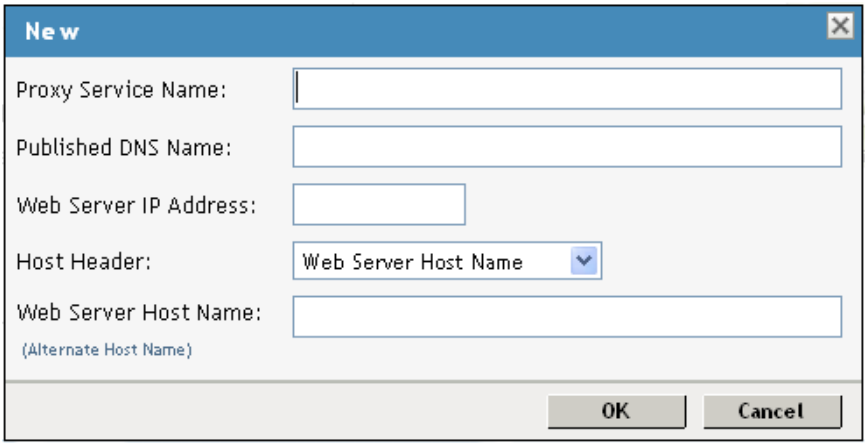
This basic configuration does not set up SSL. For SSL information, see Chapter 3, “Enabling SSL Communication,” on page 33.

6 Configure a listening port.

Non-Secure Port: Select 80, which is the default port for HTTP.

Secure Port: This is the HTTPS listening port. This port is unused and cannot be configured until you enable SSL.

7 In the *Proxy Service List*, click *New*.



8 Fill in the fields.

Proxy Service Name: A display name for the proxy service.

Published DNS Name: The DNS name you want the public to use to access your site. This DNS name must resolve to the IP address you set up as the listening address. For the example in Figure 1-2 on page 12, this name would be www.mytest.com.

Web Server IP Address: The IP address of your Web server. This is usually a Web server with content that you want to share with authorized users and protect from all others. In Figure 1-2 on page 12, this is Server 4, whose IP address is 10.15.70.21.

Host Header: The name you want sent in the HTTP header to the Web server. This can be either the Published DNS Name (the *Forward Received Host Name* option) or the DNS name of the Web Server (the *Web Server Host Name* option).

Web Server Host Name: The DNS name that the Access Gateway should forward to the Web server. This option is not available if you selected *Forward Received Host Name* for the *Host Header* option. The name you use depends upon how you have set up the Web server. If your Web server has been configured to verify that the host name in the header matches its name, you need to specify that name here. In Figure 1-2 on page 12 the Web Server Host Name is mywebserver.com.

9 Click *OK*.

10 Continue with Section 1.4.2, "Configuring a Public Protected Resource," on page 20.

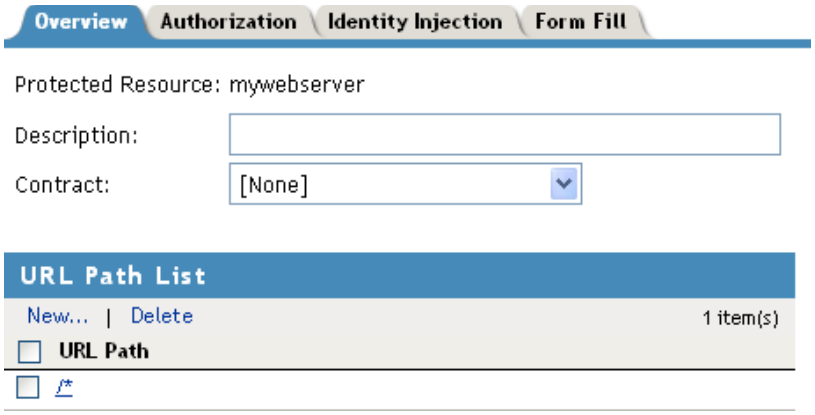
1.4.2 Configuring a Public Protected Resource

The first protected resource in this configuration tutorial is configured to be a public resource. For information on how to set up authentication for a protected resource, see Section 1.5, "Configuring the Access Gateway for Authentication," on page 22.

1 In the *Proxy Service List*, click *[Name of Proxy Service] > Protected Resources*.

2 In the *Protected Resource List*, click *New*.

3 Specify a display name for the protected resource, then click *OK*.



4 (Optional) Specify a description for the protected resource.

5 In the *Contract* field, select *None*.

The *Contract* field must be set to *None*. This is what makes this resource a public resource.

6 Configure the *URL Path List*.

The default path is `/*`, which allows access to everything on the Web server. Modify this if you need to restrict access to a specific directory on your Web server.

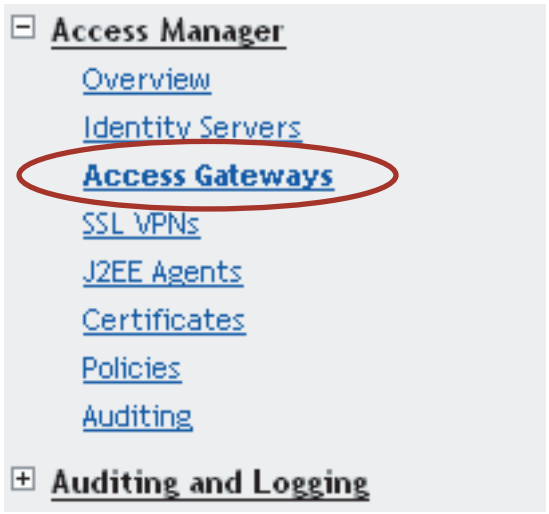
- To delete the default path, select the check box by the path, then click *Delete*.
- To edit a path in the list, click the path, modify it, then click *OK*.
- To add a path, click *New*, specify the path, then click *OK*. For example, to allow access to the pages in the public directory on the Web server, specify the following path:

  `/public/*`

7 Click *OK*.

8 In the *Protected Resource List*, verify that the protected resource you created is enabled, then click OK.

9 Click the *Access Gateways* link.



10 To apply the changes, click *Update* > *OK*.

Until this step, nothing has been permanently saved or applied. The *Update* status pushes the configuration to the server and writes the configuration to the configuration data store. When the update has completed successfully, the server returns the status of *Current*.

To save the changes to the configuration store without applying them, do not click *Update*. Instead, click *Edit*. If you have pending configuration settings, the *OK* button is active, and the configuration page indicates which services will be updated. Click *OK* to write these changes to the configuration store. The changes are not applied until you click *Update* on the Access Gateways page.

11 To update the Identity Server to establish the trust relationship with the Access Gateway, click *Identity Servers* > *Update*, then click *OK*.

Wait until the *Command* status is *Complete* and the *Health* status is green.

12 Click *Close*.

13 (Optional). To test this configuration from a client browser, enter the published DNS name as the URL in the browser. For the example illustrated in Figure 1-2 on page 12, you would enter the following URL:

```
http://www.mytest.com
```

This should resolve to the published DNS name you specified in Step 8 on page 20, and the user should be connected to the Web server through the Access Gateway.

14 Continue with Section 1.5, "Configuring the Access Gateway for Authentication," on page 22.

1.5 Configuring the Access Gateway for Authentication

The procedures in Section 1.4, "Configuring the Access Gateway," on page 18 set up the Access Gateway to protect your Web server by hiding its IP address and DNS name from Internet users. The procedure does not require the user to log in before accessing resources on the Web server. This section explains how to configure the Access Gateway so that the users are required to authenticate by supplying login credentials before they can access a protected resource. There are two parts to enabling authentication to protected resources:

- Section 1.5.1, "Verifying Time Synchronization," on page 22
- Section 1.5.2, "Enabling Trusted Authentication," on page 24

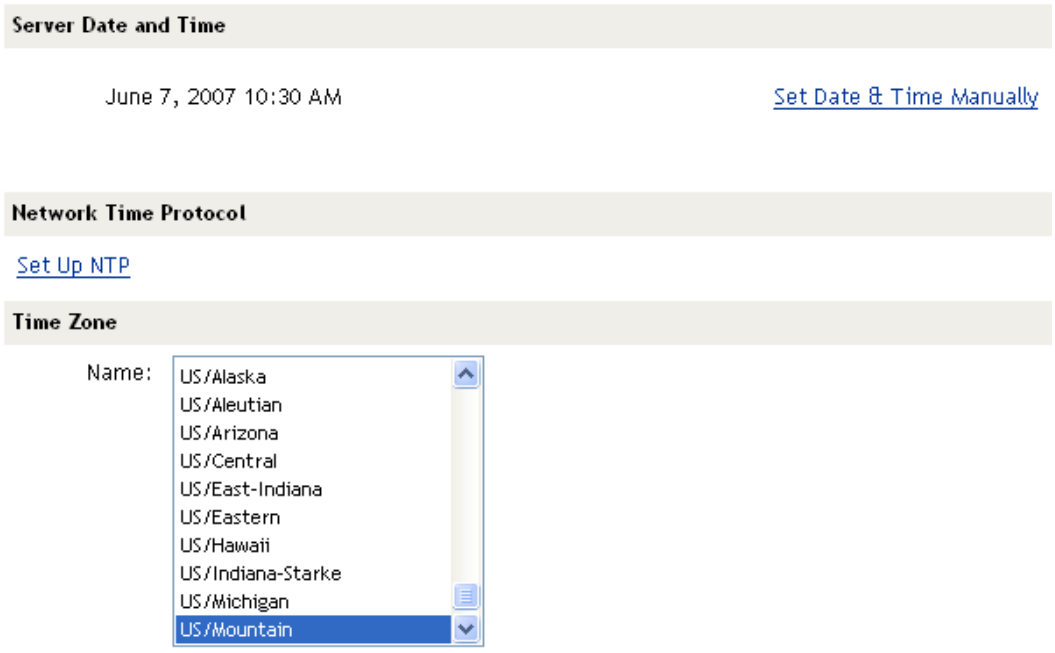
1.5.1 Verifying Time Synchronization

The time must be synchronized between the Identity Server and the Access Gateway or set so the time difference is within one minute of each other for trusted authentication to work.

For the Identity Server, use YaST to verify the time settings. If you have a Network Time Protocol server, configure the server to use it.

For an Access Gateway, complete the following steps:

1 In the Administration Console, click *Access Manager* > *Access Gateways* > *Edit* > *Date & Time*.



2 Select the method you want to use for time:

Set Date & Time Manually: Allows you to select the current time. Click this option to select the year, month, day, hour, and minutes in your current time zone, then click *OK*.

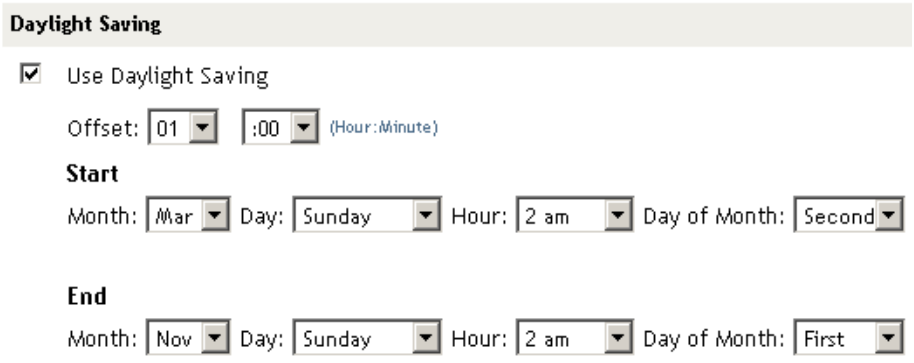
Set Up NTP: Allows you to specify the IP address of an NTP server. Click *Set Up NTP*. Use the public pool.ntp.org server or click *New*, then specify the IP address of an NTP server. To accept the configuration, click *OK*.

If the time on the machine is wrong by more than an hour, use both methods to set the time. Set it manually first, and then configure it to use NTP.

3 In the *Time Zone* section, select your time zone, then click *OK*.

Regardless of the method you used to set the time, you must select a time zone.

4 (NetWare only) Configure daylight saving time.



In the Daylight Saving section, configure the following fields:

Use Daylight Saving: Enables daylight saving time for your time zone.

Offset: The hours and minutes that daylight saving time varies from standard time.

Start: The month, day, hour, and day of month when daylight saving time starts.

Stop: The month, day, hour, and day of month when daylight saving time ends.

5 To save the changes to browser cache, click *OK*.

6 To apply your changes, click the *Access Gateways* link, then click *Update* > *OK*.

7 Continue with "Enabling Trusted Authentication" on page 24.

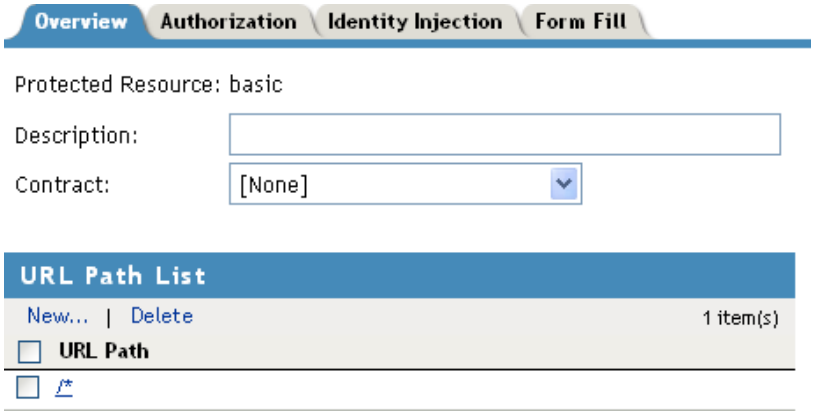
1.5.2 Enabling Trusted Authentication

Trusted authentication requires an authentication contract that specifies the type of authentication credentials. The Identity Server and the Access Gateway control these authentication requirements. You do not need to configure your Web server to require authentication. Access Manager enforces the requirements for you.

In this example, you set up an authentication contract that requires a username and a password to access a directory on a Web server.

1 In the Administration Console, click *Access Manager* > *Access Gateways* > *Edit* > *[Name of Reverse Proxy]* > *[Name of Proxy Service]* > *Protected Resources* > *New*.

2 Specify a display name for the protected resource, then click *OK*.



3 Select either the *Name/Password - Basic* or the *Name/Password - Form* contract:

- **Name/Password - Basic:** Basic authentication over HTTP using a standard login page provided by the Web browser.
- **Name/Password - Form:** Form based authentication over HTTP.

Others are available, but for this basic setup, which does not enable SSL, select one of the above contracts. The contract needs to match the protocol.

If these default authentication contracts are not available, you have not configured a relationship between the Access Gateway and the Identity Server. See Section 1.4.1, "Configuring a Reverse Proxy," on page 18 and select a value for the *Identity Server Cluster* field.

4 In the *URL Path List*, configure the URL path to the page that this authentication contract will protect. For the Web server configuration described in "Prerequisites for Setup" on page 12, click the `/*` path and modify it to specify the following path:

```
/protected/*
```

5 Click *OK*.

6 To save the changes to browser cache, click *OK*.

7 To apply your changes, click the *Access Gateways* link, then click *Update* > *OK*.

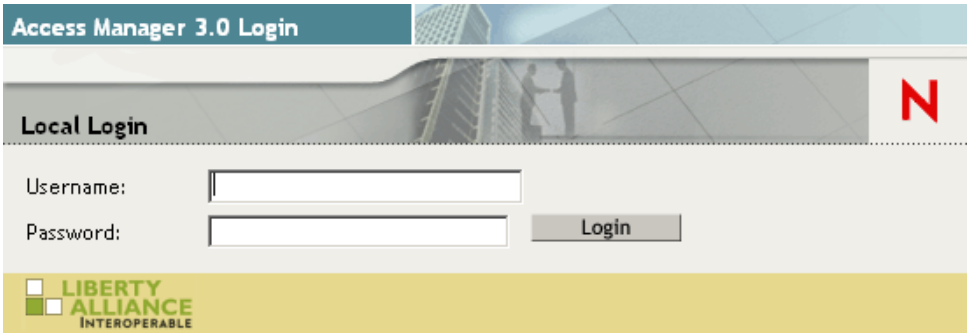
8 (Optional) To test this configuration from a client browser, log in to the Access Manager Portal:

8a Specify the published DNS name to this resource in the browser. For the example illustrated in Figure 1-2 on page 12, you would enter the following URL:

```
http://www.mytest.com
```

8b Click the link to the protected page. This should be a link to the same page you configured in Step 4.

Your browser should prompt you with a login page. If you selected *Name/Password - Basic* as the contract, the standard login page issued by your browser is displayed. If you selected *Name/Password - Form*, the default Access Manager login page is displayed.



8c Log in to the Identity Server with a username and password that is stored in your LDAP directory (Server 3 in Figure 1-2 on page 12).

You should have access to the information you have placed in the `protected` directory on your Web server.

If you have set up your Web server to require basic authentication to access this directory, you are prompted again for login credentials.

9 Continue with Section 1.6, "Setting Up an Identity Injection Policy," on page 25.

1.6 Setting Up an Identity Injection Policy

The Access Gateway lets you retrieve information from your LDAP directory and inject the information into HTML headers, query strings, or basic authentication headers. The Access Gateway can then send this information to the back-end Web servers. Access Manager calls this technology *Identity Injection*. Novell iChain® calls it Object Level Access Control (OLAC). This is one of the features within Access Manager that enables single sign-on. The user is prompted once for the login credentials, and Access Manager then supplies them for the resources you have configured for Identity Injection.

This section explains how to set up an Identity Injection policy for basic authentication. This policy is assigned to the third directory on your Web server, the `basic` directory that your Web server has been configured to require basic authentication before allowing access.

1 In the Administration Console, click *Access Manager* > *Access Gateways* > *Edit* > *[Reverse Proxy Name]* > *[Proxy Service Name]* > *Protected Resources* > *New*.

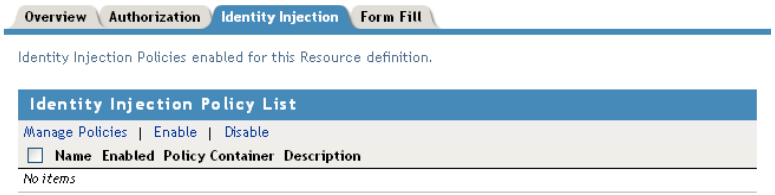
2 Configure the resource for the `basic` directory as described in Section 1.2, "Prerequisites for Setup," on page 12.

2a For the contract, select *Name/Password - Basic* or *Name/Password - Form*.

2b For the URL path, enter the path to the basic directory (`/basic/*`).

2c Click *OK*.

3 Click *[Protected Resource Name] > Identity Injection*.



On a new installation, the list is empty because no policies have been created.

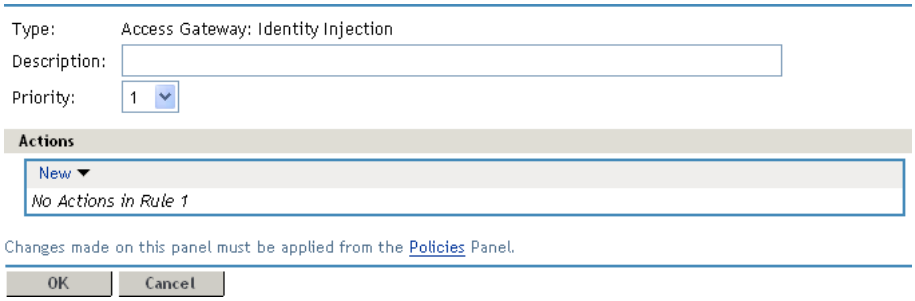
4 In the *Identity Injection Policy List* section, click *Manage Policies*.

5 In the *Policy List* section, click *New,* then specify values for the following fields.

Name: Specify a name for the Identity Injection policy.

Type: Select *Access Gateway: Identity Injection*.

6 Click *OK*.



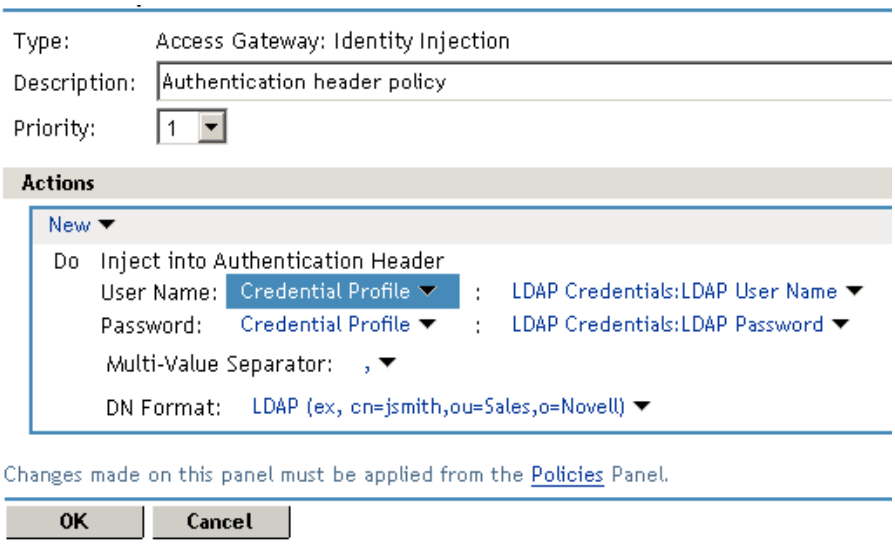
7 (Optional) Specify a description for the policy.

8 In the *Actions* section, click *New > Inject into Authentication Header*.

9 Set up the policy for *User Name* and *Password*:

- For *User Name*, select *Credential Profile* and *LDAP Credentials: LDAP User Name*. This injects the value of the cn attribute into the header.
- For *Password*, select *Credential Profile* and *LDAP Credentials: LDAP Password*.

The policy should look similar to the following:



10 Click *OK* twice, then click *Apply Changes*.

11 Click *Close*.

12 Select the new Identity Injection policy, then click *Enable*.

13 To save the changes to browser cache, click *OK*.

14 To apply your changes, click the *Access Gateways* link, then click *Update* > *OK*.

15 To test this configuration from a client browser, enter the published DNS name as the URL in the browser. Click the link to the page using basic authentication.

   You are prompted to log in. If you have set up Web applications on your Web server that require login, any additional login prompts are hidden from the user and are handled by the identity injection system.

For an example of how Identity Injection policies can be used for single sign-on to the IDM User Application, see Configuring Access Manager for UserApp and SAML (http://www.novell.com/coolsolutions/appnote/19981.html).

Configuring SSL VPN to Protect an Application

2

The Novell® SSL VPN is a remote access security solution that extends the reach of HTTP and non-HTTP enterprise applications to mobile workers, telecommuters, partners, and customers. By using secure sockets layer (SSL) as the underlying security protocol, Novell SSL VPN allows for truly unrestricted remote access. This solution uses the ubiquitous Web browser as the primary client interface and integrates with Novell Identity Provider for authentication.

- Section 2.1, "Prerequisites," on page 29
- Section 2.2, "Injecting the SSL VPN Header," on page 29

2.1 Prerequisites

- You have installed the SSL VPN server. See "Installing SSL VPN" in the *Novell Access Manager 3.0 SP3 IR2 Installation Guide*.
- You have configured a basic Access Manager system with a functional Identity Server and Access Gateway. See Chapter 1, "Setting Up a Basic Access Manager Configuration," on page 11.
- You have configured some Identity Server roles. The roles you create depend upon the requirements of your application. See "Creating Roles" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

  NOTE: The role name in the application might be case sensitive. When you create your roles in Access Manager, make sure you match the case.

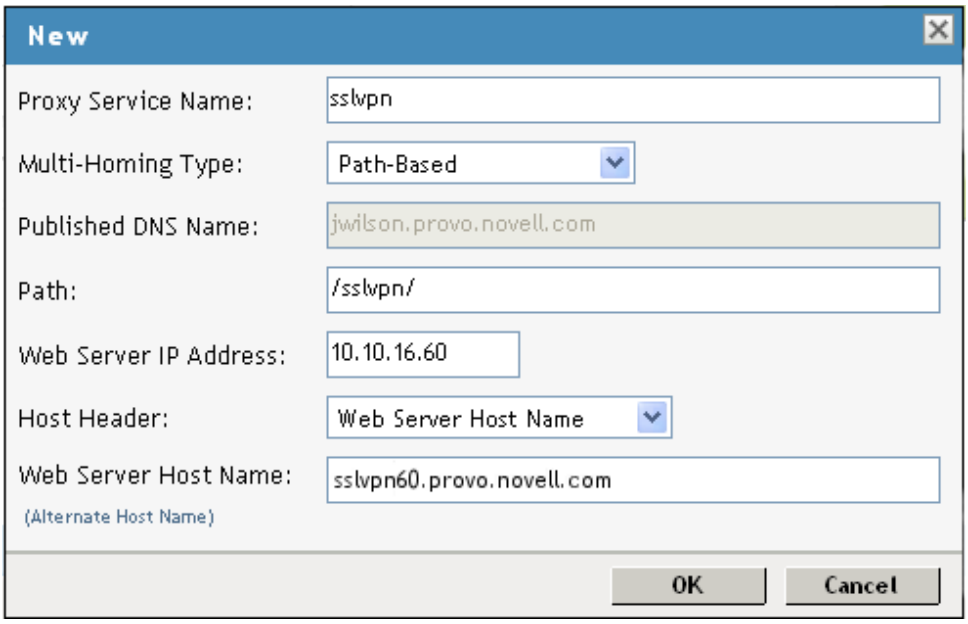
- You have a TCP-based application that you want to protect with SSL VPN. To do this on an example Web server, see "Configuring the SSL VPN as a Protected Resource" on page 126.

2.2 Injecting the SSL VPN Header

The example in this section explains how to accelerate SSL VPN server in a path-based multi-homing configuration.

Before you begin, make sure you have already created a proxy service and an authentication procedure. For more information on creating a proxy service and authentication procedure, see Section 1.4.1, "Configuring a Reverse Proxy," on page 18.

1. In the Administration Console, click *Access Manager* > *Access Gateways* > *Edit* > *[Name of Reverse Proxy]*.
2. In the *Proxy Service List* section, click *New*.



3 Fill in the following fields.

Proxy Service Name: Specify a name for proxy service.

Multi-Homing Type: Specify the method for finding a second resource on the reverse proxy. For this example configuration, *Path-Based* has been selected.

Published DNS Name: This field is populated by default with the published DNS name.

Path: Specify the path to the SSL VPN resource. This must be `/sslvpn/`

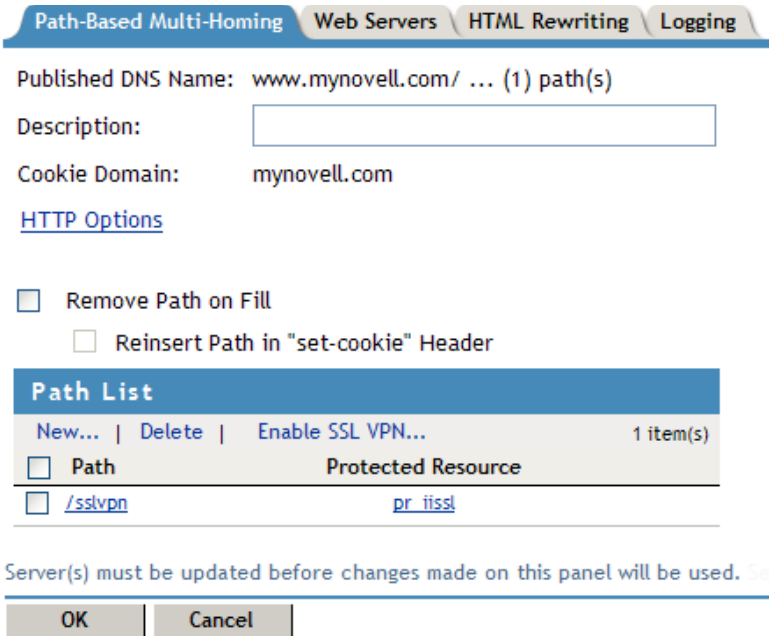
Web Server IP Address: Specify the IP address of the SSL VPN server.

Host Header: Select which hostname is forwarded to the Web server in the host header. If your SSL VPN server has a DNS name, select *Web Server Host Name*.

Web Server Host Name: Specify the DNS name of the SSL VPN server.

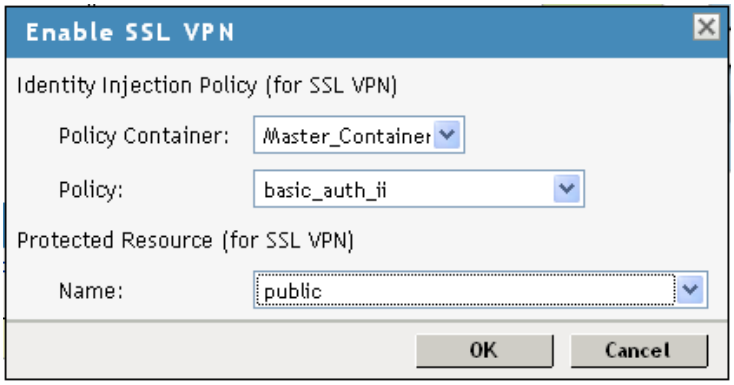
4 Click *OK*.

5 To configure the default Identity Injection policy and protected resources, click the newly added proxy service.



6 In the *Path List* section, make sure the *Path* is */sslvpn*.

7 In the *Path List* section, select the */sslvpn* check box, then click *Enable SSL VPN*. The Enable SSL VPN pop-up is displayed.



8 Fill in the following fields:

- **Policy Container:** Leave the default value unchanged.
- **Policy:** Select *Create SSL VPN Default Policy* from the drop-down list. A policy pop-up appears. Click *Apply Changes* in the pop-up, then click *Close*.

  The default SSL VPN policy injects both the username and password in the authentication header. If you do not want the password to be pushed to the authentication header, configure a policy with a username and a string constant. For more information on configuring policies, see "Creating Identity Injection Policies" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

  You can also configure the SSL VPN policy to inject the client IP address, so that the IP address can then be included in log entries. For more information, see "Configuring the Default Identity Injection Policy" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

- **Name:** Select *Create SSL VPN Default Protected Resource* from the drop-down list.

9 Click *OK* to close the *Enable SSL VPN* pop-up.

10 Click the *Web Servers* tab.

11 Specify 8080 in the *Connect Port* field, then click *OK*.

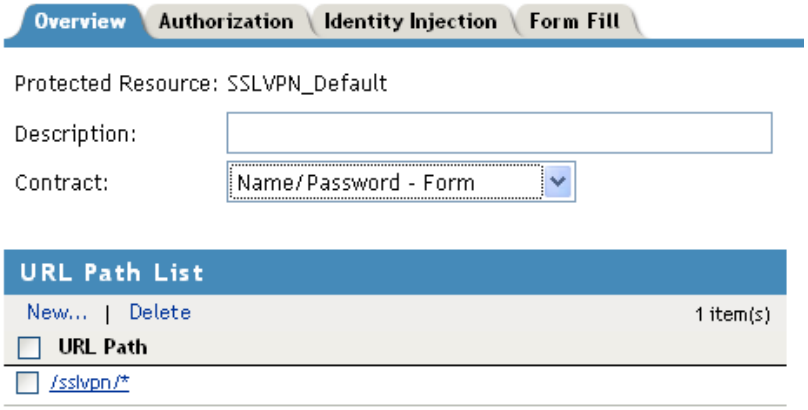
12 In the *Proxy Service List* section, click the name of the parent proxy service of the newly created SSL VPN proxy service. This host does not have a multi-homing value.

13 Select the *Protected Resources* tab.

14 Select *SSLVPN_Default* from *Protected Resources List*.

15 Select an authentication contract from the *Contract* drop-down list. Make sure you select *Name/Password - Form* as the authentication contract.

16 In the *URL Path List* section, ensure that the URL is */sslvpn/**.



IMPORTANT: Make sure that you configure the URL as given above. Any variation leads to the failure of SSL VPN service.

17 Click *Configuration Panel,* then click *OK*.

18 On the *Configuration* page, click *OK*.

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

20 To update the Identity Server, click *Identity Servers* > *Update*.

21 Click *Close*.

Enabling SSL Communication

3

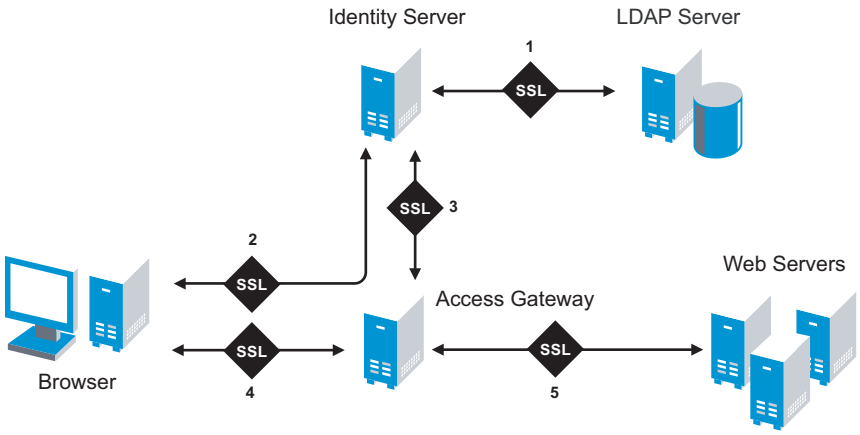
Because the Identity Server handles authentication, it must be configured for SSL before any of the other Access Manager components. You can then configure the Access Gateway to use SSL in its connections to the Identity Server, to the browsers, and to its Web servers.

- Section 3.1, “Identifying the SSL Communication Channels,” on page 33
- Section 3.2, “Using Access Manager Certificates,” on page 34
- Section 3.3, “Using Externally Signed Certificates,” on page 42

3.1 Identifying the SSL Communication Channels

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*



You were instructed to set the first channel between the Identity Server and the LDAP servers when you configured the user stores (see Step 10 in Section 1.3, “Creating a Basic Identity Server Configuration,” on page 13). The other channels need to be configured according to their numeric values. You need to configure SSL between the Identity Server and the browsers before you configure the channel between the Access Gateway and the Identity Server for SSL.

The eDirectory™ that resides on the Administration Console is the main certificate store for all of the Access Manager components. You can use this local certificate authority (CA) to create certificates for SSL or you can purchase certificates from a well-known certificate authority. This section describes how to use both types of certificates to enable secure communication.

- Section 3.2, “Using Access Manager Certificates,” on page 34
- Section 3.3, “Using Externally Signed Certificates,” on page 42

3.2 Using Access Manager Certificates

By default, all Access Manager components (Identity Server, Access Gateway, SSL VPN, and J2EE Agents) trust the local CA. However, the browsers are not set up to trust the Access Manager CA. You need to import the public key of the trusted root certificate (configCA) into the browsers to establish the trust.

This section discusses the following procedures:

- Section 3.2.1, “Configuring Secure Communication on the Identity Server,” on page 34
- Section 3.2.2, “Configuring the Access Gateway for SSL,” on page 37

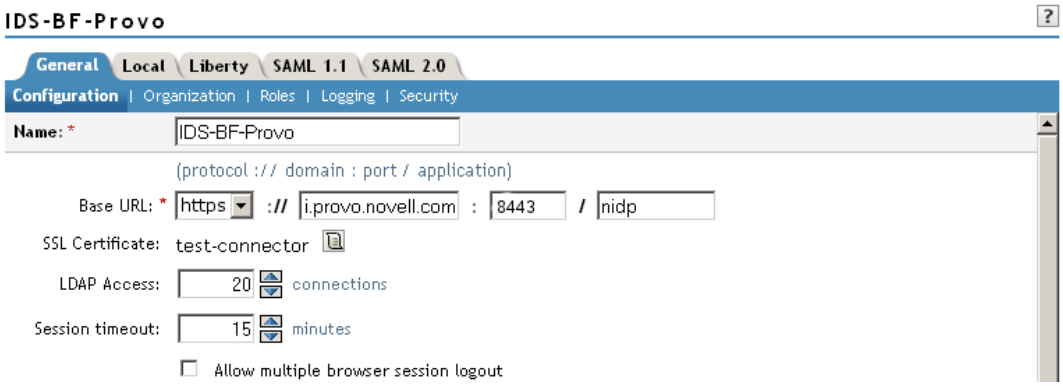
3.2.1 Configuring Secure Communication on the Identity Server

The Identity Server comes with a the test-connector certificate. This procedure shows you how to replace this certificate by completing the following tasks:

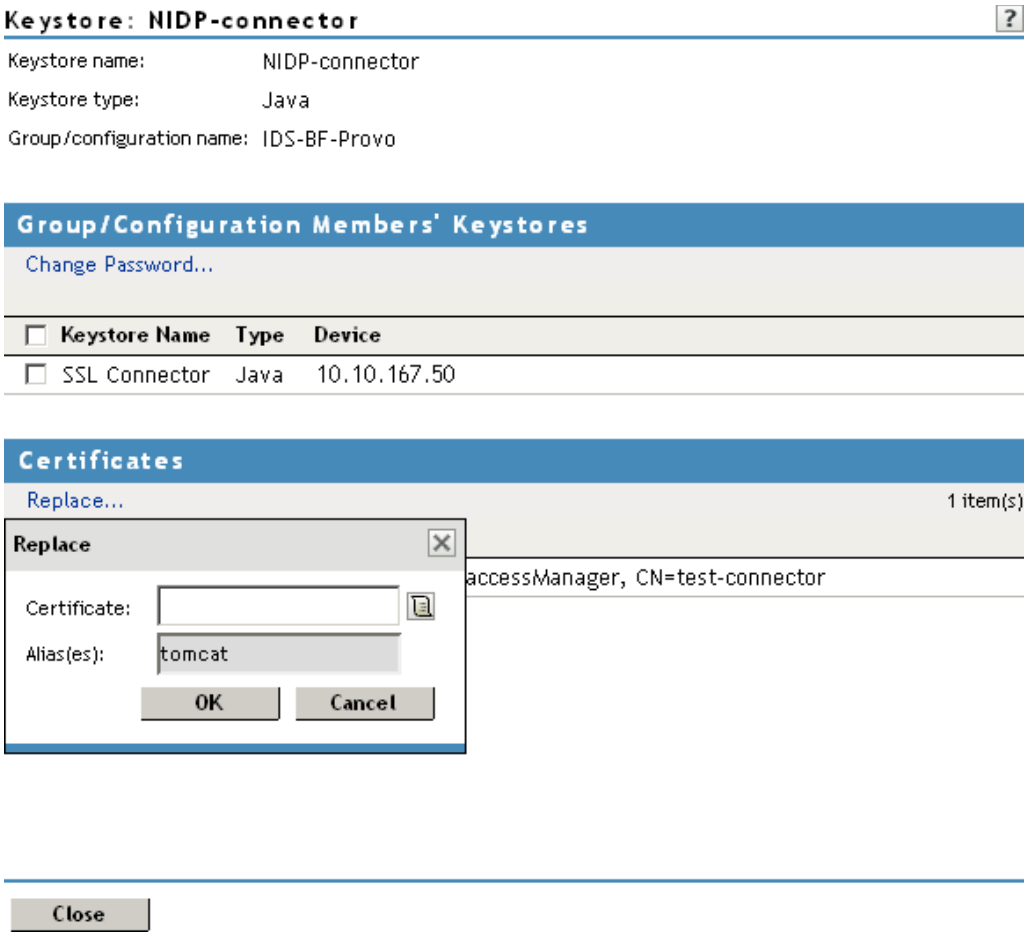
- Enable SSL on the Identity Server (changing from HTTP to HTTPS)
- Create a certificate
- Replace the test-connector certificate with the newly created certificate

To configure SSL on the Identity Server:

1. In the Administration Console, click *Access Manager* > *Identity Servers* > *Edit*.
2. Change *Protocol* to HTTPS (the system changes the port to 8443).
3. Copy the domain name of your Identity Server configuration to the Clipboard, or take note of the name. It must match the common name of the new certificate.

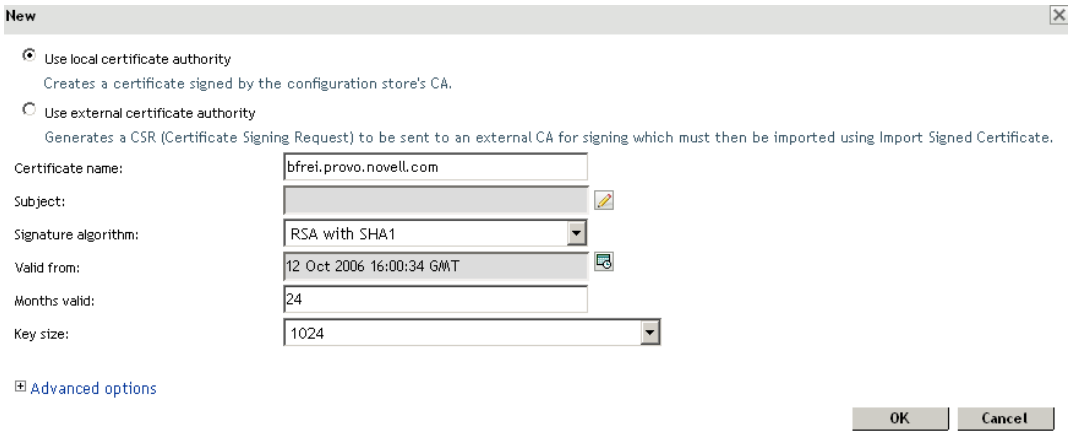


4. Click *SSL Certificate*, then click *Replace*.



5 In the *Replace* dialog box, click the *Select Certificate* icon next to the *Certificate* field.

6 On the Select Certificate page, click *New*.



7 Click *Use local certificate authority*.

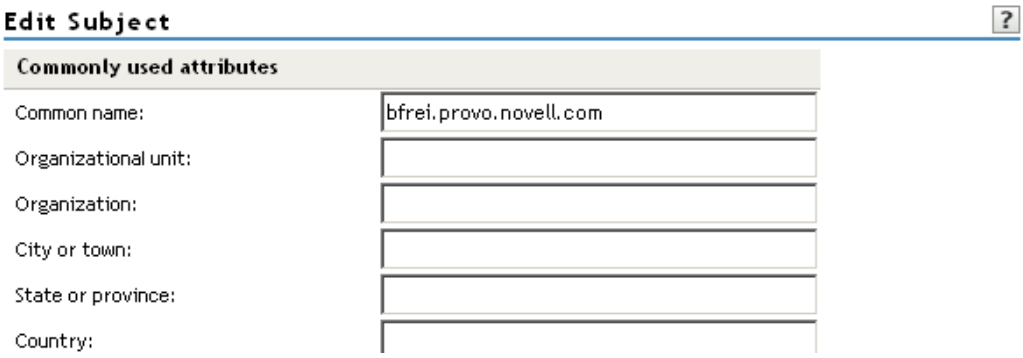
This option creates a certificate signed by the local CA (or Organizational CA), and creates the private key.

8 Fill in the following fields:

Certificate name: The name that you can associate with this certificate. For easy reference, you might want to paste the domain name of the Identity Server configuration in this field.

For information on how to modify the default values before clicking *OK*, see "Creating Certificates" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

Subject: Click the *Edit Subject* icon. In the *Common Name* field, paste the domain name of the base URL of the Identity Server configuration. This value cannot be an IP address or begin with a number, in order to ensure that trust does not fail between providers.

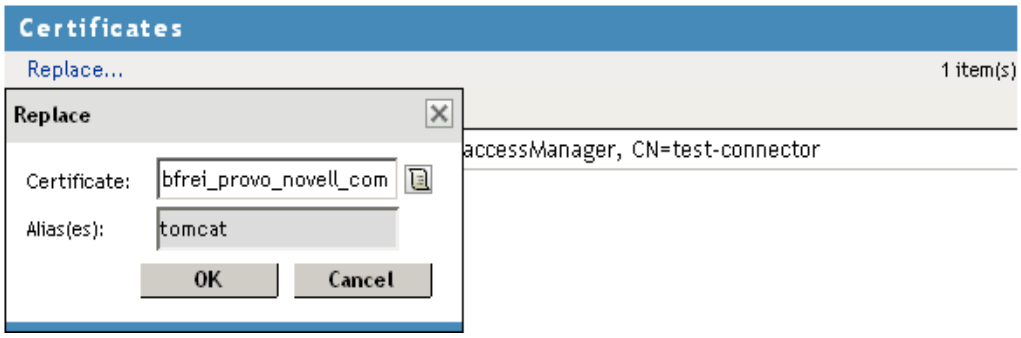


9 Click *OK*.

10 To accept the default values in the other fields, click *OK* twice.

The new certificate is displayed on the Select Certificate page.

11 Verify that the new certificate is selected, then click *OK*.



12 Click *OK* on the *Replace* dialog box.

13 Click *Restart Now* to restart Tomcat, as prompted.

14 Click *Close* on the *Keystore* page.

You should wait about thirty seconds for the restart. If your Identity Server and Administration Console are on the same machine, you need to log in to the Administration Console again.

15 To update the Identity Server, click *Access Manager > Identity Servers > Update*.

16 To update the embedded service provider of the Access Gateway to use the new URL, click *Access Gateways > Update*.

This re-establishes the trust between the Access Gateway and the new base URL for the Identity Server.

17 Verify that the trusted relationship between the Identity Server and the Access Gateway has been reestablished.

17a Enter the URL to a protected resource on the Access Gateway.

17b Complete one of the following:

- If you are prompted for login credentials, enter them. The trusted relationship has been reestablished. Continue with Section 3.2.2, "Configuring the Access Gateway for SSL," on page 37.
- If you receive a 100101043 or 100101044 error, the trusted relationship has not been established. For information on solving this problem, see "Troubleshooting 100101043 and 100101044 Liberty Metadata Load Errors" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

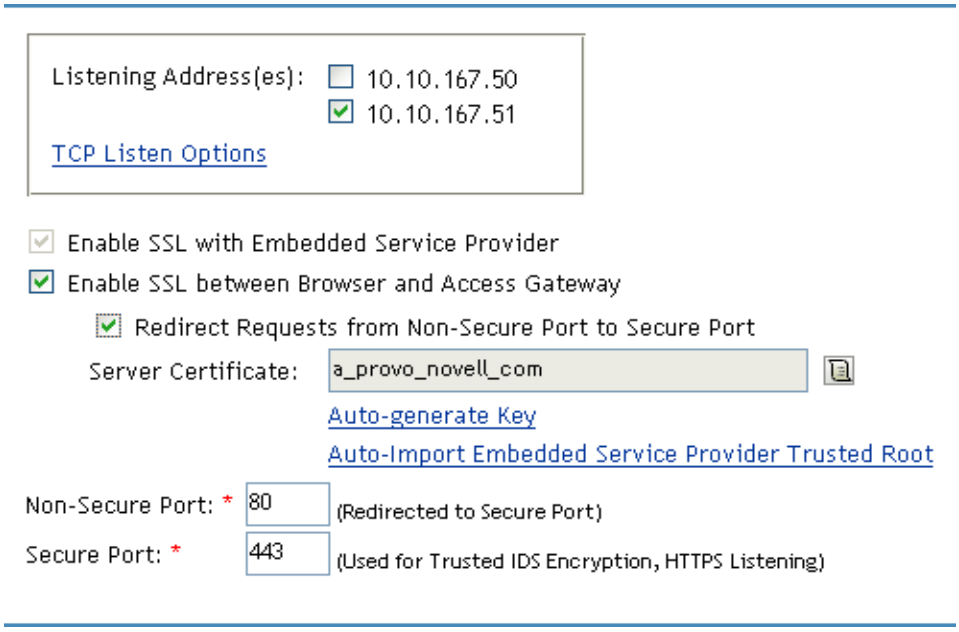
3.2.2 Configuring the Access Gateway for SSL

This section describes how to set up SSL for the Access Gateway communication channels:

- "Configuring SSL Communication with the Browsers and the Identity Server" on page 37
- "Enabling SSL between the Reverse Proxy and Its Web Servers" on page 39

Configuring SSL Communication with the Browsers and the Identity Server

1 In the Administration Console, click *Access Manager* > *Access Gateways* > *Edit* > *[Name of Reverse Proxy]*.



2 To configure the reverse proxy for SSL, fill in the following fields:

Enable SSL with Embedded Service Provider: Select this option to encrypt the data exchanged for authentication (the communication channel between the Identity Server and the Access Gateway). This option is only available for the reverse proxy that has been assigned to perform authentication.

If you enable SSL between the browsers and the Access Gateway, this option is automatically selected for you. You can enable SSL with the embedded service provider without enabling SSL between the Access Gateway and the browsers. This allows the authentication and identity information that the Access Gateway and the Identity Server exchange to use a secure channel, but allows the Access Gateways to use non-secure channels with the browsers and the Web servers. This saves processing overhead if the data on the Web servers is not sensitive.

Enable SSL between Browser and Access Gateway: Select this option to require SSL connections between your clients and the Access Gateway. SSL must be configured between the browsers and the Access Gateway before you can configure SSL between the Access Gateway and the Web servers. For this process, see Section , "Enabling SSL between the Reverse Proxy and Its Web Servers," on page 39.

Redirect Requests from Non-Secure Port to Secure Port: Determines whether browsers are redirected to the secure port and allowed to establish an SSL connection. If this option is not selected, browsers that connect to the non-secure port are denied service.

3 To generate a certificate key by using the Access Manager CA:

3a Click *Auto-generate Key*, then click *OK* twice.

3b On the Select Certificate page, make sure the certificate is selected, then click *OK*.

The generated certificate appears in the *Server Certificate* text box.

4 Configure the ports for SSL:

Non-Secure Port: Specifies the port on which to listen for HTTP requests. The default port for HTTP is 80. If you have selected the *Redirect Requests from Non-Secure Port to Secure Port* option, requests sent to this port are redirected to the secure port. If the browser can establish an SSL connection, the session continues on the secure port. If the browser cannot establish an SSL connection, the session is terminated.

Secure Port: Specifies the port on which to listen for HTTPS requests (which is usually 443). This port needs to match the configuration for SSL. If SSL is enabled, this port is used for all communication with the browsers. The listening address and port combination must not match any combination you have configured for another reverse proxy or tunnel.

5 In the *Proxy Service List*, click *[Name of Proxy Service] > Protected Resources*.

6 In the *Protected Resource List*, change the Contract assignments from HTTP contracts to HTTPS contracts.

For example, if a protected resource is using the Name/Password - Basic contract, click the name and change it to the Secure Name/Password - Basic or the Secure Name/Password - Form contract. Then click *OK*.

To enable single sign-on, select the same contract for all the protected resources.

7 Click *Configuration Panel*, then in the confirmation box, click *OK*.

8 On the Server Configuration page, click *Reverse Proxy / Authentication*.

9 In the *Embedded Service Provider* section, click *Auto-Import Identity Server Configuration Trusted Root*, click *OK*, specify an alias, click *OK* twice, then click *Close*.

This option imports the public key of the Identity Server into the trust store of the embedded service provider. This sets up a trusted SSL relationship between the embedded service provider and the Identity Server.

The configCA public key certificate of the Access Manager CA is automatically added to the ESP Trust Store. If you are using Access Manager CA certificates for the Identity Server, you

do not need to import the configCA certificate unless someone has deleted it from this trust store.

10 Click *Configuration Panel*, then in the confirmation box, click *OK*.

11 On the Server Configuration page, click *OK*.

12 On the Access Gateways page, click *Update* > *OK*.

13 Update the Identity Server so that it uses the new SSL configuration. Click *Identity Servers* > *Update*.

14 Verify that the trusted relationship between the Identity Server and the Access Gateway has been reestablished:

14a Enter the URL to a protected resource on the Access Gateway. For example, enter

```
https://www.mytest.com
```

14b Complete one of the following:

- If you are prompted for login credentials, enter them. The trusted relationship has been reestablished.
- If you receive a 100101043 or 100101044 error, the trusted relationship has not been established. For information on solving this problem, see "Troubleshooting 100101043 and 100101044 Liberty Metadata Load Errors" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

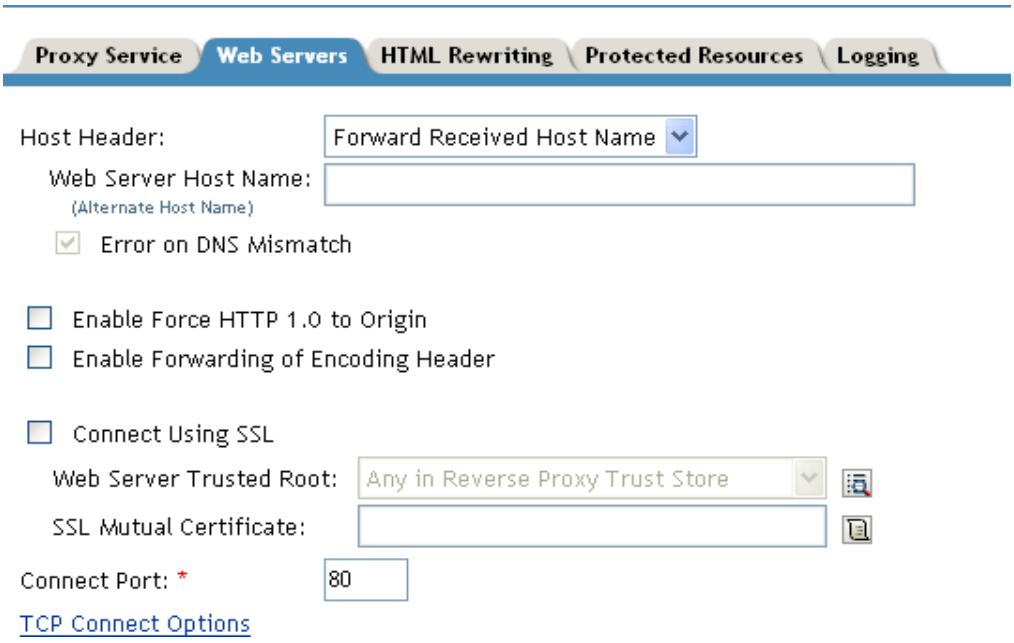
Enabling SSL between the Reverse Proxy and Its Web Servers

To enable SSL between the reverse proxy and the Web servers, you must have already performed the following tasks:

- ❑ Enabled SSL between the Access Gateway and the browsers. See Section 1.4.1, "Configuring a Reverse Proxy," on page 18 and select the *Enable SSL between Browser and Access Gateway* field.
- ❑ Enabled SSL on the Web server. See your Web server documentation.

If you have completed these tasks:

1 In the Administration Console, click *Access Manager* > *Access Gateways* > *Edit* > *[Name of Reverse Proxy]* > *[Name of Proxy Service]* > *Web Servers*.



2 To configure SSL, select *Connect Using SSL*.

This option is not available if you have not set up SSL between the browsers and the Access Gateway. See Section 1.4.1, "Configuring a Reverse Proxy," on page 18 and select the *Enable SSL between Browser and Access Gateway* field.

3 In the *Connect Port* field, specify the port that your Web server uses for SSL communication.

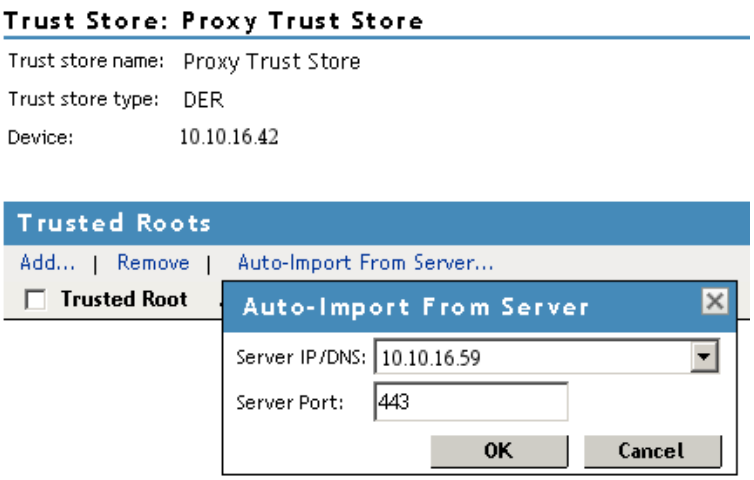
4 Configure how you want the certificate verified. The Access Gateway platforms support different options:

4a (Conditional) If you are configuring a Linux Access Gateway, select one of the following options:

- To not verify this certificate, select *Do not verify* for the *Web Server Trusted Root*. Continue with Step 9.
- To allow the certificate to match any certificate in the trust store, select *Any in Reverse Proxy Trust Store* for the *Web Server Trusted Root*. Continue with Step 9.
- To add a certificate to the trust store for the Web server, click the *Manage Reverse Proxy Trust Store* icon. Continue with Step 4c.

4b (Conditional) If you are configuring a NetWare® Access Gateway, all the certificates in the certificate chain of the Web server must be in its trust store. To add these certificates to the trust store, click *Any in Reverse Proxy Trust Store*. Continue with Step 4c.

4c The auto import screen appears.



5 Ensure that the IP address of the Web server and the port match your Web server configuration.

If these values are wrong, you have entered them incorrectly on the Web server page. Click *Cancel* and reconfigure them before continuing.

6 Click *OK*.

Wait while the Access Gateway retrieves the server certificate, the root CA certificate, and any CA certificates from a chain from the Web server.

7 Specify an alias, then click *OK*.

All the displayed certificates are added to the trust store.

8 Click *Close*.

9 (Optional) For mutual authentication, the Access Gateway platforms support different options:

9a (Conditional) If you are configuring a Linux Access Gateway, you need to select the certificate. Click the *Select Certificate* icon, select the certificate you created for the reverse proxy, then click *OK*.

This is only part of the process. You need to import the trusted root certificate of the CA that signed the proxy service's certificate to the Web servers assigned to this proxy service.

9b (Conditional) If you are configuring a NetWare Access Gateway, the text box displays the certificate that is sent to the Web server if the Web server requires it. If the Web server is not set up for mutual SSL, the certificate is not sent.

To set up the Web server for mutual SSL, you need to import the trusted root certificate of the CA that signed the certificate displayed in the text box.

10 Click *Configuration Panel*, then click *OK*.

11 On the *Configuration* page, click *OK*.

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

13 (Optional). To test this configuration from a client browser:

13a Enter the published DNS name as the URL in the browser.

13b Click the links that require authentication for access.

3.3 Using Externally Signed Certificates

When the Identity Server is configured to use an SSL certificate that is signed externally, the trusted store of the embedded service provider for each component must be configured to trust this new CA. The browsers that are used to authenticate to the Identity Server must be configured to trust the CA that created the certificate for the Identity Server. If you obtain a certificate from a well-known external CA, most browsers are already configured to trust certificates from well-known CAs.

The following procedures explain how to use certificates signed by an external Certificate Authority.

- Section 3.3.1, "Obtaining Externally Signed Certificates," on page 42
- Section 3.3.2, "Configuring the Identity Server to Use an Externally Signed Certificate," on page 44
- Section 3.3.3, "Configuring the Access Gateway to Use an Externally Signed Certificate," on page 45

3.3.1 Obtaining Externally Signed Certificates

The following sections explain how to create certificate signing requests for the Identity Server and Access Gateway, how to use the requests to obtain a signed certificates, then how to import the signed certificates and the root certificate of the Certificate Authority into Access Manager.

- "Creating the Certificate Signing Request" on page 42
- "Getting a Signed Certificate" on page 43
- "Importing the Signed Certificates and Root Certificate" on page 44

Creating the Certificate Signing Request

You need to create two certificate signing requests: one for the Identity Server and one for the Access Gateway. The *Certificate name* and the *Common name* need to be different, but the other values can be the same.

What you need to know or create	Example	Your Value
Certificate name	ipda_test or lag_test	_____ _____
Certificate Subject Fields:		
Common name	ipda.test.novell.com or lag.test.novell.com	_____ _____
Organizational unit	o=novell	_____
Organization	test	_____
City or town	Provo	_____
State or province	UT	_____
Country	US	

To create a signing request for the Identity Server:

1. In the Administration Console, click *Access Manager* > *Certificates* > *New*.
2. Select the *Use External certificate authority* option.
3. Fill 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.
4. Click the *Edit* icon on the *Subject* line.
5. 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`
6. Click *OK* twice, then click the name of the certificate.
7. Click *Export CSR*.

   The signing request is saved to a file.
8. Repeat Step 1 through Step 7 to create a signing request for the Access Gateway. Use `lag_test` for the *Certificate name* and `lag.test.novell.com` for the *Common name*.

Getting a Signed Certificate

You can send the certificate signing request to a Certificate Authority and wait for the CA to return a signed certificate or you can use a trial certificate while you wait for the official certificate. Companies such as Thawte* and VeriSign* offer trial signed certificates.

Modify the following instructions for the CA you have selected to sign your certificates:

1. Set up an account with a Certificate Authority and select the free trial option.
2. Open your certificate signing request for the Identity Server in a text editor.
3. Copy and paste the text of the certificate request into the appropriate box for a trial certificate.
4. Click *Next*, then copy the signed certificate and paste it into a new text file or at the bottom of the signing request file.
5. Click *Back*, and repeat Step 2 through Step 4 for the Access Gateway.
6. Follow the instructions on the Web site to download the root certificate of the Certificate Authority.

Importing the Signed Certificates and Root Certificate

The following steps explain how to imported the signed certificates and the trust root into the Administration Console so that they are available to be assigned to key stores and trusted root stores.

1. In the Administration Console, click *Access Manager* > *Certificates* > *Trusted Roots*.
2. Click *Import*, then specify a name for the root certificate.
3. Click *Browse*, and locate the root certificate file.
4. Click *OK*.

   The trusted root is added and is now available to add to trusted root stores.
5. In a text editor, open the signed certificate for the Identity Server.
6. In the Administration Console, click *Access Manager* > *Certificates*, then click the name of certificate signing request for the Identity Server.
7. Click *Import Signed Certificate*, then select *Certificate data text (PEM/Based64)*.
8. Paste the text for the signed certificate into the data text box. Copy everything from

   `-----BEGIN CERTIFICATE-----`

   through

   `-----END CERTIFICATE-----`
9. Click *Add trusted root*, then click the *Browse* icon and locate the root certificate file.
10. Click *OK*.

    The certificate is now available to be assigned to the keystore of a device.

    If the certificate fails to import and you receive an error, it is probably missing a trusted root certificate in a chain of trusted roots. To determine whether this is the problem, see "Resolving a -1226 PKI Error " and "Importing an External Certificate Key Pair" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.
11. Repeat Step 5 through Step 10 for the Access Gateway certificate.

3.3.2 Configuring the Identity Server to Use an Externally Signed Certificate

This section explains how to enable SSL between the Identity Servers and the browsers.

1. In the Administration Console, click *Access Manager* > *Identity Servers* > *Edit*.
2. For the protocol in the *Base URL* option, select *https*.
3. In the *SSL Certificate* line, click the *Browse* icon.
4. In the *Certificates* section, click *Replace*, then click the *Browse* icon.
5. Select the Identity Server certificate, then click *OK* twice.
6. At the prompt to restart Tomcat, select to restart Tomcat now.
7. Click *Close* > *OK*.
8. Wait for the Identity Server health to turn green.
9. Click Access Gateway > *Edit* > *Service Provider Certificates* > *Trusted Roots*.
10. In the *Trusted Roots* section, click *Add*, then click the *Browse* icon.

11 Select the trusted root certificate of the Certificate Authority that signed the Identity Server certificate.

12 Click *OK* until you return the Service Provider Certificates page.

IMPORTANT: If the external Certificate Authority writes the DN in reverse order (the cn element comes first rather than last), you receive an error message that the certificate names do not match. You can ignore this warning, if the order of the DN elements is the cause.

---

13 Click *Close*, then click the *Access Gateways* task.

14 Click *Update*.

15 Test the SSL connection between the browser and the Identity Server:

15a Enter the Base URL of the Identity Server in a browser.

```
https://idpa.test.novell.com:8443/nidp
```

15b If the URL returns a login page, 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 trusts the CA that created the certificate.
- The browser can resolve the DNS name of the Identity Server
- The browser can access port 8443.

16 Verify that the trusted relationship between the Identity Server and the Access Gateway has been reestablished:

16a Enter the URL to a protected resource on the Access Gateway.

16b Complete one of the following:

- If you are prompted for login credentials, enter them. The trusted relationship has been reestablished.
- If you receive a 100101043 or 100101044 error, the trusted relationship has not been established. For information on solving this problem, see "Troubleshooting 100101043 and 100101044 Liberty Metadata Load Errors" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

3.3.3 Configuring the Access Gateway to Use an Externally Signed Certificate

This section explains how to enable SSL communication between the Access Gateway and the Identity Server (channel 3 in Figure 3-1 on page 33) and between the Access Gateway and the browsers (channel 4 in Figure 3-1 on page 33).

1 In the Administration Console, click *Access Manager > Access Gateways > Edit > [Name of Reverse Proxy]*.

2 Select *Enable SSL with Embedded Service Provider*.

3 Select *Enable SSL between Browser and Access Gateway*.

4 In the *Server Certificate* line, click the *Browse* icon.

5 Select the Access Gateway certificate, then click *OK*.

IMPORTANT: If the external Certificate Authority writes the DN in reverse order (the cn element comes first rather than last), you receive an error message that the subject name does not contain the cn of the device. You can ignore this warning, if the order of the DN elements is the cause.

6 To add the trusted root of the CA that signed the Access Gateway certificate, click *Auto-Import Embedded Service Provider Trusted Root*, then click *OK*.

7 Specify an *Alias* for the certificate, then click *OK* > *Close*.

8 On the Reverse Proxy page, click *OK* twice.

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

10 Click *Identity Servers* > *Update*.

11 Verify that the trusted relationship between the Identity Server and the Access Gateway has been reestablished:

11a Enter the URL to a protected resource on the Access Gateway.

11b Complete one of the following:

- If you are prompted for login credentials, enter them. The trusted relationship has been reestablished.
- If you receive a 100101043 or 100101044 error, the trusted relationship has not been established. For information on solving this problem, see "Troubleshooting 100101043 and 100101044 Liberty Metadata Load Errors" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

Clustering and Fault Tolerance

4

For additional capacity and for failover, you can cluster a group of Identity Servers and configure them to act as a single server. You can also create a cluster of Access Gateways and configure them to act as a single server. Clustering enables the following features:

- **Configuration Synchronization:** You configure the cluster, and the configuration is synchronized to all members of the cluster.
- **Session Sharing:** Each cluster member can handle sessions held by another server in the cluster. After a session is established, the same member usually handles all requests for that session. However, if that cluster member is not available to handle a request, another member steps in and processes the request.

You can also provide fault tolerance for the configuration store on the Administration Console by installing secondary versions of the console. The following sections explain how to set up these components for fault tolerance:

- Section 4.1, “Installing Secondary Versions of the Administration Console,” on page 47
- Section 4.2, “Clustering Identity Servers,” on page 49
- Section 4.3, “Clustering Access Gateways,” on page 53
- Section 4.4, “Configuration Tips for the L4 Switch,” on page 56

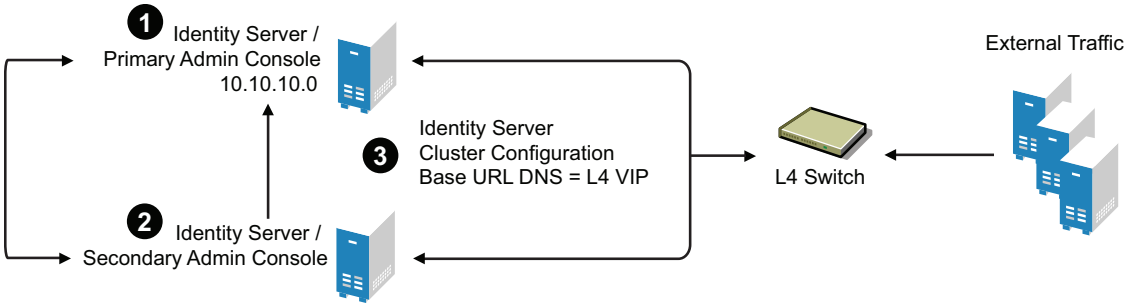
4.1 Installing Secondary Versions of the Administration Console

The Administration Console contains an embedded version of eDirectory™, which contains all the configuration information for the Access Manager. It also contains a server communications module, which is in constant communication with the Access Manager modules. If the Administration Console goes down and you have not installed any secondary consoles, your Access Manager components also go down and your protected resources become unavailable.

You can install the Administration Console and the Identity Server on the same machine in a production environment. You can install a secondary Administration Console on the same machine as a clustered Identity Server. Two or more Administration Consoles cannot be configured as a virtual group on an L4 switch, because the L4 switch interferes with the communication process between the Administration Consoles and the Access Manager components. Each Access Manager component knows which Administration Console is its primary console and its secondary console and knows how to communicate directly with each console. The component, rather than an L4 switch, needs to make the decision on which console it needs to contact.

However, traffic destined for a cluster of components (Identity Servers or Access Gateways) can pass through an L4. Figure 4-1 illustrates this configuration, showing Identity Servers on the same machine as Administration Consoles.

Figure 4-1 *Identity Server Clustering with a Secondary Administration Console*



1. Install the primary Administration Console and an Identity Server on one machine, using the Administration Console's IP address when importing the Identity Server component. (See "Installing the Novell Identity Server" in the *Novell Access Manager 3.0 SP3 IR2 Installation Guide*.)
2. Install the secondary Administration Console and a second Identity Server on another machine, using the primary Administration Console's IP address when importing the second Identity Server.
3. Specify the L4 VIP as the DNS for the Identity Server cluster configurations that both Identity Servers use. (See Section 1.3, "Creating a Basic Identity Server Configuration," on page 13.)

When the primary console goes down, the secondary console can be used for the following tasks:

- Administrators can make configuration changes on a secondary console, and these changes are sent to the Access Manager components.
- Access Manager components can use the secondary console to access their configuration information and to respond to configuration changes. As soon as the primary console comes back online, the components revert to using the primary machine, but they continue to accept commands from the secondary consoles.

WARNING: As long as the primary console is running, all configuration changes should be made at the primary console. If you make changes at both a primary console and a secondary console, browser caching can cause you to create an invalid configuration.

You can create fault tolerance by installing up to two secondary consoles. We highly recommend that you install at least one secondary console.

- Section 4.1.1, "Prerequisites," on page 48
- Section 4.1.2, "Installing a Second Console," on page 49
- Section 4.1.3, "Tasks Requiring the Primary Console," on page 49

4.1.1 Prerequisites

- For a secure configuration, secondary consoles must be installed on the same network as the primary console. The administration consoles should not be required to use a router to communicate with each other.
- The administration consoles must have their time synchronized. The easiest way to ensure this is to configure the machines to use the same network time server for time synchronization.

4.1.2 Installing a Second Console

1. Insert the CD containing the Administration Console software.

   Most of the installation process is the same for a secondary console as for a primary. For these basic instructions, see "Installing the Access Manager Administration Console" in the *Novell Access Manager 3.0 SP3 IR2 Installation Guide*.

2. To install a secondary console, answer No to the following prompt:

   ```
   Is this the primary administration server in a failover group?
   ```

3. When prompted, enter the IP address of the primary console.

4. Continue with the installation process.

   After installing a secondary console, you might have to wait from 30 to 60 minutes before using it. The components query the primary console hourly for information about available consoles, and they reject commands from a console that is not in their approved list. You can force the components to recognize the secondary console by restarting the Integration Agent on each Identity Server, Linux Access Gateway, and Linux J2EE Agent with the following command:

   ```
   /etc/init.d/novell-jcc restart
   ```

   For the NetWare Access Gateway, you need to wait until the primary console informs it of the new secondary console.

5. If you have added multiple replicas for any of the user stores, you need to manually add them to the secondary console. See "Configuring the User Store " in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

4.1.3 Tasks Requiring the Primary Console

The primary console must be used for the following tasks:

- **New Device Installation:** The primary console must be running when you install new devices such as another Access Gateway or SSL VPN server.
- **Backup and Restore:** Backup and restore must be run on the primary console. When the restore has completed, you must restart Tomcat on all secondary consoles. Use the following command:

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

  For more information about backup and restore, see "Backing Up and Restoring Components" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

4.2 Clustering Identity Servers

A cluster of Identity Servers should reside behind an L4 switch. Clients access the virtual IP address of the cluster presented on the L4 switch, and the L4 switch alleviates server load by balancing traffic across the cluster. If your Identity Server is on the same machine as an Administration Console, and your second Identity Server is on the same machine as a secondary Administration Console, ensure that you are familiar with Section 4.1, "Installing Secondary Versions of the Administration Console," on page 47 before proceeding.

Whenever a user accesses the virtual IP address (port 8080) assigned to the L4 switch, the system routes the user to one of the Identity Servers in the cluster, as traffic necessitates.

The system automatically enables clustering when multiple Identity Servers exist in a group. If only one Identity Server exists in a group, clustering is disabled.

This section describes how to set up and manage a cluster of Identity Servers:

- Section 4.2.1, “Services of the Real Server,” on page 50
- Section 4.2.2, “Prerequisites,” on page 50
- Section 4.2.3, “Setting Up a Cluster,” on page 51

4.2.1 Services of the Real Server

A user’s authentication remains on the real (authentication) server cluster member that originally handled the user’s authentication. If this server malfunctions, all users whose authentication data resides on this cluster member must reauthenticate.

Requests that require user authentication information are processed on this server. When the system identifies a server as not being the real server, the HTTP request is forwarded to the appropriate cluster member, which processes the request and returns it to the requesting server.

A Note about Alteon Switches

When configuring an Alteon switch for clustering, direct communication between real servers must be enabled. If direct access mode is not enabled then when one of the real servers tries to proxy another real server, the connection fails and times out.

To enable direct communication on the Alteon:

1. Go to cfg > slb > adv > direct.
2. Specify *e* to enable direct access mode.

With some L4 switches, you should configure only the services that you are using. For example, if you configure the SSL service for the L4 and you have not configured SSL in Access Manager, then the HTTP service on the L4 will not work. If the health check for the SSL service fails, then the L4 assumes that all the services configured to use the same virtual IP are down.

4.2.2 Prerequisites

- ❑ An L4 server installed. You can use the same server for Identity Server clustering and Access Gateway clustering, provided that you use different virtual IPs. The LB algorithm can be anything (hash/sticky bit), defined at the Real server level.
- ❑ Persistence (sticky) sessions enabled on the L4 server. You usually define this at the virtual server level.
- ❑ An Identity Server configuration created for the cluster. You assign all the Identity Servers to this configuration. See “Creating a Cluster Configuration” in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide* for information about creating an Identity Server configuration. See “Assigning an Identity Server to a Cluster Configuration” in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide* for information about assigning Identity Servers to configurations.

  The base URL DNS name of this configuration must resolve via DNS to the IP address of the L4 virtual IP address. The L4 balances the load between the identity servers in the cluster.

- ❑ Ensure that the L4 administration server using port 8080 has the following ports open:
  - 8443 (secure Administration Console)
  - 7801 (TCP)
  - 636 (for secure LDAP)
  - 389 (for clear LDAP, loopback address)
  - 524 (network control protocol on the L4 machine for server communication)

  The identity provider ports must also be open:
  - 8080 (nonsecure login)
  - 8443 (secure login)
  - 1443 (server communication)

  If you are using introductions (see "Creating a Cluster Configuration" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*), you must configure the L4 switch to load balance on ports 8445 (identity provider) and 8446 (identity consumer).

4.2.3 Setting Up a Cluster

1. Install the additional Identity Servers.

   During the installation, choose option 2, *Install Novell Identity Server*, from CD 1 of the Access Manager installation discs. Specify the IP address and administration credentials of each additional Identity Server. If you are installing on a machine without the Administration Console, the installation asks you for the Administration Console's IP address. After you install the Identity Servers, the servers are displayed on the Servers page in Identity Servers.
2. Assign the Identity Servers to the same cluster configuration.

   For more information about assigning servers to a configuration, see "Assigning an Identity Server to a Cluster Configuration" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.
3. Ensure that the L4 VIP is the DNS for the Identity Server clusters configuration. (See Section 1.3, "Creating a Basic Identity Server Configuration," on page 13.)
4. Click the configuration name you created for the cluster under *Configuration Assignment*.
5. On the Cluster Details page, click the configuration name.

6. Fill in the following fields as required:

   Name: Lets you change the name of the Identity Server cluster configuration.

Cluster Communication Backchannel: Provides a communications channel over which the cluster members maintain the integrity of the cluster. For example, this TCP channel is used to detect new cluster members as they join the cluster, and to detect members that leave the cluster. A small percentage of this TCP traffic is used to help cluster members determine which cluster member would best handle a given request. This back channel should not be confused with the IP address/port over which cluster members provide proxy requests to peer cluster members.

- **Port:** Specifies the TCP port of the cluster back channel on all of the Identity Servers in the cluster. 7801 is the default TCP port.

  Because the cluster back channel uses TCP, you can use cluster members on different networks. However, firewalls must allow the port specified here to pass through. To do so use the port number plus 1 for additional devices in the cluster. For example, if you use four devices, your port numbers would be 7801, 7802, 7803, and 7804.

- **Encrypt:** Encrypts the content of the messages that are sent between cluster members.

Level Four Switch Port Translation: Configures the L4 switch to translate the port of the incoming request to a new port when the request is sent to a cluster member. Because the cluster members communicate with each other over the same IP address/port as the L4 switch, the cluster implementation needs to know what that port is. The translated port is the port on the cluster members where other cluster members can contact it. This is the IP address and port where cluster members provide proxy requests to other cluster members.

- **Port translation is enabled on switch:** Specifies whether the port of the L4 switch is different from the port of the cluster member.
- **Cluster member translated port:** Specifies the port of the cluster member.

7 Click *OK*.

8 Under *Cluster Members*, you can refresh, start, stop, and assign servers to Identity Server configurations.

9 Click *OK*, then update the Identity Server as prompted.

Real Server Settings Example

```
Current real servers settings:
  1: 149.44.171.116, enabled, name l52, weight 1, timeout 10 mins, maxcon 200000
    backup none, inter 2, retry 4, restr 8
    remote disabled, proxy enabled, submac disabled
    cookie assignment server: disabled
    exclusionary string matching: disabled
    service ports: 8443 8080
    real ports:
      8443: vport 8443, group 1, pbind clientip
          virtual server:  1, 149.44.174.220,  enabled
      8080: vport 8080, group 1, pbind clientip
          virtual server:  1, 149.44.174.220,  enabled
  2: 149.44.174.51, enabled, name brie, weight 1, timeout 10 mins, maxcon 200000
    backup none, inter 2, retry 4, restr 8
    remote disabled, proxy enabled, submac disabled
    cookie assignment server: disabled
    exclusionary string matching: disabled
    service ports: 8443 8080
    real ports:
      8443: vport 8443, group 1, pbind clientip
          virtual server:  1, 149.44.174.220,  enabled
      8080: vport 8080, group 1, pbind clientip
          virtual server:  1, 149.44.174.220,  enabled
```

Virtual Server Settings Example

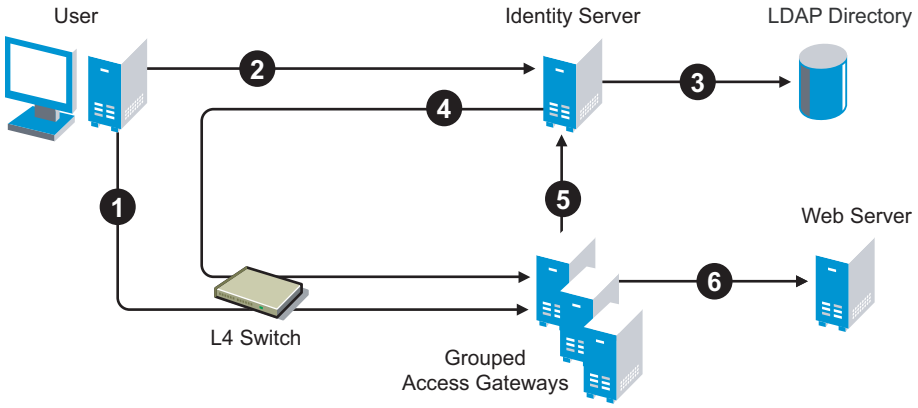
```
Current virtual servers settings:
  1: 149.44.174.220, enabled, dname idp
    virtual ports:
      8443: rport 8443, group 1, pbind clientip, frags
          real servers:
             1: 149.44.171.116,  weight 1,  enabled, backup none
             2: 149.44.174.51,   weight 1,  enabled, backup none
      8080: rport 8080, group 1, pbind clientip, frags
          real servers:
             1: 149.44.171.116,  weight 1,  enabled, backup none
             2: 149.44.174.51,   weight 1,  enabled, backup none
```

4.3 Clustering Access Gateways

A cluster of Access Gateways must reside behind a Layer 4 (L4) switch. Clients access the virtual IP on the L4, and the L4 alleviates server load by balancing traffic across the cluster of Access Gateways. Whenever a user enters the URL for an Access Gateway resource, the request is routed to the L4 switch, and the switch routes the user to one of the Access Gateways in the cluster, as traffic necessitates.

Figure 4-2 illustrates the flow of a user request when the Access Gateways are clustered behind an L4 switch.

Figure 4-2 *Grouping Access Gateways*



1. The user requests access to a protected resource by sending a request to the L4 switch. The request is sent to one of the Access Gateway servers in the cluster.
2. The Access Gateway redirects the request to the Identity Server for authentication. The Identity Server presents the user with a login page, requesting a user name and a password.
3. The Identity Server verifies the user's credentials with the directory.
4. The validated credentials are sent through the L4 switch to the same Access Gateway that first received the request.
5. The Access Gateway verifies the user credentials with the Identity Server.
6. If the credentials are valid, the Access Gateway forwards the request to the Web server.

If the Access Gateway where the user is assigned goes down, the user's request is sent to another Access Gateway in the cluster. This Access Gateway pulls the user's session information from the Identity Server. This allows the user to continue accessing resources, without having to reauthenticate.

The following sections describe how to set up and manage a cluster of Access Gateways.

- Section 4.3.1, "Prerequisites," on page 54
- Section 4.3.2, "Configuring a Cluster," on page 55

4.3.1 Prerequisites

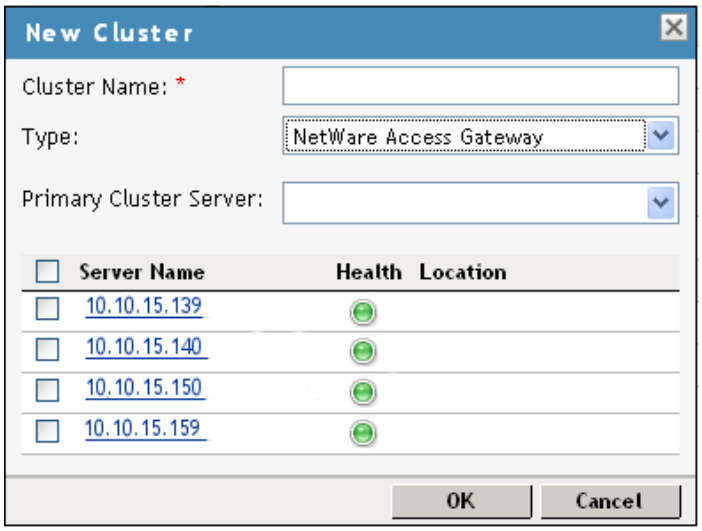
- ❑ An L4 switch installed. You can use the same switch for an Identity Server cluster and an Access Gateway cluster, provided that you use different virtual IPs.
- ❑ One or more Access Gateways installed. They must all be of the same type: either Linux Access Gateways or NetWare® Access Gateways. You cannot mix these two types in the same cluster.

  When you install each new Access Gateway, configure it to use the same Administration Console.
- ❑ Your DNS server must to be configured to resolve the published DNS names that you specify for your proxy services to the L4 switch.
- ❑ Enabling persistent (sticky) sessions on the L4 switch is highly recommended, but not required.

IMPORTANT: If you have created a configuration for one or more of the Access Gateways you are going to put in a cluster, you need to carefully select the primary cluster server. The current configuration of the primary cluster server is pushed to the other servers in the cluster. If you have created configurations for the other servers in the cluster, these configurations are overwritten.

4.3.2 Configuring a Cluster

1 In the Administration Console, click *Access Manager* > *New Cluster*.



2 Fill in the following fields:

- **Cluster Name:** Specify a display name for the cluster.
- **Type:** Select whether the cluster contains NetWare Access Gateways or Linux Access Gateways. A cluster cannot contain a mixture of these two types.

3 In the *Server Name* list, select the servers that you want to be members of the cluster.

You can create a cluster of one, and add additional servers later.

Each server you add to the cluster adds about 30 seconds to the time it takes to configure the cluster because certificates must be synchronized and configuration options must be sent to that server. If you create a very large cluster of twenty servers, it can take up to ten minutes to configure and create the cluster.

4 In the *Primary Cluster Server* field, select the server that is to be the primary server in the cluster.

The list is empty until you select the servers for the cluster. The configuration of the primary server is pushed to the other servers in the cluster. If any of the selected servers have been configured, their configurations are lost.

5 Click *OK*.

6 After the cluster has been created, each server in the cluster needs be restarted. On the *Access Gateways* page, click *Update All* by the name of the cluster.

7 (Conditional) If the Access Gateways in the cluster have multiple network adapters or IP addresses, you need to configure the listening address for each reverse proxy.

When creating the cluster configuration for newly added servers, the listening address is always the IP address of eth0. If this is not the address you want the reverse proxy to listen for requests, click *Access Gateways* > *Edit* > *[Name of Reverse Proxy]*, select the Access Gateway as the *Cluster Member*, then enable the *Listening Address* you want to use.

8 To configure the cluster, click *Access Gateways* > *Edit*.

A cluster of Access Gateways has the same configuration options as a single Access Gateway. The only difference is that for some options you need to select the Access Gateway to configure. For example, the *Date & Time* option allows you to set the time separately for each member of the cluster.

Applying the configuration to a cluster is slightly different. You have the option to apply the changes to all servers in the cluster by selecting the *Update All* option, or to apply them to one server at a time by selecting the *Update* option for each server.

If you prefer to apply changes to the servers one at time, you should save the changes to the configuration datastore. To do this, click *OK* on the Server Configuration page. The *OK* buttons on the other configuration pages save the changes to browser cache. If your session times out before you update all servers in the cluster, the changes are lost and are not applied to the servers that are still in an *Update* status.

4.4 Configuration Tips for the L4 Switch

When you use an L4 switch to cluster Identity Servers, Access Gateways, or both, you need to configure it and the DNS server for each cluster. You need to configure the DNS server to resolve the base URL of the Identity Server configuration to the Identity Server VIP on the L4 switch. You need to configure the DNS server to resolve the published DNS names of the Access Gateway to the Access Gateway VIPs on the L4 switch.

In addition to this basic setup, consider the following:

- Section 4.4.1, “Sticky Bit,” on page 56
- Section 4.4.2, “Network Configuration Requirements,” on page 56
- Section 4.4.3, “Health Checks,” on page 57
- Section 4.4.4, “Real Server Settings Example,” on page 61
- Section 4.4.5, “Virtual Server Settings Example,” on page 62

4.4.1 Sticky Bit

Each L4 switch has a slightly different method and terminology for the sticky bit or persistence bind. This bit allows a client, who has established a session, to be directed to the same Identity Server or Access Gateway for all requests sent during the session. This minimizes the need to forward session information between Access Gateways or between Identity Servers and thus maximizes performance.

4.4.2 Network Configuration Requirements

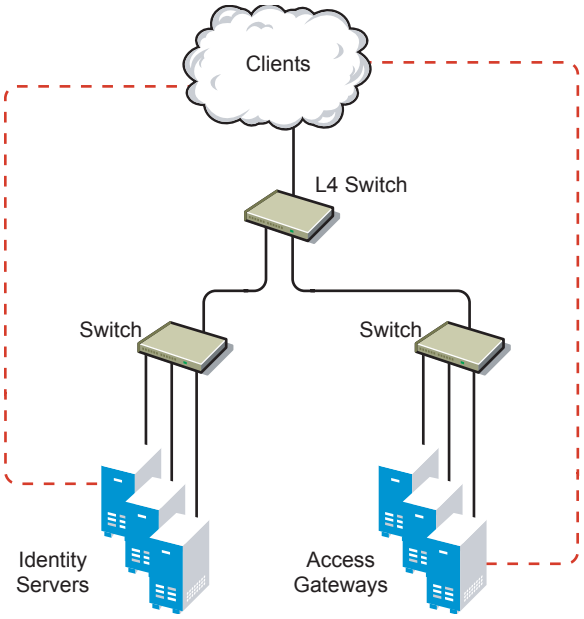
When setting up the L4 switch, be aware of the following configuration requirements that are required to route all Access Manager traffic through the L4 switch.

Switches: When installing an L4 switch, you can plug the machines directly into the L4 switch or plug them into an inner switch that is plugged into the L4 switch. When using inner switches with an

L4 switch, you must use at least two inner switches, one for the Identity Servers and one for the Access Gateways. An Identity Server and an Access Gateway cannot share the same inner switch. Such a configuration causes communication problems because the Access Gateway and the Identity Server try to establish direct communication with each other rather than routing all traffic through the L4 switch.

Network Routing Requirements: You need to analyze your routing configuration. The Identity Servers and the Access Gateways must have only one route to the network, and this route must be through the L4 switch. If you have loops in your network that allow an Identity Server or an Access Gateway to communicate directly with a client without going through the L4 switch, the Access Gateway and the Identity Server try to establish direct communication with the client. Such a configuration causes communication problems because all traffic needs to be routed through the L4 switch. Figure 4-3 illustrates this problem.

Figure 4-3 *Network Configuration with a Potential Communication Problem*



If your network allows for this type of communication, you need to block the communication channels illustrated with the dotted red lines.

4.4.3 Health Checks

L4 switches use health checks to determine which cluster members are ready to receive requests and which cluster members are unhealthy and should not receive requests. You need to configure the L4 switch to monitor the heartbeat URL of the Identity Servers and Access Gateways, so that the L4 switch can use this information to accurately update the health status of each cluster member.

The procedure is slightly different for Identity Servers and Access Gateways:

- “Health Checks for an Identity Server” on page 58
- “Health Checks for the Access Gateway” on page 58

Health Checks for an Identity Server

The Administration Console uses the heartbeat URL to display the health status of the Identity Servers. The Identity Server heartbeat is the DNS name of the Identity Server plus the following path:

```
/nidp/app/heartbeat
```

L4 switches require you to use IP address rather than the DNS name. If the IP address of the Identity Server is 10.10.16.50, and you have configured the Identity Server for HTTPS, the heartbeat has the following URL:

```
https://10.10.16.50:8443/nidp/app/heartbeat
```

You need to configure the L4 switch to use this heartbeat to perform a health check. If you have configured SSL on the Identity Servers and your L4 switch has the ability to do an SSL L7 health check, you can use HTTPS. The SSL L7 health check returns a value of `200 OK`, indicating everything is healthy; any other status code indicates an unhealthy state.

For a Foundry switch, the L7 health check script string should look similar to the following when the hostname is nidp1 and the IP address is 10.10.16.50:

```
healthck nidp1ssl tcp
  dest-ip 10.10.16.50
  port ssl
  protocol ssl
  protocol ssl url "GET /nipd/app/heartbeat HTTP/1.1\r\nHost:
st160.lab.tst"
  protocol ssl status-code 200 200
  l7-check
```

If your switch does not support an SSL L7 health check, the HTTPS URL returns an error, usually a 404 error. Because the Identity Server heartbeat URL listens on both HTTPS and HTTP, you can use an HTTP URL for switches that do not support the SSL L7 health check. For example:

```
http://10.10.16.50:8080/nidp/app/heartbeat
```

An Alteon switch does not support the L7 health check, so the string for the health check should look similar to the following:

```
open 8080,tcp
send GET /nidp/app/heartbeat HTTP/1.1\r\nHOST:heartbeat.lab.tst
\r\n\r\n
expect HTTP/1.1 200
close
```

Health Checks for the Access Gateway

External communication to the Access Gateway is typically configured to use HTTPS. In an HTTPS configuration, an L4 performs health checks of the Access Gateways with the published DNS name of the Access Gateway plus the following path:

```
/nesp/app/heartbeat
```

L4 switches require you to use IP address rather than the DNS name. If the IP address of the Access Gateway is 10.10.16.172, and you have configured the Access Gateway for HTTPS, the heartbeat has the following URL:

```
https://10.10.16.172:443/nesp/app/heartbeat
```

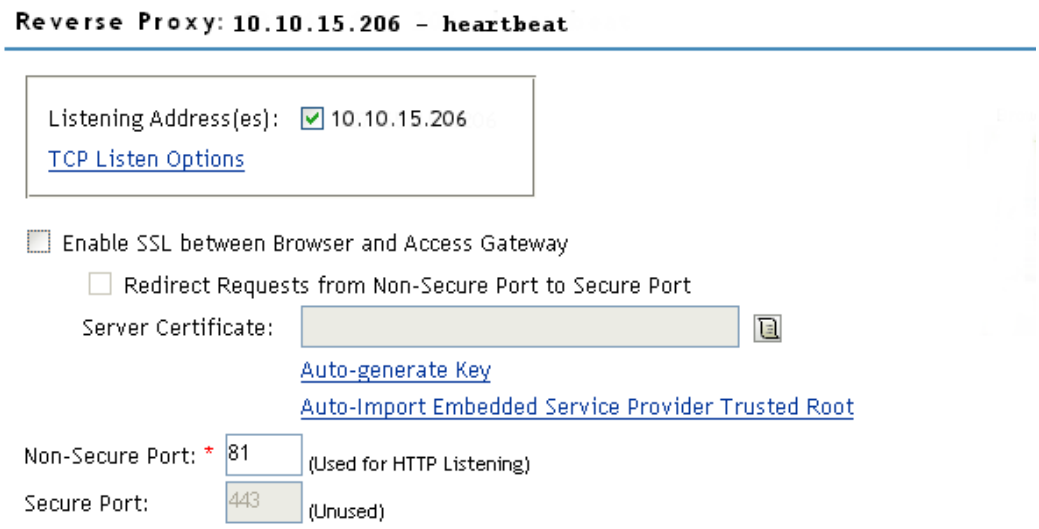
For a Foundry switch, the L7 health check script string should look similar to the following when the hostname is ag1 and the IP address is 10.10.172.

```
healthck ag1ssl tcp
  dest-ip 10.10.16.172
  port ssl
  protocol ssl
  protocol ssl url "GET /nesp/app/heartbeat HTTP/1.1\r\nHost:
st160.lab.tst"
  protocol ssl status-code 200 200
  l7-check
```

An Access Gateway configured for HTTPS listens only on the SSL port. If your L4 switch does not support an SSL L7 health check, the HTTPS health check URL returns an error, usually a 404 error. To solve this problem, you can create a specialized reverse proxy that opens a non-SSL port for the heartbeat URL.

To create a heartbeat reverse proxy:

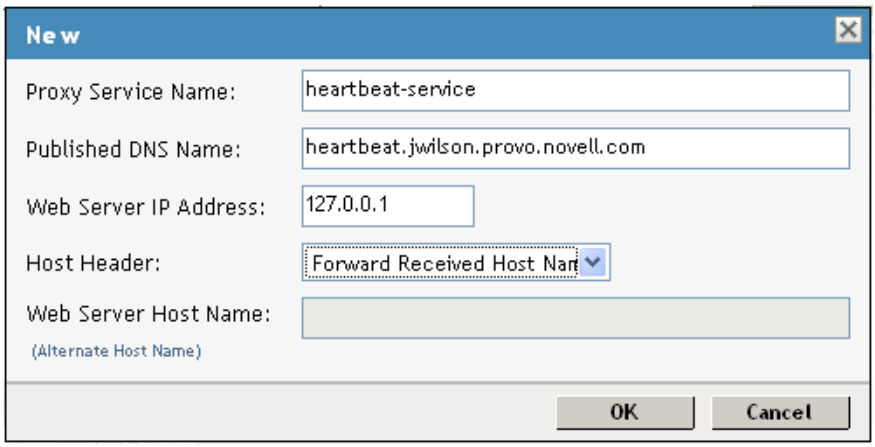
1. In the Administration Console, click *Access Manager* > *Access Gateways* > *Edit* > *Reverse Proxy / Authentication*.
2. To create an additional reverse proxy service (such as *heartbeat*), click *New*, then specify a name.



3. Change the *Non-Secure Port* to 81.

   You configure the Access Gateway to listen on the same IP address as the service using port 443. For non-SSL, port 81 is recommended. Do not use port 80.

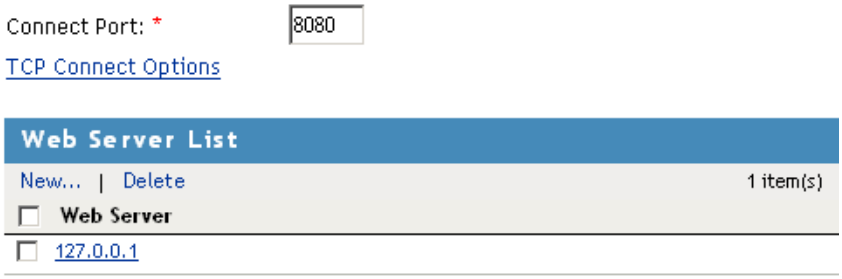
   For proper heartbeat information when there are multiple IP addresses configured in your Access Gateway, ensure that you configure the reverse proxy service created for the heartbeat URL to listen in the same IP address as the authenticating reverse proxy service.
4. Click *New* to create the proxy service.



For the *Published DNS Name*, specify a DNS name that your DNS server resolves to the Access Gateway.

5 Configure the *Web Server IP* address to be 127.0.0.1, then click *OK*.

6 On the Reverse Proxy page, click the new proxy service, then click *Web Servers*.



7 Change the *Connect Port* value on the Web Servers page to 8080.

The service provider (ESP) in Access Gateway that provides the heartbeat service listens on 127.0.0.1:8080.

8 Click *Protected Resources*.

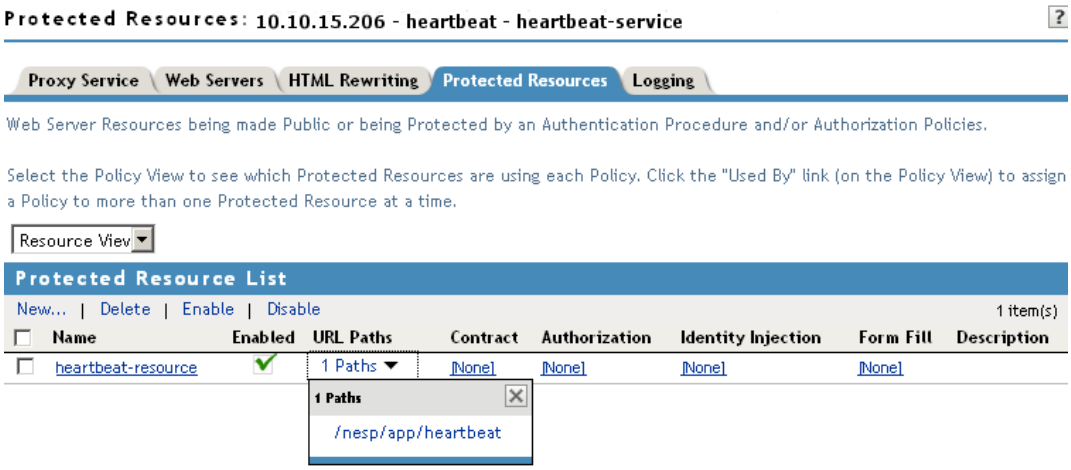
9 Click *New*, then specify a name.

10 In the URL Path List, click /*, and modify the path to contain the following value:

```
/nesp/app/heartbeat
```

This is the path to the heartbeat application.

11 Click *OK* twice. Your protected resource for the heartbeat application should look similar to the example below.



The heartbeat of this Access Gateway is available from the following URL (See Step 4.):

```
http://heartbeat.jwilson.provo.novell.com:81/nesp/app/heartbeat
```

If the protected resource is configured with a path of / or /*, the solution works but it can be vulnerable to attacks because the configuration opens the ESP over a non-SSL port. Restricting the resource to `/nesp/app/heartbeat` automatically denies access to the ESP except for the heartbeat.

12 Click *OK* and apply the changes to the configuration.

13 Add a line similar to the following to the health check script:

For a Foundry switch, your string should look similar to the following if the hostname is ag1 and the IP address is 10.10.16.172:

```
healthck ag1 tcp
  dest-ip 10.10.16.172
  port http
  protocol http
  protocol http url "GET /nesp/app/heartbeat HTTP/
1.1\r\nHost:st160.lab.tst"
  protocol http status-code 200 200
  l7-check
```

For an Alteon switch, your string should look similar to the following if the hostname is ag1 and the IP address is 10.10.16.172:

```
open 81,tcp
send GET /nesp/app/heartbeat HTTP/1.1\r\nHOST:heartbeat.lab.
tst\r\n\r\n
expect HTTP/1.1 200
close
```

4.4.4 Real Server Settings Example

After setting up the health checks, you need to configure the real server settings. The following is an example from a Foundry switch.

```
Current real servers settings:
  1: 149.44.171.116, enabled, name l52, weight 1, timeout 10 mins, maxcon 200000
    backup none, inter 2, retry 4, restr 8
    remote disabled, proxy enabled, subnac disabled
    cookie assignment server: disabled
    exclusionary string matching: disabled
    service ports: 8443 8080
    real ports:
      8443: vport 8443, group 1, pbind clientip
          virtual server:  1, 149.44.174.220,  enabled
      8080: vport 8080, group 1, pbind clientip
          virtual server:  1, 149.44.174.220,  enabled
  2: 149.44.174.51, enabled, name brie, weight 1, timeout 10 mins, maxcon 200000
    backup none, inter 2, retry 4, restr 8
    remote disabled, proxy enabled, subnac disabled
    cookie assignment server: disabled
    exclusionary string matching: disabled
    service ports: 8443 8080
    real ports:
      8443: vport 8443, group 1, pbind clientip
          virtual server:  1, 149.44.174.220,  enabled
      8080: vport 8080, group 1, pbind clientip
          virtual server:  1, 149.44.174.220,  enabled
```

4.4.5 Virtual Server Settings Example

After setting up the real server settings, you need to configure the virtual server settings. The following is an example from a Foundry switch.

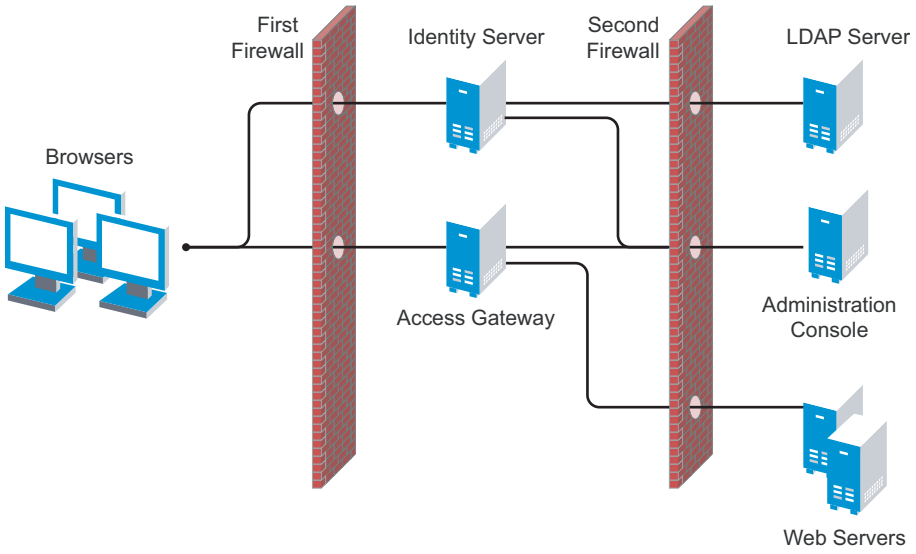
```
Current virtual servers settings:
  1: 149.44.174.220, enabled, dname idp
    virtual ports:
      8443: rport 8443, group 1, pbind clientip, frags
          real servers:
             1: 149.44.171.116,  weight 1,  enabled, backup none
             2: 149.44.174.51,   weight 1,  enabled, backup none
      8080: rport 8080, group 1, pbind clientip, frags
          real servers:
             1: 149.44.171.116,  weight 1,  enabled, backup none
             2: 149.44.174.51,   weight 1,  enabled, backup none
```

Setting Up Firewalls

5

Access Manager is not a firewall; it should be used with firewalls. Figure 5-1 illustrates a simple firewall set up for a basic Access Manager configuration of an Identity Server, an Access Gateway, and an Administration Console.

Figure 5-1 *Access Manager Components between Firewalls*



The first firewall separates the Access Manager components from the Internet, allowing browsers to access the resources through specific ports. The second firewall separates the Access Manager components from the Web servers they are protecting and the Administration Console. This is one of many configurations possible. This section describes the following:

- Section 5.1, “Required Ports,” on page 63
- Section 5.2, “Sample Configurations,” on page 71

5.1 Required Ports

The following tables list the ports that need to be opened when a firewall separates one component from another. Some combinations appear in more than one table, but this allows you to discover the required ports whether you are thinking that a firewall is separating an Access Gateway from the Administration Console or that a firewall is separating an Administration Console from the Access Gateway.

With these tables, you should be able to place the Access Manager components of your system anywhere within your existing firewalls and know which ports need to be opened in the firewall.

- Table 5-1, “When a Firewall Separates an Access Manager Component from a Global Service,” on page 64
- Table 5-2, “When a Firewall Separates the Administration Console from a Component,” on page 64

- Table 5-3, “When a Firewall Separates the Identity Server from a Component,” on page 65
- Table 5-4, “When a Firewall Separates the Access Gateway from a Component,” on page 67
- Table 5-5, “When a Firewall Separates the SSL VPN from a Component,” on page 68
- Table 5-6, “When a Firewall Separates the J2EE Agent from a Component,” on page 70

Table 5-1 *When a Firewall Separates an Access Manager Component from a Global Service*

Component	Port	Description
NTP Server	UDP 123	Access Manager components must be synchronized or authentication fails. We highly recommend that all components be configured to use an NTP (network time protocol) server. Depending upon where your NTP server is located in relationship to your firewalls, you might need to open UDP 123 so that the Access Manager component can use the NTP server.
DNS Servers	UDP 53	Access Manager components must be able to resolve DNS names. Depending upon where your DNS servers are located, you might need to open UDP 53 so that the Access Manager component can resolve DNS names.
Remote Administration Workstation	TCP 22	If you use SSH for remote administration and want to use it for remote administration of Access Manager components, you need to open TCP 22 to allow communication from your remote administration workstation to your Access Manager components.

Table 5-2 *When a Firewall Separates the Administration Console from a Component*

Component	Port	Description
Access Gateway, Identity Server, SSL VPN, or J2EE Agent	TCP 1443	For communication from the Administration Console to the devices.
	TCP 8444	For communication from the devices to the Administration Console.
	TCP 289	For communication from the devices to the Novell® Audit server on the Administration Console.
	TCP 524	For NCP™ certificate management with NPKI. The port needs to be opened so that both the device and the Administration Console can use the port.
	TCP 636	For secure LDAP communication from the devices to the Administration Console.

Component	Port	Description
Importing a Linux Access Gateway	ICMP	During an import, the Linux Access Gateway sends two ICMP pings to the Administration Console. When the import has finished, you can close this port.
LDAP User Store	TCP 524	Required only if the user store is eDirectory™. When configuring a new eDirectory user store, NCP is used to enable SecretStore by adding a SAML authentication method and storing a public key for the Administration Console. It is not used in day-to-day operations.
Administration Console	Not a supported configuration. The primary and secondary consoles need to be on the same side of the firewall.	
Browsers	TCP 8080	For HTTP communication from the browsers to the Administration Console.
	TCP 8443	For HTTPS communication from the browsers to the Administration Console.
	TCP 8028, 8030	To use iMonitor or DSTrace from a client to view information about the configuration store on the Administration Console.

Table 5-3 *When a Firewall Separates the Identity Server from a Component*

Component	Port	Description
Access Gateway	TCP 8080 or 8443	For authentication communication from the Access Gateway to the Identity Server and from the Identity Server to the Access Gateway. TCP 8080 and 8443 are the default ports. They are configurable. You need to open the port of the Base URL of the Identity Server.
SSL VPN	N/A. The SSL VPN never communicates directly with the Identity Server.	
J2EE Agent	TCP 8080 or 8443	For authentication communication from the J2EE Agent to the Identity Server. TCP 8080 and 8443 are the default ports. They are configurable. You need to open the port of the Base URL of the Identity Server. See "Translating the Identity Server Configuration Port" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

Component	Port	Description
Administration Console	TCP 1443	For communication from the Administration Console to the devices. This is configurable.
	TCP 8444	For communication from the Identity Server to the Administration Console.
	TCP 289	For communication from the Identity Server to the Novell Audit server on the Administration Console.
	TCP 524	For NCP certificate management with NPKI from the Identity Server to the Administration Console.
	TCP 636	For secure LDAP communication from the Identity Server to the Administration Console.
Identity Server	Not a supported configuration. All members of a cluster must be on the same side of the firewall.	
LDAP User Stores	TCP 636	For secure LDAP communication from the Identity Server to the LDAP user store.
Service Providers	TCP 8445	If you have enabled Identity Provider introductions, you need to open a port to allow HTTPS communication from the user's browser to the service provider.
	TCP 8446	If you have enabled Identity Provider introductions, you need to open a port to allow HTTPS communication from the user's browser to the service consumer.
Browsers	TCP 8080	For HTTP communication from the browser to the Identity Server. You can use iptable to configure this for TCP 80. See "Translating the Identity Server Configuration Port" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.
	TCP 8443	For HTTPS communication from the browser to the Identity Server. You can use iptable to configure this for TCP 443. See "Translating the Identity Server Configuration Port" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

Table 5-4 *When a Firewall Separates the Access Gateway from a Component*

Component	Port	Description
Identity Server	TCP 8080 or 8443	For authentication communication from the Access Gateway to the Identity Server. TCP 8080 and 8443 are the default ports. They are configurable. You need to open the port of the Base URL of the Identity Server. See "Translating the Identity Server Configuration Port" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.
Administration Console	TCP 1443	For communication from the Administration Console to the Access Gateway. This is configurable.
	TCP 8444	For communication from the Access Gateway to the Administration Console.
	TCP 289	For communication from the Access Gateway to the Novell Audit server on the Administration Console.
	TCP 524	For NCP certificate management with NPKI from the Access Gateway to the Administration Console.
	TCP 636	For secure LDAP communication from the Access Gateway to the Administration Console.
SSL VPN	TCP 8080	For HTTP communication from the Access Gateway to the SSL VPN.
	TCP 8443	If SSL has been enabled between the Access Gateway and the SSL VPN, TCP 8443 needs to be opened for HTTPS communication from the Access Gateway to the SSL VPN.
J2EE Agent	Only required if the Access Gateway is configured to protect the J2EE server as a Web server.	
	TCP 8080, 8443	For communication from the Access Gateway to the JBoss* server. These are the default ports. They are configurable.
	TCP 9080, 9443	For communication from the Access Gateway to the WebSphere* server. These are the default ports. They are configurable.
	TCP 7001, 7002	For communication from the Access Gateway to the WebLogic* server. These are the default ports. They are configurable.
Access Gateway	Not a supported configuration. All members of an Access Gateway group need to be on the same side of the firewall.	

Component	Port	Description
Browsers/Clients	TCP 80	For HTTP communication from the client to the Access Gateway. This is configurable.
	TCP 443	For HTTPS communication from the client to the Access Gateway. This is configurable.
	UDP 8880	For RDB communication from the client to the Access Gateway. Only required if you enable RDB on the NetWare® Access Gateway
	TCP 23	For Telnet communication from the client to the Access Gateway. Only required if you enable Telnet on the NetWare Access Gateway.
	TCP 21	For FTP communication from the client to the Access Gateway. Only required if you enable Mini FTP on the NetWare Access Gateway.
	TCP 524	For SFTP communication from the client to the Access Gateway. Only required if you load the `ncpip.nlm` for SFTP on the NetWare Access Gateway.
Web Servers	TCP 80	For HTTP communication from the Access Gateway to the Web servers. This is configurable.
	TCP 443	For HTTPS communication from the Access Gateway to the Web servers. This is configurable.

Table 5-5 *When a Firewall Separates the SSL VPN from a Component*

Component	Port	Description
Access Gateway	TCP 8080	For HTTP communication from the Access Gateway to the SSL VPN.
	TCP 8443	If SSL has been enabled between the Access Gateway and the SSL VPN, TCP 8443 needs to be opened for HTTPS communication from the Access Gateway to the SSL VPN.
Identity Server	N/A. The SSL VPN never communicates directly with the Identity Server.	

Component	Port	Description
Administration Console	TCP 1443	For communication from the Administration Console to the SSL VPN. This is configurable.
	TCP 8444	For communication from the SSL VPN to the Administration Console.
	TCP 289	For communication from the SSL VPN to the Novell Audit server on the Administration Console.
	TCP 524	For NCP certificate management with NPKI from the SSL VPN to the Administration Console.
	TCP 636	For secure LDAP communication from the SSL VPN to the Administration Console.
J2EE Agent	N/A. The SSL VPN never communicates with the J2EE Agent.	
Browsers	TCP 7777 UDP 7777	This is the default port for access to the SSL VPN, but it can be configured to use TCP 443 and UDP 443.
SOCKS server	TCP 2010	For SOCKS communication from the SSL VPN to the SOCKS server. This port is configurable.
Application Servers (E-mail, Telnet, Thin Client, etc.)	TCP 22	For SSH communication from the SSL VPN to the application server.
	TCP 23	For Telnet communication from the SSL VPN to the application server.
	Application ports	Specific to the application that SSL VPN is providing access to.
Firewall on same machine as the SSL VPN	tun0	SSL VPN creates a tunnel that needs to be open on the internal networks list of the machine. For configuration information, see the following Note.

NOTE: If you are running the SSL VPN on SLES 9 with a firewall, you cannot use YaST to configure the firewall for access to UDP ports and internal networks. You need to edit the `/etc/sysconfig/SuSEfirewall2` file and add lines similar to the following:

```
FW_SERVICES_EXT_UDP=7777
FW_DEV_INT=tun0
```

On SLES 10, you can edit this file or use YaST to configure UDP ports and internal networks.

Table 5-6 *When a Firewall Separates the J2EE Agent from a Component*

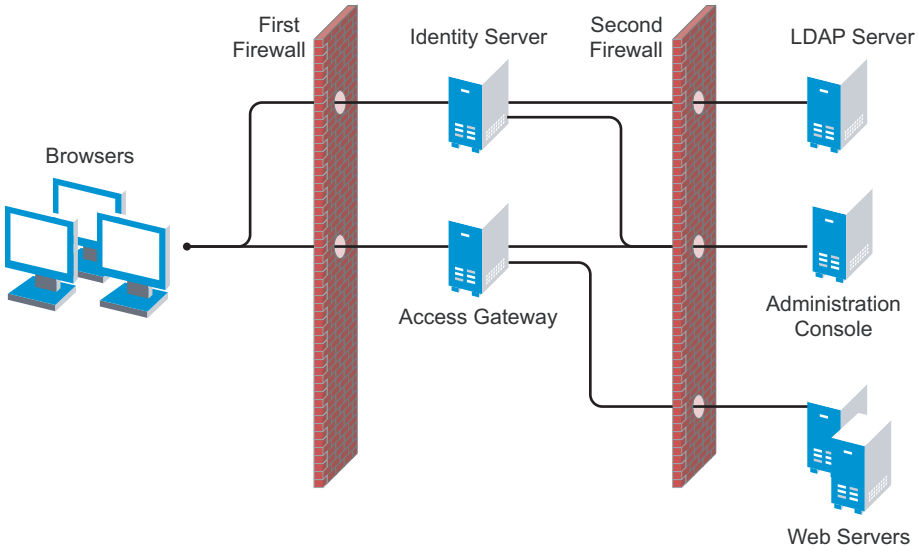
Component	Port	Description
Administration Console	TCP 1443	For communication from the Administration Console to the J2EE Agent. This is configurable.
	TCP 8444	For communication from the J2EE Agent to the Administration Console.
	TCP 289	For communication from the J2EE Agent to the Novell Audit server on the Administration Console.
	TCP 524	For NCP certificate management with NPKI from the J2EE Agent to the Administration Console.
	TCP 636	For secure LDAP communication from the J2EE Agent to the Administration Console.
Identity Server	TCP 8080 or 8443	For authentication communication from the J2EE Agent to the Identity Server and from the Identity Server to the J2EE Agent. TCP 8080 and 8443 are the default ports. They are configurable. You need to open the port of the Base URL of the Identity Server. See "Translating the Identity Server Configuration Port" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.
Access Gateway	Only required if the Access Gateway is configured to protect the J2EE server as a Web server.	
	TCP 8080, 8443	For communication from the Access Gateway to the JBoss server. These are the default ports. They are configurable.
	TCP 9080, 9443	For communication from the Access Gateway to the WebSphere server. These are the default ports. They are configurable.
	TCP 7001, 7002	For communication from the Access Gateway to the WebLogic server. These are the default ports. They are configurable.
SSL VPN	N/A. The J2EE Agent never communicates with the SSL VPN.	
Browsers	TCP 8080, 8443	For communication from the browser to the JBoss server. These are the default ports. They are configurable.
	TCP 9080, 9443	For communication from the browser to the WebSphere server. These are the default ports. They are configurable.
	TCP 7001, 7002	For communication from the browser to the WebLogic server. These are the default ports. They are configurable.

5.2 Sample Configurations

- Section 5.2.1, “The Access Gateway and Identity Server in the DMZ,” on page 71
- Section 5.2.2, “A Firewall Separating Access Manager Components from the LDAP Servers,” on page 72
- Section 5.2.3, “Configuring the Firewall for the SSL VPN Server,” on page 73
- Section 5.2.4, “Configuring the Firewall for the J2EE Agent,” on page 74

5.2.1 The Access Gateway and Identity Server in the DMZ

Figure 5-2 *The Identity Server and the Access Gateway in the DMZ*



First Firewall

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

Table 5-7 *Ports to Open in the First Firewall*

Port	Purpose
TCP 80	For HTTP communication.
TCP 443	For HTTPS communication.
Any TCP port assigned to a reverse proxy or tunnel.	

Port	Purpose
TCP 8080	For HTTP communication with the Identity Server. For information about redirecting the Identity Server to use port 80, see "Translating the Identity Server Configuration Port" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.
TCP 8443	For HTTPS communication with the Identity Server. For information about redirecting the Identity Server to use port 443, see "Translating the Identity Server Configuration Port" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.
TCP 8445	For HTTP Identity Provider introductions. If you do not enable Identity Provider introductions, you do not need to open this port. For more information about this option, see the *Use Introductions* option in "Creating a Cluster Configuration" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.
TCP 8446	For HTTPS Identity Provider introductions. If you do not enable Identity Provider introductions, you do not need to open this port. For more information about this option, see the *Use Introductions* option in "Creating a Cluster Configuration" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

Second Firewall

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

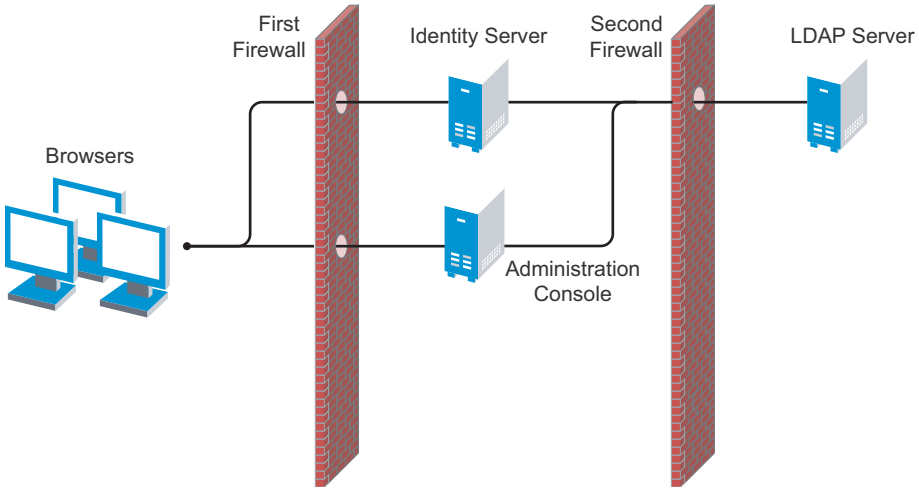
Table 5-8 *Ports to Open in the Second Firewall*

Port	Purpose
TCP 80	For HTTP communication with Web servers.
TCP 443	For HTTPS communication with Web servers.
Any TCP connect port assigned to a Web server or to a tunnel.	
TCP 1443	For communication from the Administration Console to the devices.
TCP 8444	For communication from the devices to the Administration Console.
TCP 289	For communication from the devices to the Novell Audit server installed on the Administration Console. If you do not enable auditing, you do not need to open this port.
TCP 524	For NCP certificate management in NPKI. The port needs to be opened so that both the device and the Administration Console can use the port.
TCP 636	For secure LDAP communication of configuration information.

5.2.2 A Firewall Separating Access Manager Components from the LDAP Servers

You can configure your Access Manager components so that your Administration Console is on the same side of the firewall as your Access Manager components and have a firewall between them and the LDAP servers, as illustrated in Figure 5-3.

Figure 5-3 *A Firewall Separating the Administration Console and the LDAP Server*



In this configuration, you need to have the following ports opened in the second firewall for the Administration Console and the Identity Server.

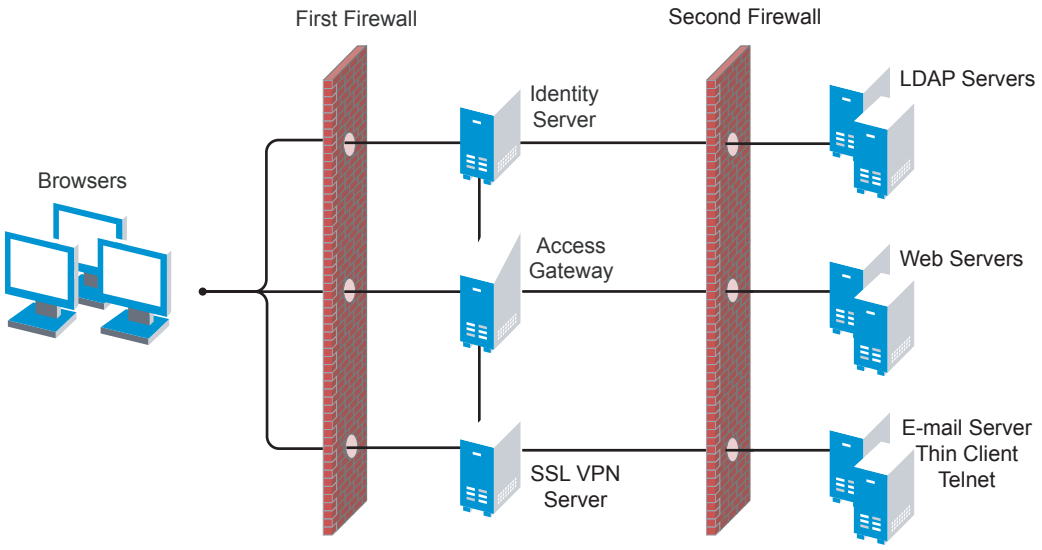
Table 5-9 *Ports to Open in the Second Firewall*

Ports	Purpose
TCP 636	For secure LDAP communication. This is used by the Identity Server and the Administration Console.
TCP 524	For configuring eDirectory as a new User Store. NCP is used to enable SecretStore by adding a SAML authentication method and storing a public key for the Administration Console. During day-to-day operations, this port is not used. If your LDAP server is Active Directory or Sun ONE, this port does not need to be opened.

5.2.3 Configuring the Firewall for the SSL VPN Server

The SSL VPN server can be installed as a separate machine or as a component running on the Linux Access Gateway. Although it is configured to be a protected resource of the Access Gateway, it also allows direct communication with the client browsers.

Figure 5-4 *SSL VPN Server and Firewalls*



The SSL VPN server needs the following port opened on the first firewall if clients are accessing the SSL VPN server directly:

Table 5-10 *Ports to Open in the First Firewall for SSL VPN*

Port	Purpose
TCP 7777	For client communication. This is the default port, but it can be configured to use TCP 443.

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

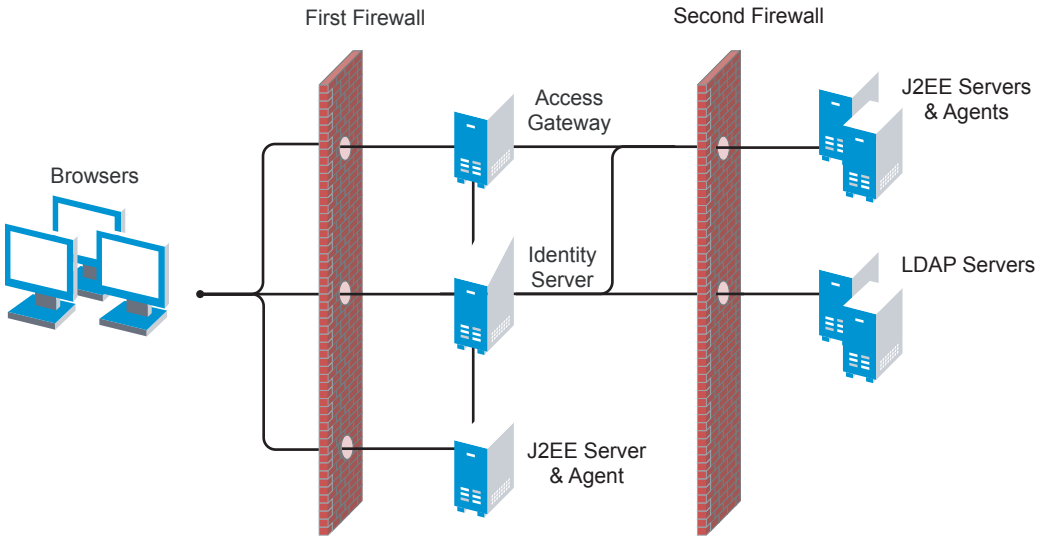
Table 5-11 *Ports to Open in the Second Firewall for SSL VPN*

Port	Purpose
TCP 22	For SSH.
TCP 23	For Telnet.
Ports specific to an application.	

5.2.4 Configuring the Firewall for the J2EE Agent

The J2EE Agent is installed on a J2EE server running JBoss, WebLogic, or WebSphere. You can configure it to be a protected resource of the Access Gateway or you can allow direct access. Figure 5-5 illustrates these configurations.

Figure 5-5 *J2EE Agent and Firewalls*



If the J2EE server is installed behind the first firewall and browsers are allowed direct access to it, the following ports need to be opened in the first firewall:

Table 5-12 *Ports to Open in the First Firewall for the J2EE Agent*

Port	Purpose
TCP 8080	For non-secure connections to a JBoss server.
TCP 8443	For secure connections to a JBoss server.
TCP 9080	For non-secure connections to a WebSphere server.
TCP 9443	For secure connections to a WebSphere server.
TCP 7001	For non-secure connections to a WebLogic server.
TCP 7002	For secure connections to a WebLogic server.

If the J2EE server is installed behind the second firewall, the following ports need to be opened in the second firewall:

Table 5-13 *Ports to Open in the Second Firewall for the J2EE Agent*

Port	Purpose
TCP 8080	For non-secure connections to a JBoss server.
TCP 8443	For secure connections to a JBoss server.
TCP 9080	For non-secure connections to a WebSphere server.
TCP 9443	For secure connections to a WebSphere server.
TCP 7001	For non-secure connections to a WebLogic server.

Port	Purpose
TCP 7002	For secure connections to a WebLogic server.
TCP 8080 or 8443	For authentication communication. The port of the Base URL of the Identity Server needs to be open.

Setting Up Federation

6

Federation allows a user to associate two accounts with each other. This allows the user to log into one account and have access to the resources of the other account without logging in to the second account. It is one method for providing single sign-on when a user has accounts in multiple user stores.

This section explains the following federation tasks:

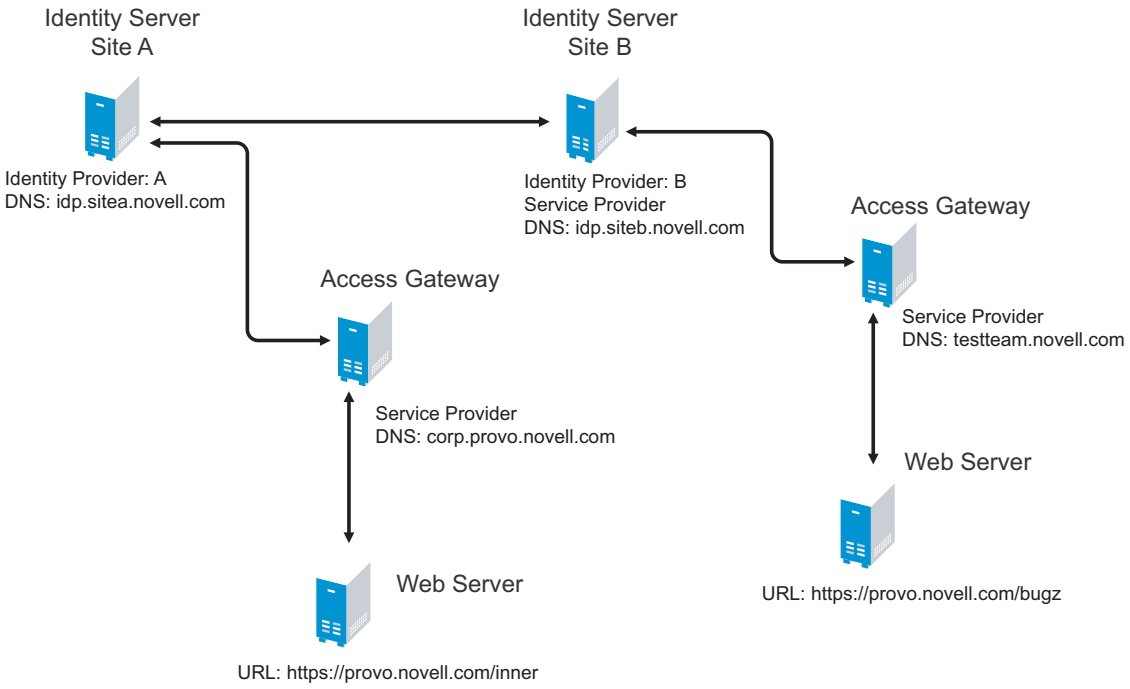
- Section 6.1, “Understanding a Simple Federation Scenario,” on page 77
- Section 6.2, “Configuring Federation,” on page 78
- Section 6.3, “Sharing Roles,” on page 89
- Section 6.4, “Setting Up Federation with Third-Party Providers,” on page 96

6.1 Understanding a Simple Federation Scenario

Suppose Company A has a centralized user store that does the authentication for most of the company’s internal resources on its inner Web site. But Company A also has a customer feedback application that employees and customers need access to, and for this application, a second user store has been created. This user store contains both employee and customer user accounts. The centralized user store can’t be used, because it can contain only employee accounts. This means that the employee must log in to both accounts to access both the inner Web site and the customer feedback application. With federation, the employee can access the resources of both sites by using a single login.

Figure 6-1 illustrates such a network configuration where the user accounts of Site A are configured to federate with the user accounts at Site B.

Figure 6-1 *Using Federated Identities*



In this configuration, Site A is the Identity Server for the corporate resources, and the employees authenticate to this site and have access to the resources on the Web server with the URL of https://provo.novell.com/inner. Site B is the Identity Server for the Bugzilla application, and both employees and customers authenticate to this site to have access to the resources of the Web server with the URL of https://provo.novell.com/bugz. After an account has been federated, the user can log in to Site A and have access to the resources on the Web servers of both Site A and Site B.

In this scenario, Site B is not as secure a site as Site A, so federation is configured to go only one way, from Site A to Site B. This means that users who log in to Site A have access to the resources at Site A and B, but users who log in to Site B have access only to the resources at Site B. Federation can be configured to go both ways, so that it doesn't matter whether the user logs into Site A or Site B. When federation is configured to be bidirectional, both sites need to be equally secure.

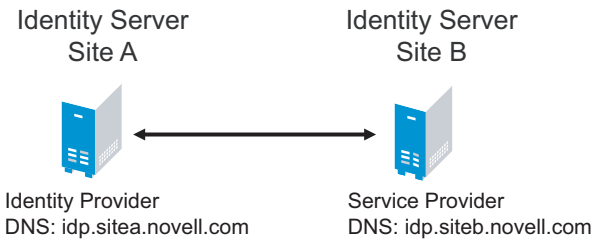
The Access Gateways in Figure 6-1 are service providers and are configured to use the Identity Servers as identity providers. The trusted relationship is automatically set up for you when you specify authentication settings for the Access Gateway and select an Identity Server Cluster.

Federation can be set up between providers in the same company or between providers of separate companies. For example, most companies have contracts with other companies for their user's health benefits and retirement accounts. Their users have accounts with these companies.These accounts can be federated with the user's employee account when both companies agree to set up the trusted relationship.

6.2 Configuring Federation

Federation requires the configuration of a trusted relationship between an identity provider and a service provider. Figure 6-2 illustrates setting up federation between two Identity Servers, because a Novell Identity Server can act as either an identity provider or a service provider.

Figure 6-2 *Configuring Trust Between Site A and Site B*



Site A must be configured to trust Site B as a service provider, and Site B must be configured to trust Site A as an identity provider. Until this two-way trust is established, federation cannot occur.

Before setting up a trusted relationship, you must make the following decisions:

Protocol: The Identity Server supports SAML 1.1, SAML 2.0, and Liberty. You need to decide which of these protocols to use. If no user interaction is needed, SAML 1.1 is probably a good choice. The SAML 2.0 and Liberty protocols permit user interaction when federating. The user decides whether to federate (link) the accounts and must be logged in at both sites to accomplish this. Liberty offers an additional service, not available with SAML 2.0, that allows the user to select attributes that can be shared with the service provider.

The instructions in this documentation, starting in Section 6.2.1, “Prerequisites,” on page 80, use the Liberty protocol. They also indicate how to configure for the SAML 2.0 and SAML 1.1 protocols.

Trust Relationship: You need to decide whether the trusted relationship is going to be from Site A to Site B, from Site B to Site A, or bidirectional from Site A to Site B and from Site B to Site A. Federation is set up to go from the most secure site to the less secure site. The only time federation is set up to be bidirectional is when both sites are equally secure. The scenario described in Figure 6-1 on page 78 is an example of a trusted relationship that you would want to go only one way, from Site A to Site B, because Site B is not as secure as Site A.

The instructions, starting in Section 6.2.1, “Prerequisites,” on page 80, explain how to set up the trusted relationship between Site A and Site B. You can easily modify them to set up the bidirectional trust relationships by substituting Site B for Site A (and vice versa) in the instructions and then repeating them for Site B

Attributes to Share: You need to decide whether there are user attributes or roles at Site A that you want to share with Site B. The attributes from Site A can be used to identify the users at Site B. Other attributes might be needed to access protected resources, for example, to satisfy the requirements of an Identity Injection policy.

For all the protocols, Section 6.3, “Sharing Roles,” on page 89 explains how to share the roles at Site A with Site B. For the SAML 1.1 protocol, the instructions starting in Section 6.2.1, “Prerequisites,” on page 80 use the LDAP mail attribute to share the user’s e-mail address.

User Identification: You need to decide how assertions can be used to map users from Site A to users at Site B. The Identity Server supports four methods.

- **Temporary:** This method allows the user access to Site B solely from the credentials of Site A. No effort is made to map the user to a user account at Site B. A temporary account is set up for the user on Site B, and when the user logs out, the account is destroyed.
- **Login:** This method requires that the user have login credentials at both Site A and Site B, and when logged in at both sites, the user can select to federate the accounts.

- **Mapped Attributes:** This method requires that the sites share attributes and that these attributes are used to create a matching expression that determines whether the user accounts match. For an added security check, the first time the accounts are matched, the user is asked to verify the match by supplying the password for Site B.

  If the match fails, you can allow the federation to fail or configure the method to allow the user to use the Login method or the Provisioning method.
- **Provisioning:** This method allows the user to create a new, permanent account at Site B.

The configuration instructions, starting in Section 6.2.1, "Prerequisites," on page 80, use the Login method for the SAML 2.0 and Liberty protocols and Mapped Attributes method for the SAML 1.1 protocol.

The instruction for setting up a trusted relationship between two Novell Identity Servers have been divided as follows:

- Section 6.2.1, "Prerequisites," on page 80
- Section 6.2.2, "Establishing Trust between Providers," on page 80
- Section 6.2.3, "Configuring SAML 1.1 for Account Federation," on page 86

6.2.1 Prerequisites

- ❑ A basic Access Manager configuration with the Identity Server and Access Gateway configured for SSL.

  This can be one you set up using the instructions in either Chapter 1, "Setting Up a Basic Access Manager Configuration," on page 11 or Chapter 7, "Digital Airlines Example," on page 97. For SSL configuration, see Chapter 3, "Enabling SSL Communication," on page 33.

  The Identity Server from this configuration becomes Site B in Figure 6-2.
- ❑ A second Identity Server with a basic configuration, an LDAP user store, and SSL. This Identity Server is configured to be Site A in Figure 6-2.
- ❑ Time synchronization must be set up for all the machines, or authentication can fail if assertions expire before they can be used.
- ❑ A DNS server must be configured to resolve the DNS names of Site A, Site B, and the Access Gateways.
- ❑ (Recommended) Logging has been enabled on the Identity Servers of Site A and Site B. See "Configuring Identity Server Logging" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*. Make sure that you enable at least Application logging at an Info level.

6.2.2 Establishing Trust between Providers

To set up this very basic example of federation, complete the following tasks.

- "Configuring Site A to Trust Site B as a Service Provider" on page 81
- "Configuring Site B to Trust Site A as an Identity Provider" on page 82
- "Verifying the Trust Relationship" on page 83
- "Configuring User Authentication" on page 84

Configuring Site A to Trust Site B as a Service Provider

To establish trust between Site A and Site B, you must perform two tasks:

- The providers must trust the certificates of each other so you need to import the trusted root certificate of Site B to Site A.
- You must also import the metadata of Site B to Site A. The metadata allows Site A to verify that Site B is truly Site B when Site B sends a request to Site A.

The following instructions explain how to import the certificate and the metadata:

1. Log in to the Administration Console for Site A.

   The configuration for Site A can be created in the same Administration Console as Site B; it cannot be configured to be a cluster member of Site B.

2. In the Administration Console, click *Access Manager* > *Identity Servers* > *Edit* > *Security* > *NIDP Trust Store*.

3. In the Trusted Roots section, click *Auto-Import From Server*, then fill the following fields:

   Server IP/DNS: Specify the IP address or DNS name of Site B. For Site B in Figure 6-2 specify the following:

   `idp.siteb.novell.com`

   Server Port: Specify 8443.

4. Click *OK*, then specify an alias for the certificate (for example, SiteB).

5. Examine the trusted root that is selected for you.

   If the trusted root is part of a chain, make sure you select the parent and all intermediate trusted roots.

6. Click *OK*.

   The trusted root certificate of Site B is added to the NIDP trust store.

7. Click *Identity Servers* > *Update* > *OK*.

   Wait for the health status to return to green.

8. To verify the certificates in the trust store, click *Certificates* > *Trusted Roots* > *NIDP-truststore*.

9. For the same Identity Server configuration, click *Identity Servers* > *Edit* > *Liberty*.

10. Click *New*, select *Service Provider*, then fill the following fields:

    Name: Specify a name for the provider. If you plan on configuring more than one protocol, include the protocol as part of the name, such as, SiteB_Liberty

    Metadata URL: Specify the URL of the Liberty metadata on Site B. For Site B in Figure 6-2, specify the following:

    `http://idp.siteb.novell.com:8080/nidp/idff/metadata`

    This example uses port 8080 to avoid any potential certificate problems that occur when the Identity Server and the Administration Console are installed on separate machines.

    SAML 2.0: If you are using SAML 2.0, the metadata path is `/nidp/saml2/metadata`. For Site B in Figure 6-2, specify the following for SAML 2.0:

    `http://idp.siteb.novell.com:8080/nidp/saml2/metadata`

    SAML 1.1: If you are using SAML 1.1, the metadata path is `/nidp/saml/metadata`. For Site B in Figure 6-2, specify the following for SAML 1.1:

`http://idp.siteb.novell.com:8080/nidp/saml/metadata`

11 Click *Next* > *Finish*.

12 Click *Identity Servers* > *Update*.

Wait for the health status to return to green.

13 Continue with "Configuring Site B to Trust Site A as an Identity Provider" on page 82.

Configuring Site B to Trust Site A as an Identity Provider

The following instructions explain how to import the trusted root certificate and metadata of Site A into the configuration for Site B.

1 Log in to the Administration Console for Site B.

The configuration of Site B can be created in the same Administration Console as Site A; it cannot be configured to be a cluster member of Site A.

2 In the Administration Console, click *Access Manager* > *Identity Servers* > *Edit* > *Security* > *NIDP Trust Store*.

3 In the Trusted Roots section, click *Auto-Import From Server*, then fill the following fields:

Server IP/DNS: Specify the IP address or DNS name of Site A. For Site A in Figure 6-2, specify the following:

`idp.sitea.novell.com`

Server Port: Specify 8443.

4 Click *OK*, then specify an alias for the certificate (for example, SiteA).

5 Examine the trusted root that is selected for you.

If the trusted root is part of a chain, make sure you select the parent and all intermediate trusted roots.

6 Click *OK*.

The trusted root certificate of Site A is added to the NIDP trust store.

7 Click *Identity Servers* > *Update* > *OK*.

Wait for the health status to return to green.

8 To verify the certificates in the trust store, click *Certificates* > *Trusted Roots* > *NIDP-truststore*.

9 For the same Identity Server configuration, click *Edit* > *Liberty*.

10 Click *New*, select *Identity Provider*, then fill the following fields:

Name: Specify a name for the provider. If you plan on configuring more that one protocol, include the protocol as part of the name, such as SiteA_Liberty

Metadata URL: Specify the URL of the Liberty metadata on Site A. For Site A in Figure 6-2, specify the following:

`http://idp.sitea.novell.com:8080/nidp/idff/metadata`

This example uses port 8080 to avoid any potential certificate problems that occur when the Identity Server and the Administration Console are installed on separate machines.

SAML 2.0: If you are using SAML 2.0, the metadata path is `/nidp/saml2/metadata`. For Site A in Figure 6-2, specify the following for SAML 2.0:

`http://idp.sitea.novell.com:8080/nidp/saml2/metadata`

SAML 1.1: If you are using SAML 1.1, the metadata path is `/nidp/saml/metadata`. For Site B in Figure 6-2, specify the following for SAML 1.1:

`http://idp.siteb.novell.com:8080/nidp/saml/metadata`

11 Click *Next* > *Finish*.

12 Click *Identity Servers* > *Update* > *OK*.

Wait for the health status to return to green.

13 Continue with one of the following:

- If you are using Liberty or SAML 2.0, continue with "Verifying the Trust Relationship" on page 83.
- If you are using SAML 1.1, continue with "Configuring SAML 1.1 for Account Federation" on page 86.

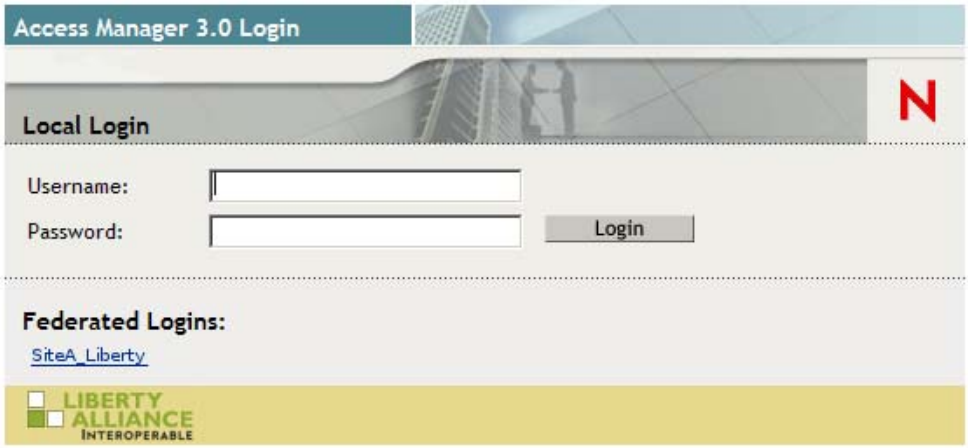
Verifying the Trust Relationship

Before continuing with federation configuration, you need to verify that Site A and Site B trust each other.

1 To test the trusted relationship, log in to the user portal of Site B. For Site B in Figure 6-2, specify the following:

`https://idp.siteb.novell.com:8443/nidp/app`

The following login screen appears.

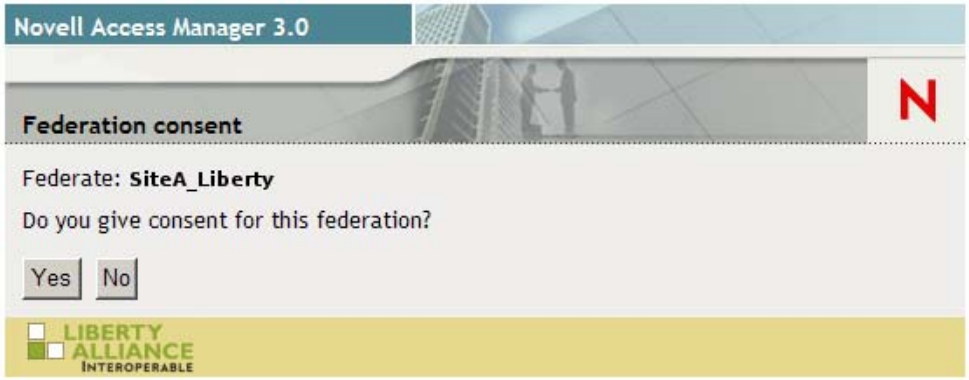


2 Click the Federated Login link.

You are directed to Site A for login.

3 Enter the credentials for a user from Site A.

The Federation consent prompt appears:



4 Click *Yes*.

You are returned to the login page for Site B.

5 Enter the credentials of a user from Site B that you want to federate with the user from Site A.

These two accounts are now federated. You can enter the URL to the user portal on Site A or Site B, and you are granted access without logging in again.

If you log out and log back in, the accounts are still federated, but you might be prompted for login credentials as you access resources on Site A, Site B, and the Access Gateways. To enable a single sign-on experience, Site A, Site B, and the Access Gateways must be configured to share a contract.

6 To enable a single sign-on experience, continue with "Configuring User Authentication" on page 84.

Configuring User Authentication

The following instructions describe one way to enable single sign-on to the Identity Servers and Access Gateways in Figure 6-1 on page 78. It explains how to configure all sites to use the same contract. The instructions explain the following tasks:

- Selecting the contract for federation
- Configuring the contract at Site B to allow authentication at Site A
- Configuring Site A so its contract can satisfy the requirements of the contract at Site B
- Configuring Site A and Site B to use this contract as their default contract

To configure the contracts:

1 Log in to the Administration Console for Site B.

2 Click *Access Manager > Identity Servers > Edit > Liberty > [Name of Identity Provider] > Access > Authentication*.

3 Verify the settings of the following fields:

Allow users to federate: Make sure this option is selected. If this option is not selected, users cannot federate their accounts at Site A with an account at Site B.

Allow after authentication: Make sure this option is selected. Enabling this option assumes that a user account exists at the service provider and that the account can be associated with a user's account at the identity provider.

Authenticate user with default contract login: Make sure this option is selected. In this example, single sign-on is enabled by specifying the same contract for all sites.

4 For *Authentication Context*, select *Use Contracts*.

5 In the *Authentication contracts* section, select the name of the contract used by the protected resources and move it to the *Contracts* section.

If you select a default contract (either Secure Name/Password-Form or Secure Name/Password-Basic), these contracts have been configured to allow federation. If you select a contract you have created, you need to verify that it is configured for federation. See Step 7.

6 Click *OK*, then update the Identity Server configuration.

7 Verify that the contract at Site B allows federation:

7a Click *Identity Servers* > *Edit* > *Local* > *Contracts*.

7b Record the URI for the contract you are using. This URI needs to exist as a contract on Site A. The name of the contract can be different at each site, but the URI must be the same.

7c Click the name of the contract.

7d Make sure the *Satisfiable by External Provider* option is selected.

7e Click *OK* twice, then update the Identity Server if you made any changes.

8 Verify that Site A contains the same contract:.

8a Log in to the Administration Console for Site A.

8b Click *Identity Servers* > *Edit* > *Local* > *Contracts*.

8c Match the URI from Step 7b to a contract.

If such a contract does not exist, you need to create it. For help, see "Configuring Authentication Contracts" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

8d Click *OK*.

9 In the Administration Console for Site A, click *Identity Servers* > *Edit* > *Local* > *Defaults*.

10 For the Authentication Contract, select the name of the contract from Step 8c.

11 (Conditional) If you have multiple user stores, set the default contract for each user store.

12 Click *OK*, then update the Identity Server.

13 Test the configuration:

13a Enter the URL to the user portal of Site B.

13b Click the federated login link to Site A.

13c Enter the credentials for Site A and log in.

13d Enter the URL for a protected resource.

You are granted access without being prompted for credentials.

14 If you want the authentication to the user portal on Site B to allow single sign-on to the Access Gateway protected resources or authentication to a protected resource to allow single sign-on to the user portal on Site B, you must configure the default contract for the Identity Server of Site B to match the contract used by the protected resources.

14a In the Administration Console for Site B, click *Access Manager* > *Identity Servers* > *Edit* > *Local* > *Defaults*.

14b For the Authentication Contract, select the name of the contract used by the protected resources.

14c (Conditional) If you have multiple user stores, set the default contract for each user store.

14d Click *OK*, then update the Identity Server.

14e To test single sign-on, log in to the user portal on Site B, then enter a URL for a protected resource.

6.2.3 Configuring SAML 1.1 for Account Federation

SAML 1.1 does not support user-controlled federation, but you can configure it so that accounts that match are automatically federated. The Liberty and SAML 2.0 protocols allow users to federate accounts without sharing any common attributes, but the SAML 1.1 protocol requires that the user accounts need to share some common attributes in order for SAML 1.1 to match them and allow federation.

- "Configuring User Account Matching" on page 86
- "Configuring the Default Contract for Single Sign-On" on page 88
- "Configuring a Federated Login Link for the Login Page" on page 88
- "Verifying the Trust Relationship with SAML 1.1" on page 89

Configuring User Account Matching

When federating with SAML 1.1, the security of a user matching method depends upon the accuracy of the mapping. You need to select an attribute or attributes that uniquely identify the user at both Site A and Site B. The attributes must identify only one user at Site A and match only one user at Site B. If the attributes match multiple users, you have a security problem,

The following steps use the e-mail address of the user and the LDAP mail attribute to set up a matching rule that matches one user account at Site A with one user account at Site B. To securely use such a matching rule, you need to have a rule in place at both Site A and Site B to ensure that all users had unique email addresses.

- "Configuring Site B for User Account Matching" on page 86
- "Configuring the Attribute for Sharing" on page 87
- "Configuring the Providers to Use the Shared Attribute" on page 87

Configuring Site B for User Account Matching

1. In the Administration Console of Site B, click *Access Manager* > *Identity Servers* > *Servers* > *Edit* > *SAML 1.1* > *[Identity Provider]* > *Access* > *Authentication*.
2. Select *Match existing user account*.
3. Click the *Define User Matching Method* icon.
4. Move the user store that you want to search for the attribute to the *User stores* list.
5. For the *User Matching Expression*, select *New User Matching Expression*.
6. Specify a name for the matching expression, such as email.
7. In *Logic Group 1*, click the *Add* icon, select *Ldap Attribute:mail [LDAP Attribute Profile]*, then click *OK*.

The form allows you to create a very complex set of matching rules, with multiple conditions. This example uses one attribute, the simplest form of a matching expression.

8 Click *Finish*, then select your matching expression for the *User Matching Expression*.

9 Click *OK*.

10 For the *Satisfies contract* option, select the contract that you want to use for single sign-on.

For this example, select *Secure Name/Password-Form*.

11 Click *OK* twice, then update the Identity Server.

12 Continue with "Configuring the Attribute for Sharing" on page 87.

Configuring the Attribute for Sharing

1 In the Administration Console of the Site B (the service provider), click *Access Manager* > *Identity Servers* > *Shared Settings*.

2 Click *Attribute Sets*, then click *New*.

3 Specify a *Set Name*, such as email, then click *Next*.

4 Click *New*, then fill the *Add Attribute Mapping* options:

Local attribute: Select *Ldap Attribute:mail [LDAP Attribute Profile]*.

Remote attribute: Leave this field empty. It is an optional value.

5 Click *OK*, then click *Finish*.

Your newly created attribute mapping appears in the list of Attribute Sets.

6 Repeat Step 1 through Step 5 for Site A (the identity provider).

If Site A and Site B are imported into the same Administration Console, skip this step.

7 Continue with "Configuring the Providers to Use the Shared Attribute" on page 87.

Configuring the Providers to Use the Shared Attribute

You need to configure Site A to send the shared attribute with the authentication credentials, and you need to configure Site B to process the shared attribute that is included with the authentication credentials.

1 In the Administration Console for Site B, click *Access Manager* > *Identity Servers* > *Edit* > *SAML 1.1* > *[Name of Identity Provider]* > *Access* > *Attributes*.

2 For the *Attribute set*, select the set name you created in "Configuring the Attribute for Sharing" on page 87.

3 Move the email attribute so that it is obtained at authentication.

4 Click *OK* twice, then update the Identity Server.

5 In the Administration Console for Site A, click *Access Manager* > *Identity Servers* > *Edit* > *SAML 1.1* > *[Name of Service Provider]* > *Access* > *Attributes*.

6 For the *Attribute set*, select the set name you created in "Configuring the Attribute for Sharing" on page 87.

7 Move the email attribute so that it is sent with authentication.

8 Click *OK* twice, then update the Identity Server.

9 Continue with "Configuring the Default Contract for Single Sign-On" on page 88

Configuring the Default Contract for Single Sign-On

The Identity Servers at Site A and Site B need to use the contract you specified in your user matching expression to be the default contract for Site A, Site B, and the protected resources of the Access Gateway.

For the user matching expression contract, see Step 10 in "Configuring Site B for User Account Matching" on page 86.

To configure the default contracts for Site A and Site B:

1. In the Administration Console for Site B, click *Access Manager* > *Identity Servers* > *Edit* > *Local* > *Defaults*.
2. For the Authentication Contract, select the name of the contract used by the user matching expression.
3. (Conditional) If you have multiple user stores, set the default contract for each user store.
4. Click *OK*, then update the Identity Server.
5. For Site A, repeat Step 1 through Step 4.
6. For the Access Gateway, review the contracts you have assigned to the protected resources.
   - **6a** In the Administration Console for Site B, click *Access Manager* > *Access Gateways* > Edit > *[Name of Reverse Proxy]* > *[Name of Proxy Service]* > *Protected Resources*.
   - **6b** For single sign-on, change the contract to match the contract for the user matching expression.
   - **6c** (Conditional) If you have multiple reverse proxies and proxy services, verify the contracts on all protected services that you want enabled for single sign-on.
   - **6d** Click *OK* to save your changes, then update the Access Gateway.
7. Continue with "Configuring a Federated Login Link for the Login Page" on page 88.

Configuring a Federated Login Link for the Login Page

The Liberty and SAML 2.0 protocols allow Access Manager to automatically add a federated login link to the Login page when a trusted relationship is established. For SAML 1.1, you must configure and enable this link.

1. In the Administration Console for Site B, click *Access Manager* > *Identity Servers* > *Edit* > *SAML 1.1* > *[Name of Identity Provider]* > *Access*.
2. In the Display section, fill the following fields:

   Icon URL: (Optional) If you have an icon you want displayed for the federated link, specify the URL to this icon.

   Login URL: Specify the Intersite Transfer Service URL to Site A. For Figure 6-1 on page 78, specify the following value:

   ```
   https://idp.sitea.novell.com:8443/nidp/saml/idpsend?PID=https://
   idp.siteb.novell.com:8443/nidp/saml/metadata&TARGET=https://
   idp.siteb.novell.com:8443/nidp/app
   ```

   For more information, see "Specifying the Intersite Transfer Service URL for the Login URL Option" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

   Advertise on Login page: Select this option.

3 Click *OK* twice, then update the Identity Server.

4 Continue with "Verifying the Trust Relationship with SAML 1.1" on page 89.

Verifying the Trust Relationship with SAML 1.1

1 To test the trusted relationship, enter the URL for the user portal of Site B. For Site B in Figure 6-2, you would specify the following:

```
https://idp.siteb.novell.com:8443/nidp/app
```

The following login screen appears.

If you do not see the Federated Login link for SAML 1.1, verify the Login URL. See "Configuring a Federated Login Link for the Login Page" on page 88.

2 Click the Federated Login link.

You are directed to Site A for login.

3 Enter the credentials for Site A.

If the user credentials at Site A successfully map to a user at Site B, you are authenticated and redirected to the User Portal on Site B.

4 Verify that the Authentication and Federation pages in the user portal for Site B contain values about your federation. If they don't, the user account matching failed. To find the problem, review the tasks in "Configuring User Account Matching" on page 86.

5 If your protected resources on the Access Gateway use the same contract, enter the URL to one of these resources.

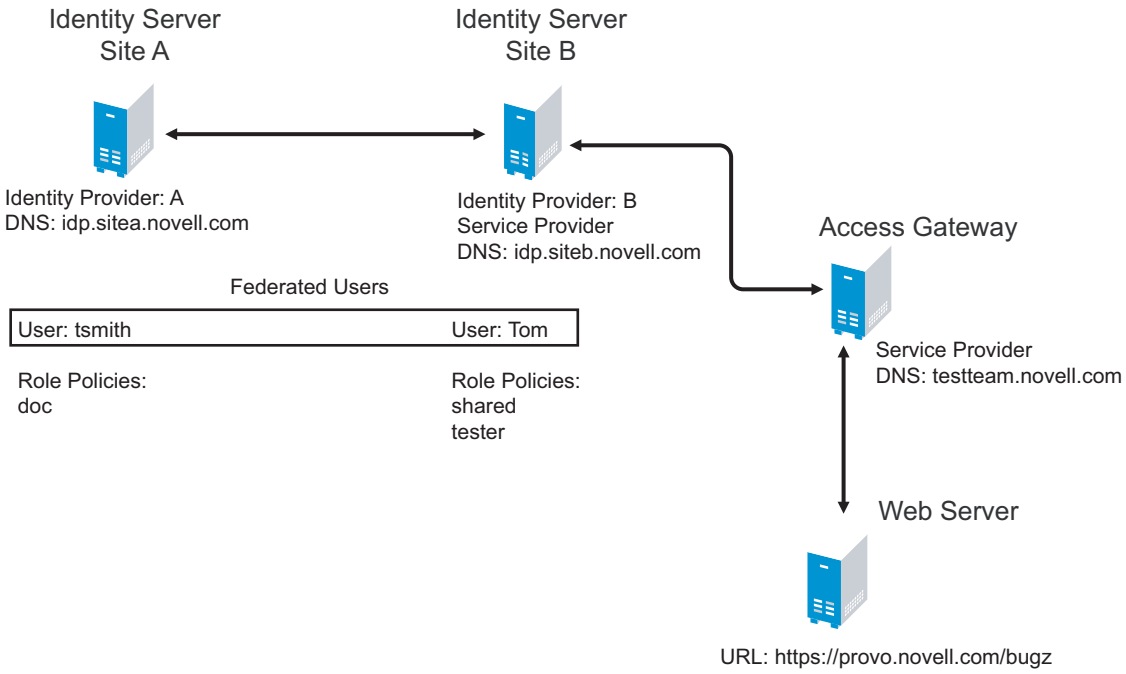
You are granted access without entering any additional credentials.

6.3 Sharing Roles

When two Identity Servers are configured to trust each other, one as an identity provider and the other as a service provider, they can be configured so that roles are shared. The following instructions are written for when both the identity provider and the service provider are Novell Identity Servers. If you are using a third-party identity or service providers, you need to modify the instructions.

Figure 6-3 illustrates a configuration where Identity Server of Site A is acting as an identity provider for Site B. When you configure the Identity Servers correctly, the Access Gateway can use the roles defined for the users of Site A in its policies.

Figure 6-3 *Two Federated Identity Servers*



The key to sharing roles is to set up the configuration so that the SAML assertion that the identity provider (Site A) sends to the service provider (Site B) contains the roles that the user has been assigned. Site B evaluates the roles and assigns them to the federated users at Site B. The Access Gateway can use these roles in its policy evaluations, and grant or deny access based on the assigned roles.

For example, when user tsmith authenticates to Site A, tsmith is assigned the role of doc. Tom, a user at Site B, is federated with the tsmith user. The doc role is shared with Site B, and Site B contains a policy that assigns users with the shared doc role to the tester role. The Access Gateway is configured with an Authorization policy that grants access to a resource when the requester is assigned the tester role. Tom does not have the qualifications at Site B to be assigned the tester role.

In this scenario, when Tom requests access to the protect resource at Site B, a login page with a federated link to Site A is displayed. If Tom selects to log in to Site A, Site A assigns him to the doc role. The doc role is sent with tsmith's authentication credentials to Site B. Site B evaluates the credentials and assigns Tom to the tester role because the following conditions are met:

- Tom is federated with tsmith.
- tsmith was assigned the doc role.
- The shared role and tester policies on Site B qualify the user to be assigned the tester role.

When the Access Gateway evaluates the credentials of Tom, Tom is granted access to the protected resource because he has the tester role.

This section describes how to set up such a configuration. It assumes that the following have already been done:

- The trusted relationship between the identity provider and service provider is set up. For configuration instructions, see Section 6.2.2, “Establishing Trust between Providers,” on page 80.
- The following policies have been created: the doc role policy at Site A, the tester role policy at Site B, and the Authorization policy (that uses the tester role) for the Access Gateway. For information on creating a Role policy, see Section 7.4.2, “Configuring a Role-Based Policy,” on page 108, and for the Authorization policy, see Section 7.4.3, “Assigning an Authorization Policy to Protect a Resource,” on page 116. The following instructions explain how to set up the shared policy.

This section explains how to configure Site A and Site B so that Site A shares its roles with Site B.

- Section 6.3.1, “Configuring Role Sharing,” on page 91
- Section 6.3.2, “Verifying the Configuration,” on page 93

6.3.1 Configuring Role Sharing

There are three major tasks for configuring role sharing. You need to configure a shared attribute for transferring the roles. You need to configure the identity provider and the service provider so that the role assignments can be added to the attribute and retrieved from the attribute. Finally, you need to create a shared Role policy for each role sent to the service provider. This policy defines how the role should be processed.

The following sections describe these configuration tasks:

- “Defining a Shared Attribute Set” on page 91
- “Obtaining the Role Assignments” on page 92
- “Configuring Policies to Process Received Roles” on page 92

Defining a Shared Attribute Set

1. In the Administration Console of the Site A (the identity provider), click *Access Manager* > *Identity Servers* > *Shared Settings*.
2. Click *Attribute Sets*, then *New*.
3. Specify a *Set Name*, such as role_sharing, then click *Next*.
4. Click *New* and fill the *Add Attribute Mapping* options:

   Local attribute: Select *All Roles*.

   Remote attribute: Leave this field empty. It is an optional value.
5. Click *OK*, then click *Finish*.

   Your newly created attribute mapping appears in the list of Attribute Sets.
6. Repeat Step 1 through Step 5 on Site B (the service provider).
7. Continue with “Obtaining the Role Assignments” on page 92.

Obtaining the Role Assignments

1. To export the roles from the identity provider, log in to the Administration Console for the identity provider. (In Figure 6-3, this is Site A.)
   - **1a** Click *Access Manager > Identity Servers > Edit > Liberty > [Name of Service Provider] > Access > Attributes*.

     If you are using SAML 2.0 or SAML 1.1 protocol, the steps are the same. You just need to click the appropriate tab after clicking *Edit*. The path is the same for all protocols.
   - **1b** Select the attribute set you created, then move *All Roles* so this attribute is sent with authentication.
   - **1c** Click *OK*.
   - **1d** Update the Identity Server of Site A.
2. To import the roles from the identity provider to the service provider, log in to the Administration Console for the service provider. (In Figure Figure 6-3, this is Site B.)
   - **2a** Click *Access Manager > Identity Servers > Edit > Liberty > [Name of Identity Provider] > Access > Attributes*.
   - **2b** Select the attribute set you created, then move *All Roles* so this attribute is obtained with authentication.
   - **2c** Click *OK*.
   - **2d** Update the Identity Server of Site B.
   - **2e** Continue with "Configuring Policies to Process Received Roles" on page 92.

Configuring Policies to Process Received Roles

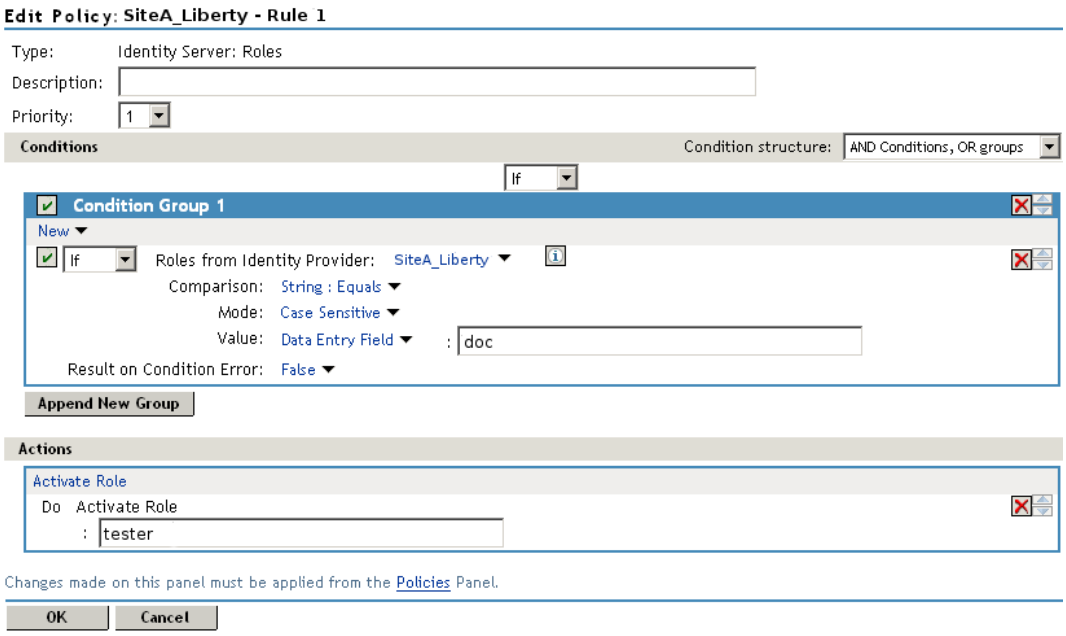
For each role that is sent from Site A, you need to create a role policy that specifies the role that should be activated on Site B. For example, suppose the tsmith user from Site A is assigned the doc role at authentication. You can create a Role policy on Site B that assigns the tester role to anyone with the doc role from Site A.

1. Log in to the Administration Console for Site B.
2. Click *Access Manager > Policies > New*.
3. Specify a name for the policy, select *Identity Server: Roles* for the type, then click *OK*.
4. In the *Condition Group 1* section, click *New*, then select *Roles from Identity Provider*.
5. (Conditional) If you have federated with more than one identity provider, select the provider. If you have federated with only one identity provider, the provider is selected for you.

   In this example, you have federated with only the identity provider at Site A, and it is selected for you.
6. For the value, select *Data Entry Field*, then specify the name of a role that is assigned by Site A, for example doc.

   If you leave *Mode* set to *Case Sensitive*, make sure you specify the case correctly.
7. In the *Actions* section, specify the role to activate on Site B for the role received from Site A.

   Your policy should look similar to the following:



8 Click *OK* twice, then click *Apply Changes*.

9 To enable the role for the Identity Server, click *Identity Servers* > *Edit* > *Roles*.

10 Select the role, then click *Enable*.

11 (Optional) Repeat Step 2 through Step 10 for other roles assigned at Site A.

If you have other Role policies at Site A, you need to set up Role policies at Site B to have the roles activated. For example, if Site A had a tester role policy and you wanted users assigned to the tester role policy to also be assigned to the tester role policy at Site B, you could create a separate policy for this activation, or you could add an Or condition group with a value field of tester to the policy in Step 7. The policy would assign federated users who belonged to the doc or tester roles at Site A, to the tester role at Site B.

12 To test role sharing:

12a Enter the URL of a protected resource that requires a role for access. For the policy above, it would be a resource requiring the tester role.

12b Click the federated link to Site A.

12c Log in with the credentials of a user who is assigned the doc role.

You are granted access to the resource. If you are denied access, continue with Section 6.3.2, "Verifying the Configuration," on page 93 to discover the problem.

6.3.2 Verifying the Configuration

This section traces the role assignment from the Identity Server that assigns it to the user, through the Identity Server that receives the roles with the user's authentication assertion, to the policy evaluation. If you are having trouble, this should help you determine the source of the problem.

The following procedures refer to the configuration displayed in Figure 6-3, "Two Federated Identity Servers," on page 90. A tsmith user from Site A, who is assigned the doc role, is federated with a Tom user at Site B. Site B does not assign Tom the tester role. The Web server has been configured to protect the bugz site, which requires the tester role.

To verify the configuration:

1. Make sure policy logging is enabled on the identity provider and the service provider. Make sure that you enable at least Application logging at an Info level.

   For configuration procedures, see "Configuring Identity Server Logging" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

   You can access log files for downloading and viewing by clicking *Access Manager* > *Auditing* > *General Logging*.

2. Have a user access a resource that is protected by a policy requiring a role from Site A.

   For this trace, the tsmith user from Site A requests access to the bugz page. The user uses the federated link and logs in with the credentials of the tsmith user.

3. Verify that Site A is assigning the user the role.

   3a View the `catalina.out` file of the Identity Server at Site A.

   3b Search for the name of the role. You should find a line similar to the following:

   ```
   <amLogEntry> 2008-02-22T20:30:19Z INFO NIDS Application:
   AM#500105013: AMDEVICEID#C5F467BA50B009AC:
   AMAUTHID#DEEF6BEC3655DEB71CA56832DDDF866E: Authenticated user
   cn=tsmith,o=novell in User Store sitea-nids-user-store with
   roles doc,authenticated. </amLogEntry>
   ```

   If the role you need is not listed, look at the policy evaluation trace to discover why the user has not been assigned the role. For more information on how to understand role traces, see "Role Assignment Traces" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

4. Verify that Site A is sending an authentication assertion to Site B.

   In the `catalina.out` file of the Identity Server from Site A, look for lines similar to the following:

   ```
   <amLogEntry> 2008-02-22T20:30:19Z INFO NIDS Application:
   AM#500105018: AMDEVICEID#C5F467BA50B009AC:
   AMAUTHID#DEEF6BEC3655DEB71CA56832DDDF866E: Responding to
   AuthnRequest with artifact
   AAPLsCVpfv3ha9Mpn+cUiCXcf3D63sc0QfscL5mZaaygHBKVOOh9aPSQ </
   amLogEntry>

   <amLogEntry> 2008-02-22T20:30:19Z INFO NIDS Application:
   AM#500105019: AMDEVICEID#C5F467BA50B009AC:
   AMAUTHID#F8B1C147EB3DDEFE9A3DB0827BA8E4A3: Sending AuthnResponse
   in response to artifact
   AAPLsCVpfv3ha9Mpn+cUiCXcf3D63sc0QfscL5mZaaygHBKVOOh9aPSQ </
   amLogEntry>
   ```

   If you do not see these types of entries, verify that you have configured Site A to send the roles. See "Obtaining the Role Assignments" on page 92.

5. Verify that Site B is receiving the SAML assertion with the roles.

   In the `catalina.out` file of the Identity Server from Site B, look for lines similar to the following:

   ```
   <amLogEntry> 2008-02-22T20:30:19Z INFO NIDS Application:
   AM#500105020: AMDEVICEID#488475009C6D3DDF:
   AMAUTHID#0FBA0CF7E41E6C7F9121DABB918D34F4: Received and processing
   ```

```
artifact from IDP -
AAPLsCVpfv3ha9Mpn+cUiCXcf3D63sc0QfscL5mZaaygHBKVOOh9aPSQ </
amLogEntry>

<amLogEntry> 2008-02-22T20:30:19Z INFO NIDS Application:
AM#500105021: AMDEVICEID#488475009C6D3DDF:
AMAUTHID#0FBA0CF7E41E6C7F9121DABB918D34F4: Sending artifact
AAPLsCVpfv3ha9Mpn+cUiCXcf3D63sc0QfscL5mZaaygHBKVOOh9aPSQ to URL
https://rholm.provo.novell.com:8443/nidp/idff/soap at IDP </
amLogEntry>
```

The artifact ID should be the same as the artifact ID in Step 4.

If you do not see these types of entries, verify that you have configured Site B to receive the roles. See "Obtaining the Role Assignments" on page 92.

6 Verify that Site B is evaluating the received role assignments and activating the roles.

In the `catalina.out` file of the Identity Server from Site B, search for a policy evaluation for RolesFromIdentityProvider. You should find lines similar to the following:

```
~~CO~1~RolesFromIdentityProvider(6670):https://
ipd.sitea.provo.novell.com:8443/nidp/idff/
metadata:TESTER,DOC,AUTHENTICATED~com.novell.nxpe.condition.NxpeOp
erator@string-equals~(0):hidden-param:hidden-value:~~~True(69)

~~PA~ActionID_1203705845727~~AddRole~tester~~~Success(0)

<amLogEntry> 2008-02-22T20:30:20Z INFO NIDS Application:
AM#500105013: AMDEVICEID#488475009C6D3DDF:
AMAUTHID#0FBA0CF7E41E6C7F9121DABB918D34F4: Authenticated user
cn=Tom,o=novell in User Store Internal with roles
tester,authenticated. </amLogEntry>
```

The policy evaluation shows that the condition evaluates to true and that the tester role is activated. Tom is the user that is federated with the tsmith user, and the entry shows that Tom has been assigned the tester role.

If you do not see a policy evaluation for RolesFromIdentityProvider, make sure you have created such a Role policy and that you have enabled it. See "Configuring Policies to Process Received Roles" on page 92.

7 If the use has been assigned the correct role, the last step is to verify how the embedded service provider evaluated the policy protecting the resource.

In the `catatina.out` file of the `ipd-esp` file for the Access Gateway, search for lines similar to the following for the authorization policy trace:

```
<amLogEntry> 2008-02-22T20:30:20Z INFO NIDS Application:
AM#501102050: AMDEVICEID#esp-2559E77C93738D15:
AMAUTHID#BCF3CB40B51E8A0AF8582BEF762B4DDD: PolicyID#65LN233O-KN19-
1L7M-176M-P942LMN6P832: NXPESID#1411: AGAuthorization Policy
Trace:
 ~~RL~1~~~~Rule Count: 2~~Success(0)
 ~~RU~RuleID_1198874340999~Allow_Tester~DNF~~1:1~~Success(0)
 ~~CS~1~~ANDs~~1~~True(69)
 ~~CO~1~CurrentRoles(6660):no-param:TESTER,AUTHENTICATED~com.
novell.nxpe.condition.NxpeOperator@string-substring~SelectedRole
(6661):hidden-param:hidden-value:~~~True(69)
 ~~PA~1~~Permit Access~~~~Success(0)
```

```
 ~~PC~1~~Document=(ou=xpemlPEP,ou=mastercdn,ou=ContentPublisher
Container,ou=Partition,ou=PartitionsContainer,ou=VCDN_Root,ou=acce
ssManagerContainer,o=novell:romaContentCollectionXMLDoc),Policy=(A
llow_Tester),Rule=(1::RuleID_1198874340999),Action=(Permit::1)~~~~
Success(0)
 </amLogEntry>
```

If the PA line does not evaluate to Permit Access, then you need to review the Authorization policy and discover the conditions, other than the tester role, that must be met to permit access.

6.4 Setting Up Federation with Third-Party Providers

Setting up federation with providers other than Novell Identity Servers requires the same basic tasks as setting up federation with Novell Identity Servers, with some modifications.

When you set up federation with identity providers and service providers that are controlled by a single company, you have access to the Administration Consoles for both Identity Servers and know the admin credentials. When setting up federation with another company, additional steps are required.

- You need to negotiate with the other company and gain approval for federation because metadata must be shared and both sites require configuration. You'll need to negotiate a schedule for these configuration changes.
- The other site might not being using Access Manager for its identity or service provider. The basic tasks need to be modified to accommodate how that implementation shares metadata, authentication methods, and roles. Many SAML 1.1 providers do not support a metadata URL, and the data has to be imported manually.

  For example, instead of sharing URLs that allow you to import metadata, you might need to share the actual metadata and paste it into the configuration. The Novell Identity Server validates the metadata of another identity provider or service provider; some implementations do not validate it. If the Identity Server determines that the metadata is invalid, you'll need to negotiate with the provider to send you metadata that has been validated.

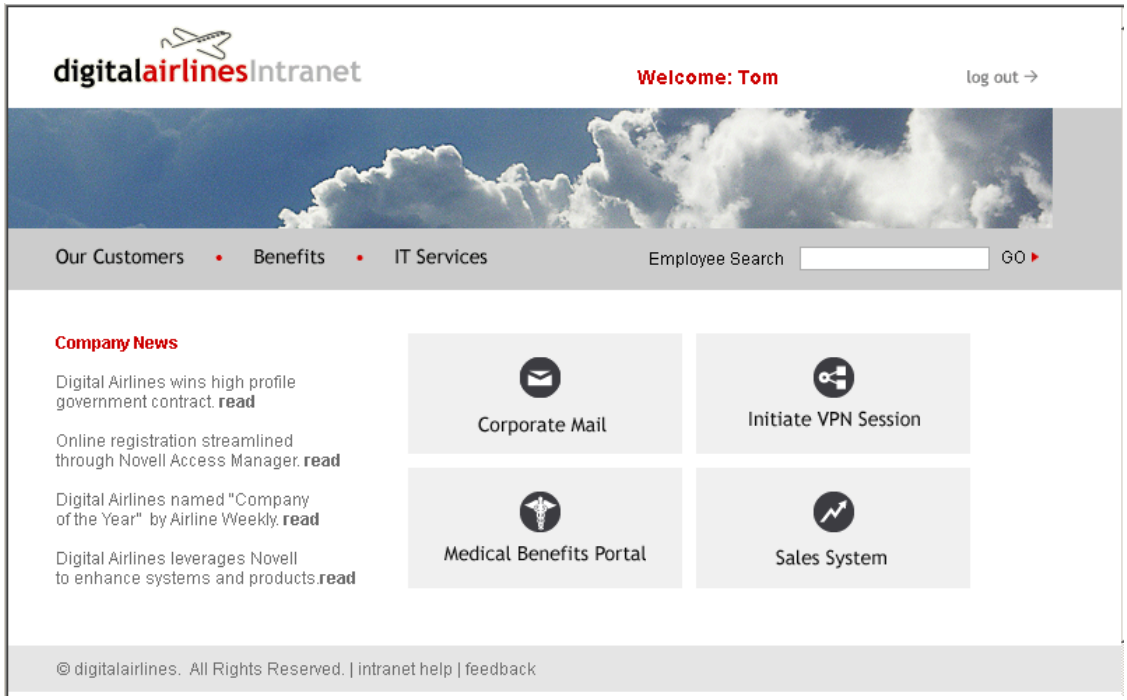
For a sample implementation with a third-party provider that explains the modifications that were required to set up the federation, see "SAML 1.1 with Concur" (http://www.novell.com/coolsolutions/appnote/19673.html).

Digital Airlines Example

7

This section explains how to use Access Manager to protect the Web site illustrated in Figure 7-1:

Figure 7-1 *Digital Airlines Web Services*



This section explains how to configure the Access Manager components to allow access to this first page, how to customize this first page, and how to create and assign policies that protect the other pages.

The example Web pages are designed to help network administrators understand the basic concepts of Novell® Access Manager by installing and configuring a relatively simple implementation of the software. The example serves as a primer for a more comprehensive production installation of Access Manager. This process is explained in the following sections:

- Section 7.1, “Installation Overview and Prerequisites,” on page 97
- Section 7.2, “Setting Up the Web Server,” on page 99
- Section 7.3, “Configuring Public Access to Digital Airlines,” on page 102
- Section 7.4, “Implementing Access Restrictions,” on page 107
- Section 7.5, “Modifying the Digital Airlines Example,” on page 131

7.1 Installation Overview and Prerequisites

This section discusses the concepts involved in installing Access Manger to protect the example Digital Airlines Web site:

- Section 7.1.1, “Installation Architecture,” on page 98

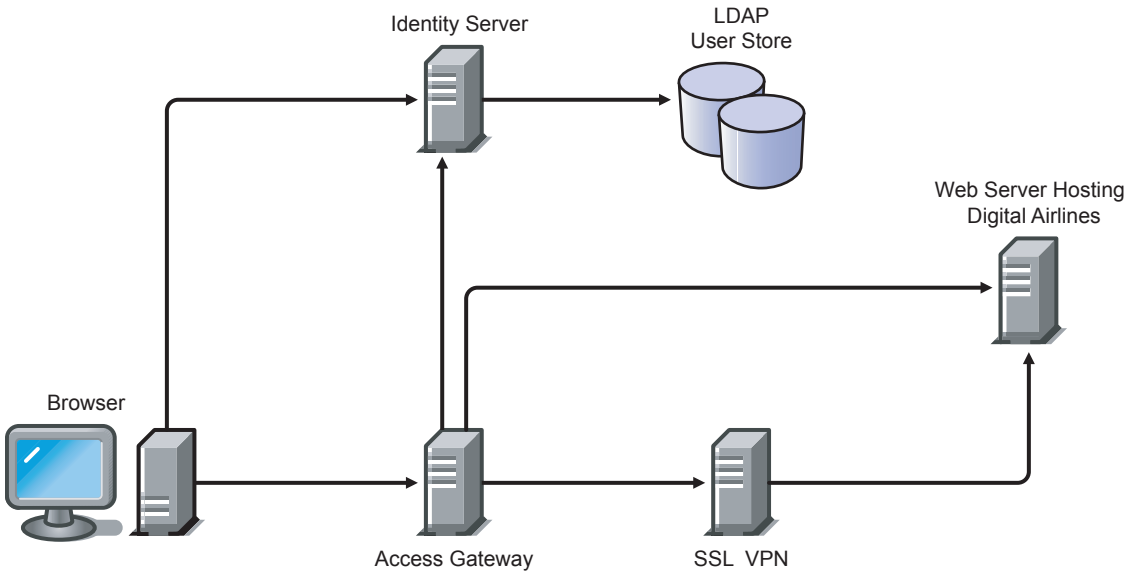
- Section 7.1.2, “Deployment Overview,” on page 99

After you deploy this example, you should understand the basic features of Access Manager and know how to configure the software to protect your own Web servers and applications. For more information about managing and configuring Access Manager components, see the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

7.1.1 Installation Architecture

The diagram below illustrates how the Digital Airlines example is integrated with the Access Manager components. The diagram shows that the Digital Airlines example can be hosted on a separate Web server, including a virtual server.

Figure 7-2 *Digital Airlines Architecture*



This document explains how to use a browser machine and two other machines for this configuration.

Table 7-1 *Novell Access Manager Components*

	Administration Console	Identity Server	Access Gateway	SSL VPN	Application Web Server	LDAP User Store	Browser
Machine 1	X	X		X	X	X	
Machine 2			X				
Machine 3							X

The simplified configuration described in this document is for a test environment only. It is not a recommended or supported configuration for a production environment. For example, the configuration database installed with the Administration Console should not be used as an LDAP user store in a production environment. This simplified configuration is designed to minimize the number of machines required for a tutorial.

After deploying the Digital Airlines example, you should understand the concepts required to deploy Access Manager in a number of other configurations. In a production environment, you need to install the necessary Access Manager components according to your specific requirements. For more information about other possible installation configurations, see "Recommended Installation Scenarios" in the *Novell Access Manager 3.0 SP3 IR2 Installation Guide*.

7.1.2 Deployment Overview

- "Prerequisite Tasks" on page 99
- "Deployment Tasks" on page 99

Prerequisite Tasks

Before starting with the Digital Airlines example, you must perform the following tasks:

- ❑ Enable pop-ups on a Firefox* browser (2.0 or above) or Internet Explorer browser (6.x or above) for managing and configuring the Access Manager components.
- ❑ Install the Novell Access Manager Administration Console, Identity Server, Access Gateway, and SSL VPN as described in the *Novell Access Manager 3.0 SP3 IR2 Installation Guide*.
- ❑ Configure the Novell® Access Manager Identity Server. For configuration details, see Section 1.3, "Creating a Basic Identity Server Configuration," on page 13.

IMPORTANT: The Digital Airlines procedures explain how to add a user to the configuration store of the Administration Console. These instructions assume that you have configured the Identity Server to use this configuration store as the LDAP user store. This is not a recommended configuration for a production environment. To enable this configuration for a test environment, specify the IP address of the Administration Console for the address of the server replica.

Do not configure the Access Gateway at this time. A later task explains how to configure the Access Gateway to allow access to the Digital Airlines site on the Web server.

Deployment Tasks

To configure access to the Digital Airlines site, you need to complete the following tasks:

1. Set up the Apache Web server on your Identity Server, then install the Digital Airline pages.

   For more information, see Section 7.2, "Setting Up the Web Server," on page 99.
2. Configure the Access Gateway to protect the Web server, but allow public access to the site. See Section 7.3, "Configuring Public Access to Digital Airlines," on page 102.
3. Configure the Access Gateway to allow access to the protected pages. See Section 7.4, "Implementing Access Restrictions," on page 107.
4. (Optional) Modify the Digital Airlines GUI, as described in Section 7.5, "Modifying the Digital Airlines Example," on page 131.

7.2 Setting Up the Web Server

- Section 7.2.1, "Installing the Apache Web Server and PHP Components," on page 100
- Section 7.2.2, "Installing Digital Airlines Components," on page 101

- Section 7.2.3, “Configuring Name Resolution,” on page 102

7.2.1 Installing the Apache Web Server and PHP Components

The following instructions are for SUSE® Linux Enterprise Server (SLES)10.x.

IMPORTANT: If you have installed your Identity Server on SLES 9.x, you need to make modifications to the following instructions. To install software with Yast, you click *Software* > *Install and Remove Software*. SLES 9.x uses PHP4 modules instead of PHP 5 modules.

---

1 Download and install the Apache 2 and PHP 5 modules:

1a On your SLES 10.x server, click the *YaST Control Center* icon, provide your root password if requested, then click *OK*.

1b In the YaST left navigation window, click the *Software* icon, then click *Software Management*.

The YaST software Search screen should open.

1c In the *Search* field, type *Apache2*, then click *Search*.

All available Apache 2 software packages are listed.

1d If they are not already selected, select the following Apache 2 check boxes:

apache2: Specifies the Apache 2.0 Web server.

apache2-mod_php5: Specifies the PHP5 module for Apache 2.0.

apache2-prefork: Specifies the Apache 2 prefork multi-processing module.

apache2-worker: Specifies the Apache 2 worker multi-processing module.

1e Click *Check* to identify and resolve any dependency issues.

1f Click *Accept*, then click *Continue*.

YaST should install the selected Apache server components.

1g To install the required PHP server components, answer *Yes* to the prompt to install additional software.

1h In the Search field, type *php*, then click *Search*.

All available PHP software packages are listed.

1i If they are not already installed, select the following PHP check boxes:

apache2-mod_php5: Installs the PHP 5 module for Apache 2.0.

php5: Installs the PHP 5 core files.

1j If you need to install the packages, click *Check* to identify and resolve any dependency issues. If the packages are already installed, click Cancel and continue with Step 2.

1k Click *Accept*, then click *Continue*.

YaST should install the selected PHP server components.

2 Configure SUSE to start the Apache server during boot up:

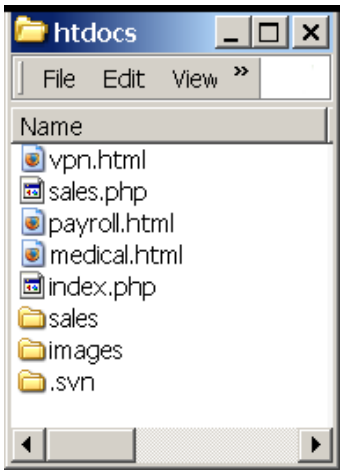
2a In the YaST left navigation window, click *Network Services* > *HTTP Server*.

2b In the HTTP Server Wizard, enable the *Start Apache2 Server When Booting* option, then click *Finish*.

7.2.2 Installing Digital Airlines Components

The Digital Airlines example package contains the following components:

Figure 7-3 *Directory Structure of Digital Airlines Sample Components*



- **vpn.html:** Specifies the GUI interface page for initiating a VPN session.
- **sales.php:** Contains the sales PHP database files associated with the example.
- **payroll.html:** Specifies the GUI interface page for initiating a payroll session.
- **medical.html:** Specifies the GUI interface page for initiating a VPN session.
- **index.php:** Contains the welcome HTML index file for establishing secure authentication.
- **sales:** Specifies subdirectory that can be configured to require basic authentication.
- **images:** Contains all image files associated with the example.
- **.svn:** Contains the associated Subversion* files necessary for revision control.

In this example configuration, you use the Access Gateway to protect the Digital Airlines Web site, which is installed on your Identity Server. This section describes where your example Digital Airlines components are located and how to add them to your Identity Server.

1. Download the Digital Airlines Sample Pages from the *Additional Resources* (http://www.novell.com/documentation/novellaccessmanager/index.html) section in the Novell Documentation site
2. Extract `htdocs.tar.gz` to a root directory of the Web server. For an Apache 2 Web server on SLES 9.*x* or 10.*x*, extract the files to the following directory:

   `/srv/www/htdocs/`
3. Determine the DNS name and IP address of the SUSE Linux server on which your example files are installed:

   3a Log in to the YaST Control Center as the root user.

   3b Click *Network Services* > *Host Names*, then write down the IP address and hostname of your server:

   IP Address: _____

   Hostname: _____

As required later in the installation (see Step 8 on page 104), you must provide the host name and server configuration information to establish the network connection between the Web server you are protecting (the server where your Web service components are located) and the Access Gateway.

4 Continue with Section 7.2.3, "Configuring Name Resolution," on page 102.

7.2.3 Configuring Name Resolution

The Identity Server needs to resolve the DNS name of the Access Gateway, the Access Gateway needs to resolve the DNS name of the Identity Server, and the client that is accessing the Digital Airlines site needs to be able to resolve the names of both the Access Gateway and the Identity Server.

You can either set up your DNS server to resolve the DNS name of the Identity Server and the Access Gateway to the correct IP address, or you need to modify the `hosts` file on the various machines to perform the resolution.

Client: The `hosts` file of the client machine needs to contain entries for the Identity Server and the Access Gateway.

Identity Server: The `hosts` file on the Identity Server needs to contain an entry for the Access Gateway.

Access Gateway: The `hosts` file on the Access Gateway needs to contain an entry for the Identity Server.

Each platform has its own location for the host file.

Platform	Location
Windows	C:\WINDOWS\SYSTEM32\DRIVERS\ETC\HOSTS
Linux	/etc/hosts
NetWare	sys:/etc/hosts

Continue with Section 7.3, "Configuring Public Access to Digital Airlines," on page 102.

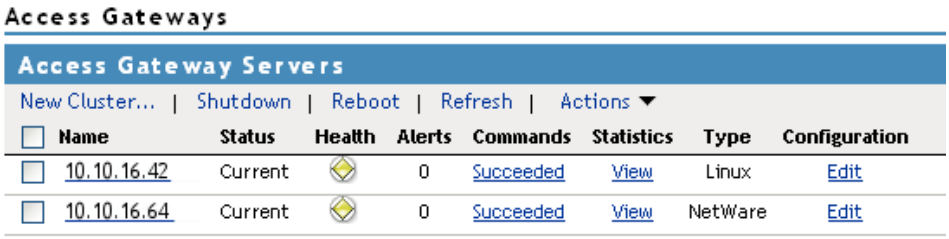
7.3 Configuring Public Access to Digital Airlines

This section describes the procedures for configuring the Access Gateway so that a client can access the Digital Airlines site. Before continuing, make sure you have completed the prerequisite tasks described in "Prerequisite Tasks" on page 99 and Section 7.2, "Setting Up the Web Server," on page 99.

1 On the client machine, open a browser and log in to the Administration Console.

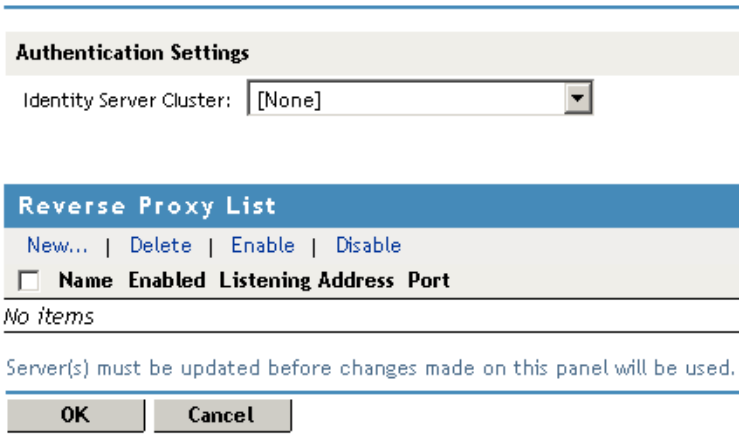
2 In the Administration Console, click *Access Manager* > *Access Gateways*.

The IP address of the Access Gateway you installed should be listed in the display window.



An Access Gateway that has not been configured displays a yellow health status.

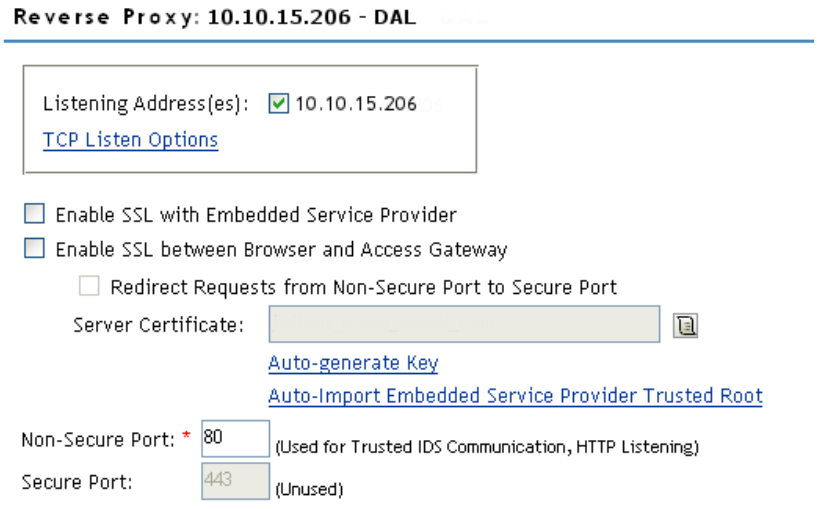
3 Click *Edit* > *Reverse Proxy / Authentication*.



4 In the *Identity Server Cluster* option, select the configuration you have assigned to the Identity Server.

This sets up the trust relationship between the Access Gateway and the Identity Server that is used for authentication.

5 In the *Reverse Proxy List*, click *New*, specify *DAL* as the new *Reverse Proxy Name*, then click *OK*.



6 Enable a listening address.

If the server has only one IP address, only one is displayed and it is automatically selected as the *Listening Address*. If the server has multiple addresses, you can select one or more IP addresses to enable. You must enable at least one address by selecting its check box.

7 Configure a listening port.

Non-Secure Port: Select 80, which is the default port for HTTP.

Secure Port: This is the HTTPS listening port. This port is unused and cannot be configured until you enable SSL. This example does not contain SSL configuration instructions.

8 In the *Proxy Service List*, click *New* and specify the following information:

Proxy Service Name: Specify any name that intuitively identifies this service on your Access Gateway server. For this example, specify *Dallistener*.

Public DNS Name: The DNS name you want the public to use to access your Digital Airlines site. This DNS name must resolve to the IP address you set up as the listening address. This example uses *am3bc.provo.novell.com*.

Web Server IP Address: The IP address of the Web server where your Digital Airlines files are installed.

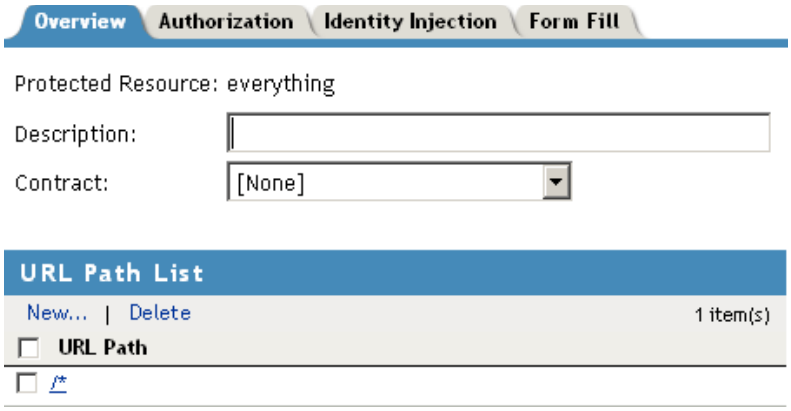
Host Header: Select *Forward Received Host Name* from the drop-down menu. The Web server and the Digital Airlines pages have not been set up to require the DNS name of the Web server in the Host Header, so it does not matter what name is placed in the Host Header.

9 Click *OK*.

10 In the *Proxy Service List*, click *Dallistener*.

11 Click *Protected Resources*, then in the *Protected Resource List*, click *New*.

12 Type `everything` in the Name field, then click *OK*.



13 In the *Contract* field, select *None* from the drop-down menu.

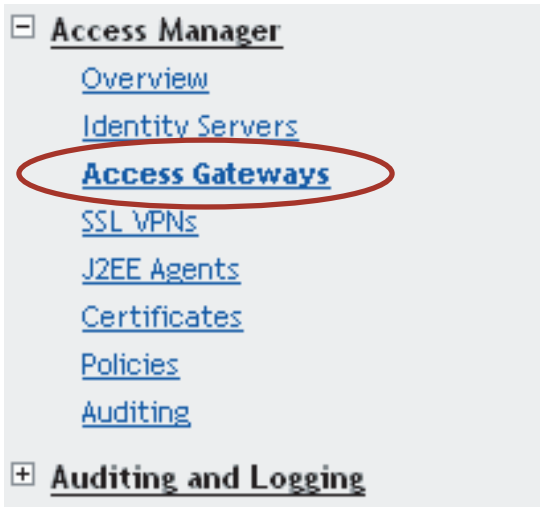
Under *URL Path List*, you should see /*, which includes everything on that server.

Later on, you will be instructed to change the *Contract* field to a *Name/Password - Form*, but for now, we want you to learn how the example works without any authentication.

14 Click *OK*.

15 In the *Protected Resource List*, verify that the protected resource you created is enabled, then click *OK*.

16 Click the *Access Gateways* link.



17 To apply the changes, click *Update* > *OK*.

Until this step, nothing has been saved. The *Update* status pushes the configuration to the server. When the configuration update has completed successfully, the server returns the status of *Current*.

18 To update the Identity Server for the trusted relationship, click *Identity Servers* > *Update* > *OK*.

19 To test the results, complete the following.

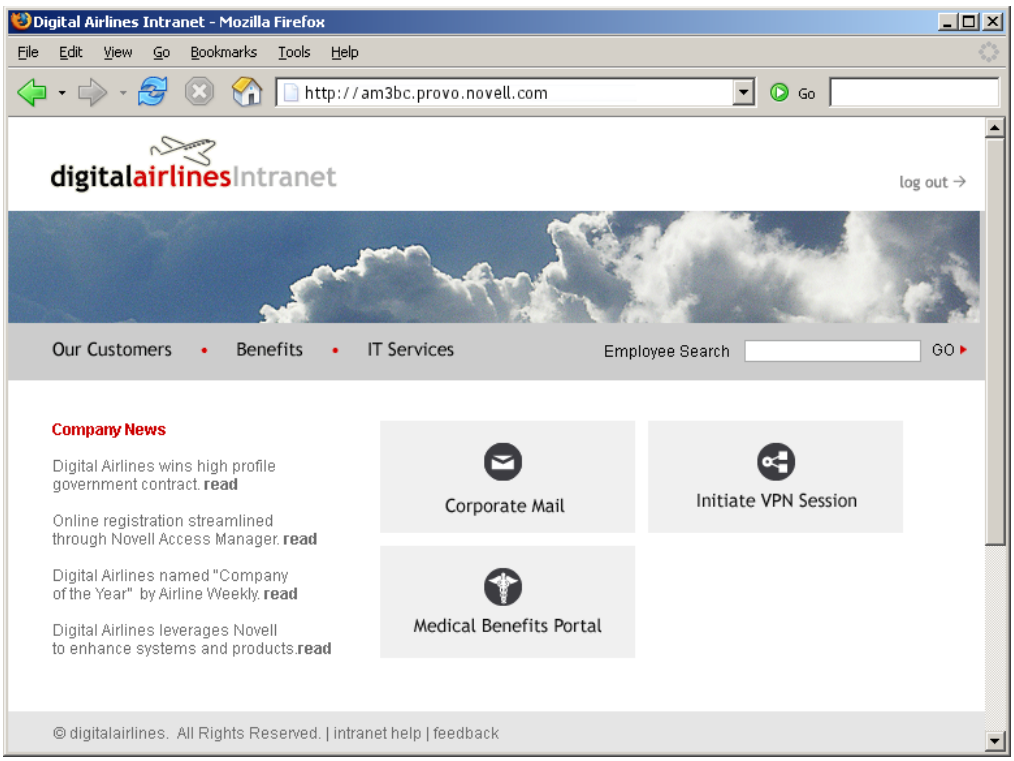
19a Open a browser on the client machine.

19b Enter the URL for the proxy service. For this example, it is

```
am3bc.provo.novell.com
```

Your network needs to be configured so that this published DNS name of the proxy service resolves to the IP address of the Access Gateway. The reverse proxy hides the internal address of the Web server.

You should see the Digital Airlines page.



If you get an error, check the time on the Access Gateway and Identity Server. They must be within 5 minutes of each other.

20 Close the browser.

21 To require authentication for access to the site and to configure access to the protected pages (the VPN application and the hidden Sales System site), continue with Section 7.4, “Implementing Access Restrictions,” on page 107.

Currently, the *Corporate Mail* and *Medical Benefits Portal* buttons do not link to available pages. They exist to illustrate what you could do when you require your users to authenticate before accessing the site.

For example, the *Corporate Mail* button could be configured so that the redirected request initiates a mail session to the user’s default e-mail application and injects the login credentials to provide access to the user’s protected, Web-based e-mail account.

The *Medical Benefits Portal* button could be configured to set up a federated account with the company that provides medical benefits for your company.

7.4 Implementing Access Restrictions

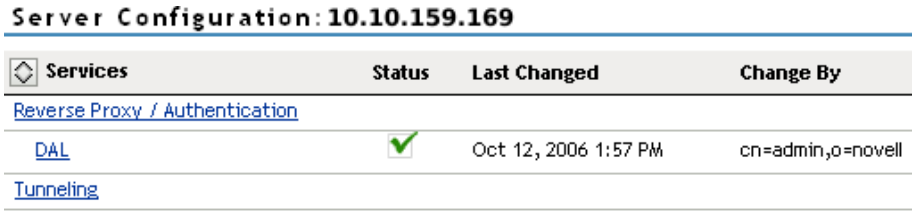
After you access the Digital Airlines site as a public resource (see Section 7.3, “Configuring Public Access to Digital Airlines,” on page 102), you can configure the site for authentication and authorization requirements. This section describes the following tasks:

- Section 7.4.1, “Enabling an Authentication Procedure,” on page 107
- Section 7.4.2, “Configuring a Role-Based Policy,” on page 108
- Section 7.4.3, “Assigning an Authorization Policy to Protect a Resource,” on page 116
- Section 7.4.4, “Configuring an Identity Injection Policy for Basic Authentication,” on page 119
- Section 7.4.5, “Initiating an SSL VPN Session,” on page 125

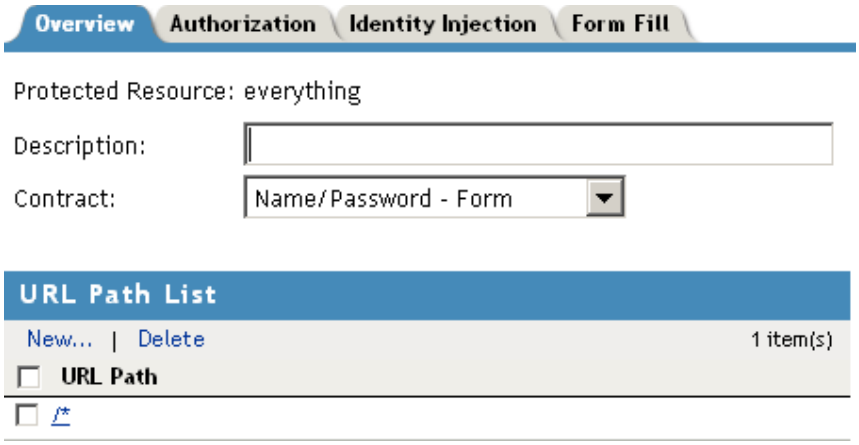
7.4.1 Enabling an Authentication Procedure

After hiding the internal Web server behind the Access Gateway, you can add an authentication method to the Web site by using the following procedure:

1 In the Administration Console, click *Access Manager* > *Access Gateways* > *Edit*.



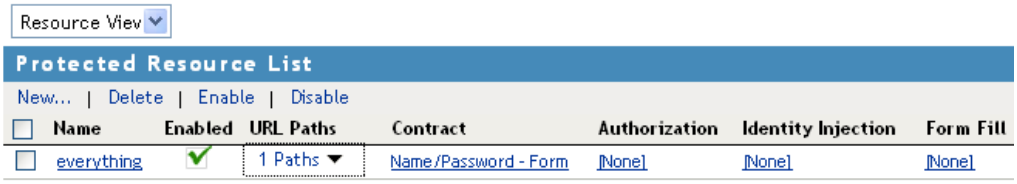
2 Click *DAL* > *Dallistener* > *Protected Resources* > *everything*.



3 In the *Contract* field, select *Name/Password - Form*.

IMPORTANT: Make sure to select the *Name/Password - Form* from the drop-down menu. *Secure Name/Password* does not work correctly if the base URL for the Identity Server is HTTP.

4 Click *OK* to return to the Protected Resources page.

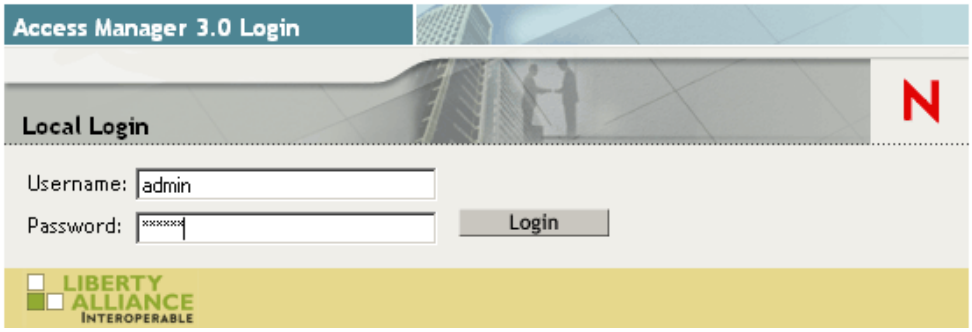


5 Click the *Access Gateways* link, then click *Update* > *OK*.

This pushes the new configuration to the server. When the configuration process is complete, the status returns to *Current*.

6 To test the results, open a browser and enter the URL of your Web site.

The Web site should now be protected and require you to log in by using a name and password. For this example, log in as the admin user of your Administration Console.



The Digital Airlines site appears.

7 Close all sessions of the browser.

The Digital Airlines page has a logout graphic, but it isn't an action. The current session is active until you log out (which isn't possible), until the session times out (the default value is 15 minutes), or you close all sessions of the browser.

8 Continue with Section 7.4.2, "Configuring a Role-Based Policy," on page 108.

7.4.2 Configuring a Role-Based Policy

Previously in the Digital Airlines example, you learned how to set up and configure Access Manager to protect a basic Web service. Access Manager also uses role-based access control (RBAC) to conveniently assign a user to a particular job function or set of permissions within an enterprise, in order to control access.

Access Manager enables you to assign roles to users, based on attributes of their identity, and then associate policies with the roles. In designing your own actual production environment, you need to decide which roles you need (such as, sales, administrative, and accounting). You create Role policies that assign the roles to your users, and then you create Authorization and Identity Injection policies that use the roles to control access.

This section explains how to set up an Identity Injection policy that customizes the main page of the Digital Airlines site. When the index.php page has access to the user's name, the main page displays the name. If the user belongs to the sales_role role, the *Sales System* button is displayed on the page.

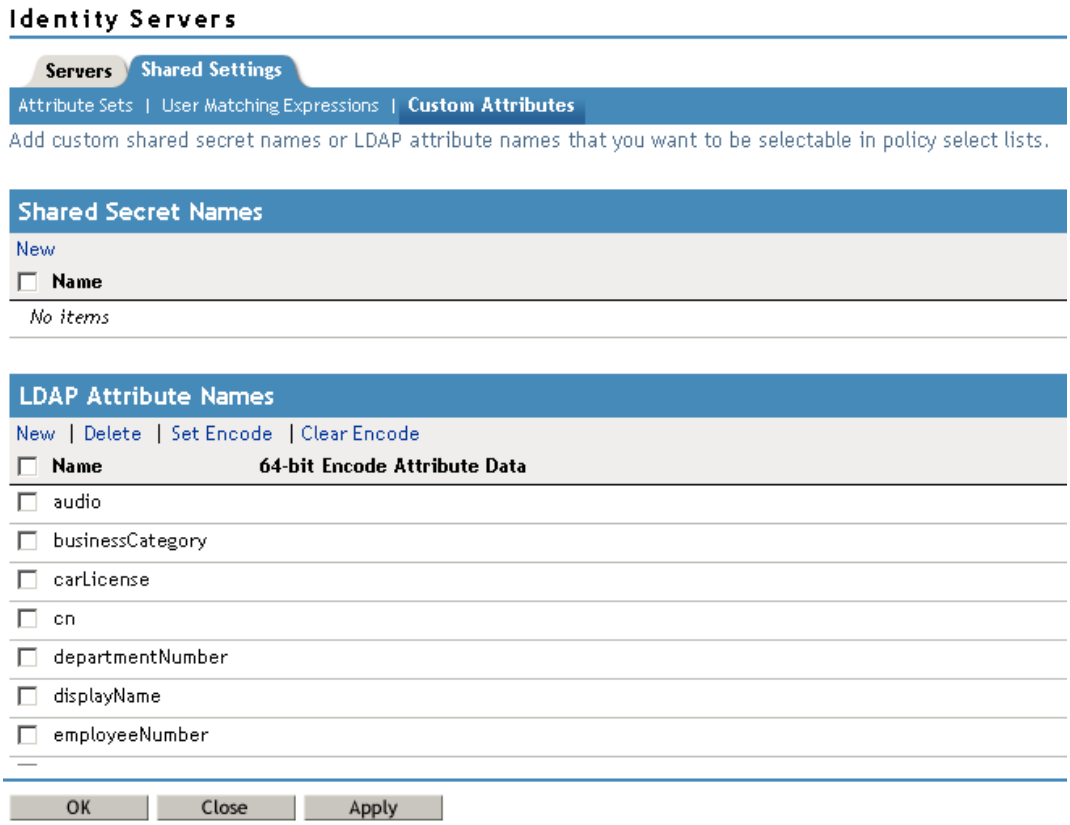
To configure an Identity Injection policy that uses a role, complete the following tasks:

- “Adding an LDAP Attribute to Your Configuration” on page 109
- “Creating a Sales Role” on page 110
- “Creating a New User with a Sales Role” on page 112
- “Creating the Identity Injection Policy for a Custom Header” on page 114

Adding an LDAP Attribute to Your Configuration

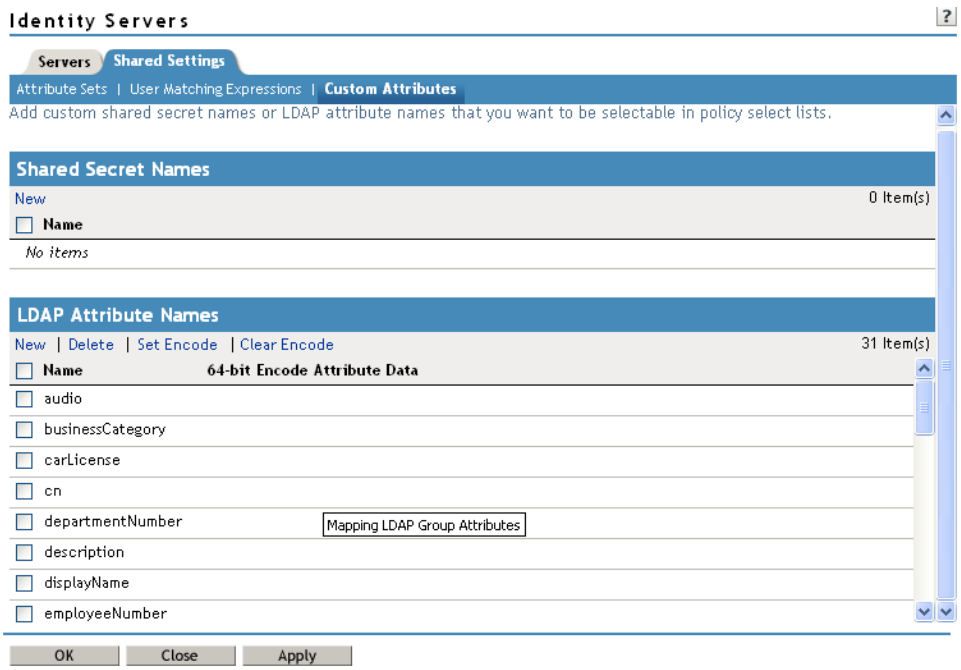
The LDAP attribute that is added in this section is an LDAP attribute assigned to the User class in eDirectory. This attribute is used to assign users to the sales role.

1 In the Administration Console, click *Access Manager* > *Identity Servers* > *Shared Settings* > *Custom Attributes*.



2 In the *LDAP Attribute Names* section, click *New*, type `description` in the *Name* field, then click *OK*.

This adds the description attribute to the policy list of available LDAP attributes, and you can use this attribute to assign a role to your users.



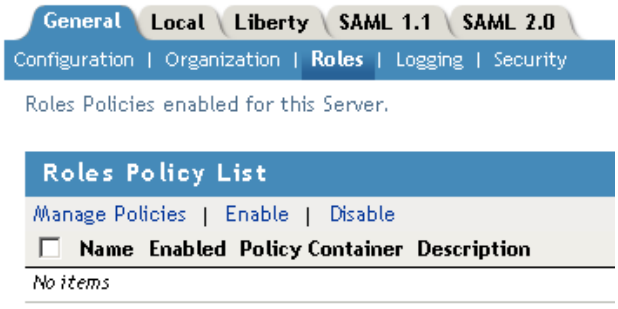
3 Click *OK*.

4 Continue with "Creating a Sales Role" on page 110.

Creating a Sales Role

Use the following procedure to create a sales role for the Digital Airlines example. (For more information about Role policies, see "Creating Role Policies" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.)

1 In the Administration Console, click *Access Manager* > *Identity Servers* > *Edit* > *Roles*.



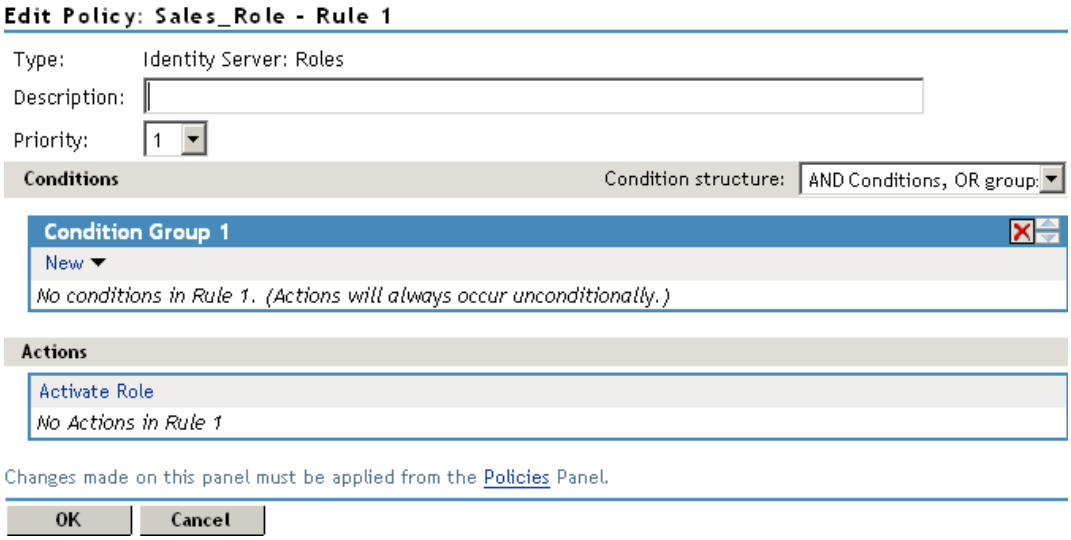
2 In the *Roles Policy List* section, click *Manage Policies*.

3 In the *Policy List* section, click *New,* then fill in the following fields:

Name: Specify *Sales_Role*.

Type: Select *Identity Server: Roles*.

4 Click *OK* to open the policy editor.



5 In *Condition Group 1*, click *New* > *LDAP Attribute*, and assign the following values:

LDAP Attribute: Select *description* (If *description* is not included in the *LDAP Attribute* list, you can add it from this page. For instructions, see Step 5a through Step 5c.)

Comparison: Select *String: Contains Substring*.

Mode: Select *Case Insensitive*.

Value: Select *Data Entry Field* (from the drop-down box); specify *Sales* as the value.

Result on Condition Error: Select *False.*

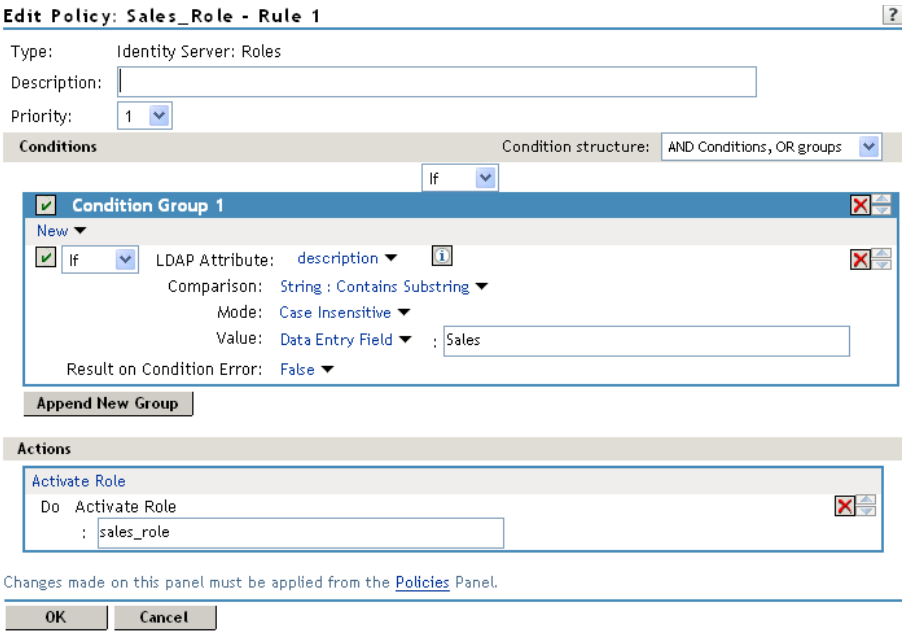
If the *description* attribute is not listed in the *LDAP Attribute* drop-down menu, create it by following this procedure:

5a In *Condition Group 1*, click *New* > *LDAP Attribute*, scroll to the bottom of the list, then click *New LDAP Attribute*.

5b In the *Name* field, specify *description*, then click *OK*.

5c In the *LDAP Attribute* field, select *description* from the drop-down menu.

6 In the *Actions* window, click *Activate Role*, then specify *sales_role* in the *Do Activate Role* field. Your rule should look similar to the following:

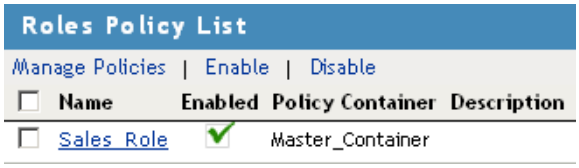


The value for *Activate Role* might be case sensitive. If you are going to inject this role into a policy for a Web server, and the page on the Web server is configured so that it evaluates case, make sure the value entered here matches what is expected on the Web server. The *Sales System* button on the Digital Airlines site requires that this value be lowercase: sales_role.

7 Click *OK* to close the Rule editor, then click *OK* to close the *Rule List*.

8 To save the Role policy, click *Apply Changes*, then click *Close* to return to the *Roles Policy List*.

9 In the *Roles Policy List*, select *Sales_Role,* then click *Enable*.



10 Click *OK*.

11 Click *Update* to update the Identity Server.

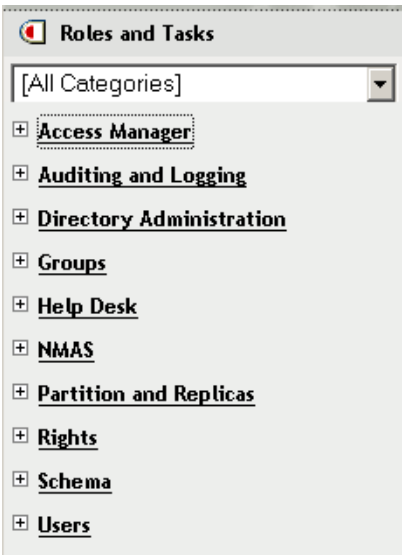
Wait for the *Status* to return to *Current*.

12 Continue with "Creating a New User with a Sales Role" on page 112.

Creating a New User with a Sales Role

After you have created a user policy, only users provisioned with that policy can access the protected Web resource. This section describes how to create a user that meets the conditions to be assigned the Sales role. These instructions assume that you are using the configuration store of the Administration Console as the LDAP user store. If you are using a different server than the LDAP user store, you need to modify these instructions:

1 In the Administration Console, click *Users*.



2 Click *Create User,* then fill in the following fields:

Username: Specify *Tom.*

First name: Specify *Tom.*

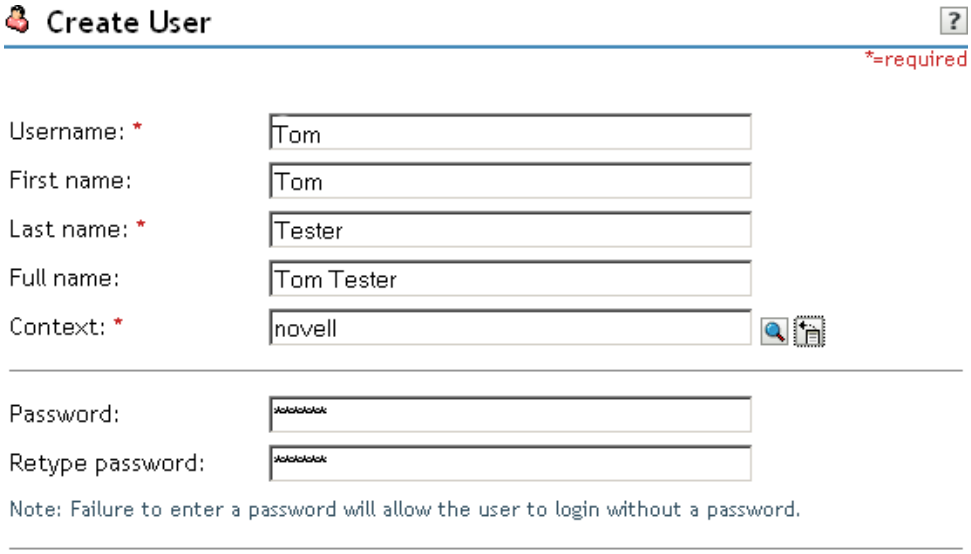
Last name: Specify *Tester.*

Context: Click the *Object Selector* icon, then click *novell*. The user is automatically assigned the context of *novell*.

Password: Assign a password to the user.

Retype password: Retype the assigned password.

Your user entry should look similar to the following:



3 Scroll to the *Description* field, then click the + icon.

4 In the *Add* text box, type `Sales` (initial uppercase), then click *OK* to return to the Create User page.

5 On the Create User page, click *OK*, then click *OK* to close the *Create User* task.

Tom meets the requirements to be assigned the Sales role when he logs in.

6 Continue with "Creating the Identity Injection Policy for a Custom Header" on page 114.

Creating the Identity Injection Policy for a Custom Header

The following policy injects the user's roles and DN into a custom header. The index.php page reads this information and uses it to display the user's name. If the user is assigned the sales_role, the *Sales System* button is displayed on the main page.

1 In the Administration Console, click *Access Manager* > *Access Gateways* > *Edit* > *DAL* > *Dallistener* > *Protected Resources* > *everything*.

2 Click *Identity Injection* > *Manage Policies*.

3 In the *Policy List* section, click *New*, then fill in the following:

Name: Specify *Custom_Injection*.

Type: Select *Access Gateway: Identity Injection*.

4 In the *Actions* section, click *New* > *Inject into Custom Header*.

5 To inject the user's name, fill in the following values:

Custom Header Name: Specify *X-Name*.

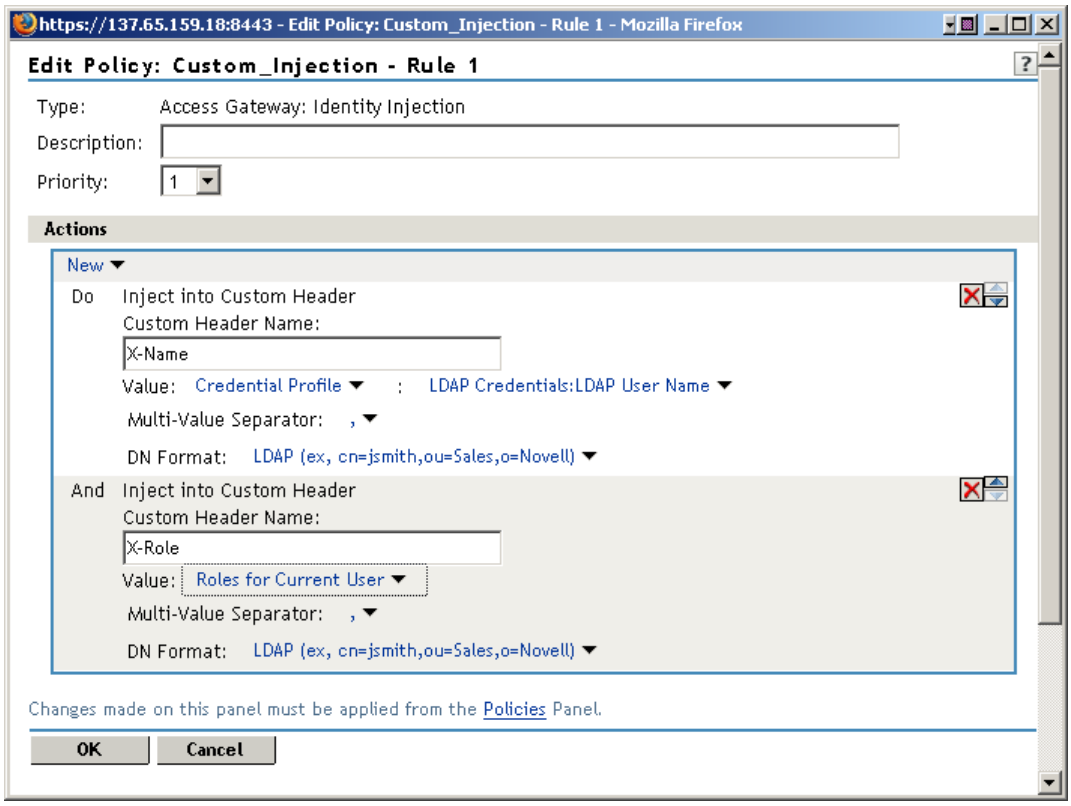
Value: Select *Credential Profile*. The *LDAP Credentials: LDAP User Name* is selected automatically for you.

6 To inject the user's roles, click *New* > *Inject into Custom Header*, then fill in the following values for the second custom header:

Custom Header Name: Specify *X-Role*.

Value: Select *Roles for Current User*.

Your policy should look similar to the following:



7 Click *OK* twice, then click *Apply Changes*.

8 Click *Close*.

9 In the *Identity Injection Policy List* section, select *Custom_Injection*, then click *Enable*.

10 Click *OK*.

11 Click the *Access Gateways* link, then click *Update* > *OK*.

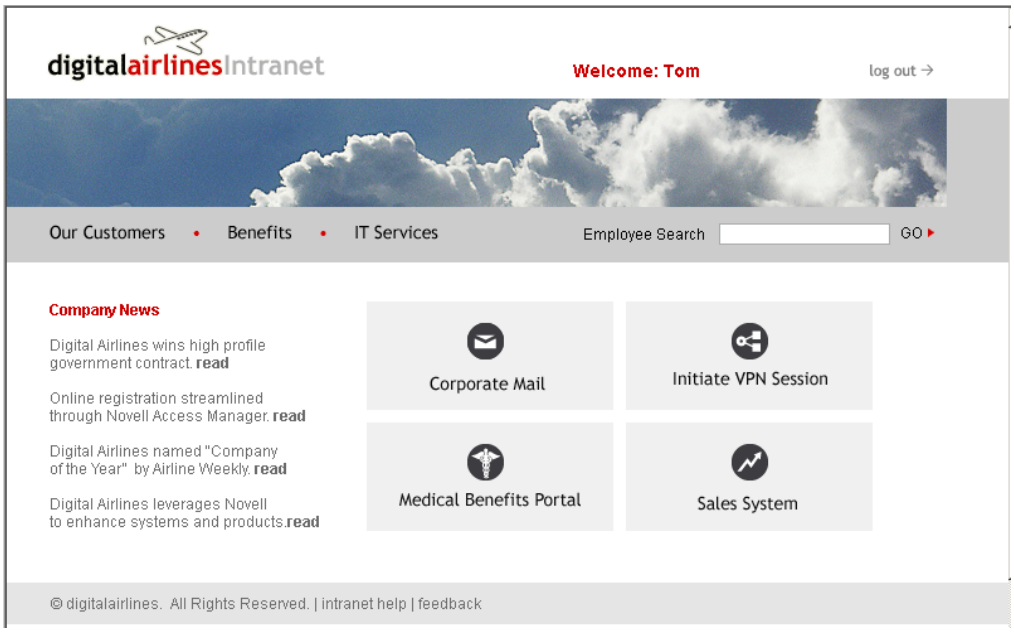
12 To test Tom's access rights, complete the following steps:

12a Open a new browser, then enter the URL of the Digital Airlines Web site you've created.

In this example, it is *am3bc.provo.novell.com*.

12b When prompted for user ID and password from Access Manager, log in with Tom's credentials.

The page appears with a *Welcome: Tom* message at the top and the *Sales System* button appears in the lower right-hand corner of the page.



12c Click the *Sales System* button, and the Sales page appears.

12d Close all sessions of the browser.

13 To test that the sales_role is required for the *Sales System* button to appear, complete the following steps:

13a Open a new browser, then enter the URL of the Digital Airlines Web site you've created.

In this example, it is *am3bc.provo.novell.com*.

13b Log in as the admin user. The page should have a *Welcome: admin* at the top of the page, but the *Sales System* button should not appear.

13c To the URL, add `/sales`, and the Sales page appears.

This illustrates that although the link is hidden, the Sales page is not protected.

13d Close all sessions of the browser.

14 Continue with Section 7.4.3, "Assigning an Authorization Policy to Protect a Resource," on page 116.

7.4.3 Assigning an Authorization Policy to Protect a Resource

Use the following procedure to limit access to the Sales page based on the Sales role:

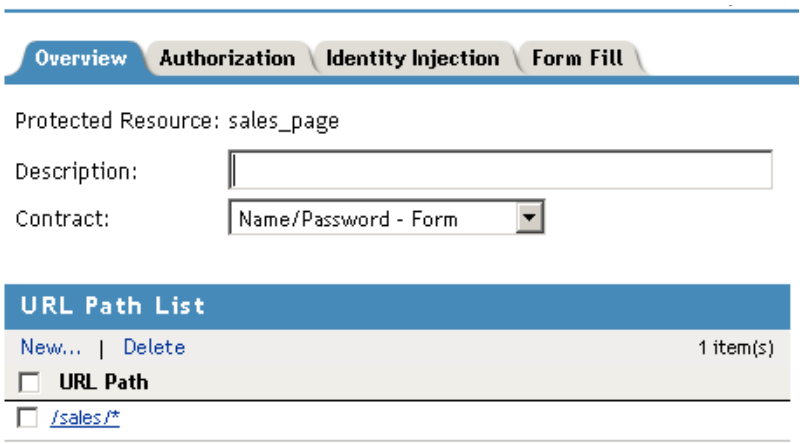
1 In the Administration Console, click *Access Manager* > *Access Gateways* > *Edit* > *DAL* > *Dallistener* > *Protected Resources*.

2 In the *Protected Resource List*, click New, specify `sales_page` for the name, then click OK.

3 For the *Contract*, select *Name/Password - Form*.

4 In the *URL Path List*, click `/*`, modify it to specify `/sales/*`, then click *OK*.

Your protected resource should look similar to the following:



5 Click *Authorization* > *Manage Policies*.

6 Click *New,* then fill in the following fields:

Name: Specify *Allow_Sales.*

Type: Select *Access Gateway: Authorization*.

7 Click *OK*.

The Edit Policy page appears.

8 In *Condition Group 1*, click *New* > *Roles for Current User*, then specify the following values:

Comparison: Select *String: Contains Substring*.

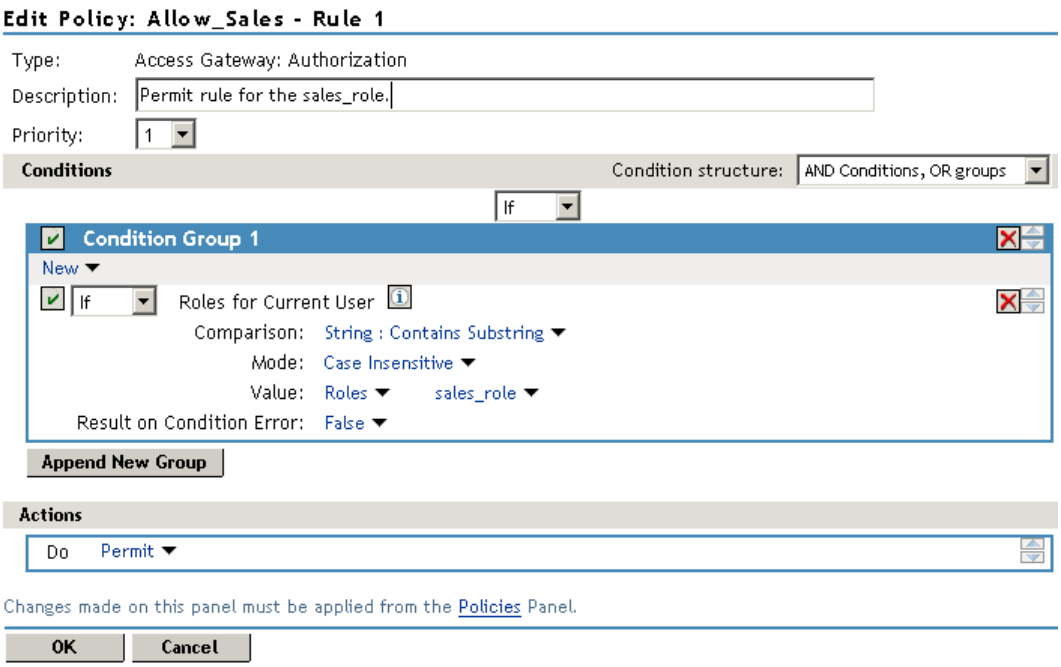
Mode: Select *Case Insensitive*.

Value: Select *Roles: sales_role.*

Return on Condition Error: Select *False.*

9 In the *Actions* section, ensure that *Permit* is selected.

Your rule should look similar to the following:



This rule allows everyone assigned to the sales_role to have access.

10 Click *OK*.

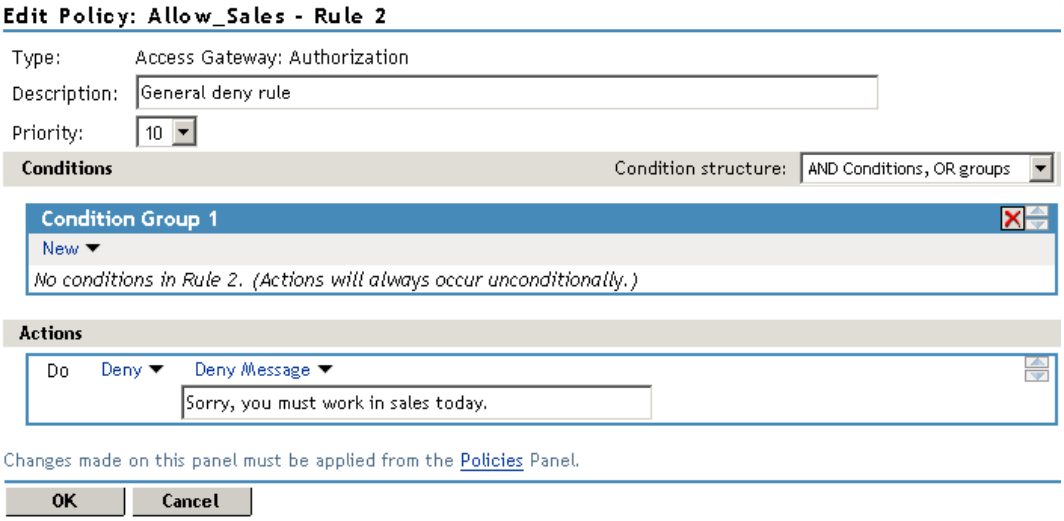
11 In the *Rule List*, select *New*.

This second rule is a general deny rule for everyone who has not been assigned the sales_role.

12 Make sure the *Priority* field is set to 10 and that the *Condition Group 1* has no conditions.

13 In the *Actions* section, click *Permit*, select *Deny*, then select *Deny Message*.

14 In the text box, type the deny message: *Sorry, you must work in sales today.* Your rule should look similar to the following.



With no conditions in the condition group, this creates a general deny rule that matches everyone. The users who have been assigned the sales role match the first rule that is processed. Everyone else matches this general deny rule.

15 Click *OK* to close the rule editor, then click *OK* to close the *Rule List*.

16 In the Policy List window, click *Apply Changes*, then click *Close*.

17 In the *Authorization Policy List*, select the *Allow_Sales* policy, then click *Enable*.

18 Click *OK*.

19 Click the *Access Gateways* link, then click *Update* > *OK*.

20 Test the results using the following procedure:

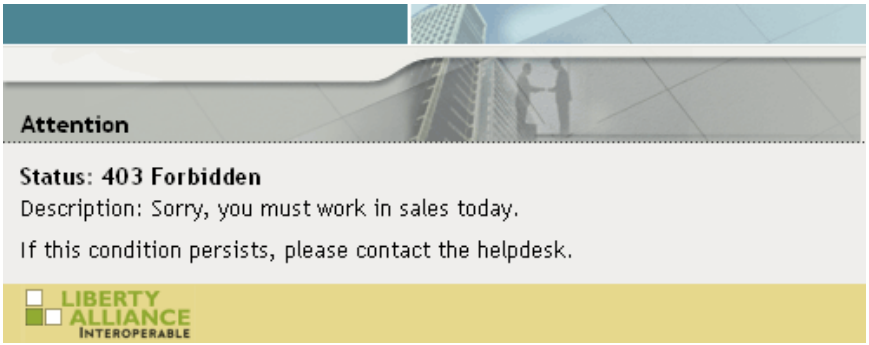
20a Open a new browser, then enter the URL of the Digital Airlines Web site you've created.

In this example, it is *am3bc.provo.novell.com*.

20b Log in as the admin user.

20c Add `/sales` to the URL.

You should receive the following response window with the message derived from the Access Gateway you just configured:



Now, only users with an assigned Sales role can access the Sales page.

21 Test the results with a user who has the Sales role.

21a Open a new browser, then enter the URL of the Digital Airlines Web site you've created.

In this example, it is *am3bc.provo.novell.com*.

21b Log in as Tom.

21c Click the *Sales System* button or add `/sales` to the URL.

The Sales page is displayed.

21d Close all sessions of the browser.

22 Continue with Section 7.4.4, "Configuring an Identity Injection Policy for Basic Authentication," on page 119.

7.4.4 Configuring an Identity Injection Policy for Basic Authentication

A common way to protect Web resources is to configure the Web server to require basic authentication for accessing a resource. The Web is configured to check for the user's name and password in the HTTP authentication header. If you have Web resources with this type of

configuration, you can enable single sign-on to these resources by creating a policy that injects the username and password into the HTTP authentication header.

This section explains how to set up the `/sales` directory to require basic authentication, and then how to create the Identity Injection policy.

- “Configuring the Web Server for Basic Authentication” on page 120
- “Creating an Identity Injection Policy for Basic Authentication” on page 122

Configuring the Web Server for Basic Authentication

It is difficult to create a configuration on the Apache Web server that provides consistent results by using LDAP SSL for basic authentication. Because this is a tutorial and is expected to be implemented in a testing environment, the following steps explain how to configure Apache to allow for a clear text password over LDAP and how to configure basic authentication in this environment. The purpose behind this section is not to explain how to configure Apache, but to explain how you can enable single sign-on for Web resources that require basic authentication.

- “Enabling LDAP Clear Text Passwords” on page 120
- “Enabling Basic Authentication” on page 120

Enabling LDAP Clear Text Passwords

To turn off the SSL requirement on the internal LDAP user store:

1. Log in to the Administration Console.
2. Click the *View Objects* icon  in the top menu bar.
3. Expand the `novell` container.
4. Browse to the `LDAP Group - <your server name>` object, click the link, then select *Modify Object*.
5. Select the *LDAP Allow Clear Text Password* attribute, then click *Edit*.
6. Select the check box, then click *OK*.
7. Click *OK* or *Apply* at the bottom of the page.

   If you do not click one of these buttons, your modifications are not saved.
8. To return the Administration Console machine to its default view, click the *Roles and Tasks* icon in the top menu bar.
9. From a terminal window on the Administration Console machine, log in as `root`.
10. Restart eDirectory with the following command:

    ```
    /etc/init.d/ndsd restart
    ```

Enabling Basic Authentication

You need to enable the Apache server to require basic authentication for the `/sales` directory. The procedure depends upon whether your Web server is installed on SLES 9.x or SLEX 10.x:

- “Configuring the Apache Server on SLES 10.x for Basic Authentication” on page 121
- “Configuring the Apache Server on SLES 9.x for Basic Authentication” on page 122

Configuring the Apache Server on SLES 10.*x* for Basic Authentication

On SLES 10.*x*, you need to enable two authentication modules and modify an Apache configuration file.

1. At the Apache server machine, log in to YaST.
2. Click *Network Services* > *HTTP Server* > *Server Modules*.
3. Scroll down, then enable the *ldap* and *authnz_ldap* modules.
4. Click *Finish*.
5. In a text editor, open the `/etc/apache2/httpd.conf` file.
6. Add the following section to the end of the file:

```
<Directory "/srv/www/htdocs/sales">
   Options Indexes FollowSymLinks
   AllowOverride None
   order allow,deny
   allow from all
   AuthType Basic
   AuthName Internal
   AuthBasicAuthoritative off
   AuthBasicProvider ldap
   AuthzLDAPAuthoritative off
   AuthLDAPURL ldap://127.0.0.1/o=novell?uid??(objectclass=*)
   require valid-user
   AuthLDAPBindDN cn=admin,o=novell
   AuthLDAPBindPassword novell
</Directory>
```

   Replace the information in the AuthLDAPURL line with the information the IP address of your LDAP user store. Modify the query string to match your user store. This sample line assumes that the Web server and your LDAP user store are installed on the Administration Console, and 127.0.0.1 is its internal address.

   The AuthLDAPBindDN and AuthLDAPBindPassword contain the distinguished name of a user and that user's password. This user needs sufficient rights to log in to the LDAP user store and to search for the users in the tree.

7. Restart the Apache server with the following command:

```
/etc/init.d/apache2 restart
```

8. To test that the `/sales` directory now requires basic authentication:

   8a Open a new browser, then enter the URL of the Digital Airlines Web site you've created.

   In this example, it is *am3bc.provo.novell.com*.

   8b Log in using the credentials for Tom.

   Even though Tom has logged in and been assigned the correct role, he is prompted to log in again to access the `/sales` directory. To enable single-sign on, you must create an Identity Injection policy that injects Tom's credentials into the authentication header.

9. Continue with "Creating an Identity Injection Policy for Basic Authentication" on page 122.

Configuring the Apache Server on SLES 9.*x* for Basic Authentication

On SLES 9.*x*, you need to modify an Apache configuration file.

1 At the Apache server machine, add the following section to the end of the `/etc/apache2/httpd.conf` file:

```
LoadModule ldap_module /usr/lib/apache2/mod_ldap.so
LoadModule auth_ldap_module /usr/lib/apache2/mod_auth_ldap.so

<Directory "/srv/www/htdocs/sales/">
   AuthType Basic
   AuthName "Sales"

   AuthLDAPURL ldap://127.0.0.1/o=novell?uid?sub
   AuthLDAPBindDN "cn=admin,o=novell"
   AuthLDAPBindPassword "novell"
   require valid-user
</Directory>
```

The AuthLDAPURL line is configured for the internal IP address of the Administration Console. If you have installed your Web server on a different machine, replace the 127.0.0.1 address with the IP address of your LDAP user store. In this configuration, this is the IP address of the Administration Console because we are using the internal configuration store as the LDAP user store.

The `AuthLDAPBindDN` and `AuthLDAPBindPassword` lines need to contain the DN and password of the administrator for the Administration Console. If you are using a different LDAP user store, make sure the search context (o=novell), the DN of the admin user, and the password are correct for your LDAP user store.

2 Restart the Apache server with the following command:

```
/etc/init.d/apache2 restart
```

3 To test that the `/sales` directory now requires basic authentication:

3a Open a new browser, then enter the URL of the Digital Airlines Web site you've created.

In this example, it is *am3bc.provo.novell.com*.

3b Log in using the credentials for Tom.

Even though Tom has logged in and been assigned the correct role, he is prompted to log in again to access the `/sales` directory. To enable single-sign on, you must create an Identity Injection policy that injects Tom's credentials into the authentication header.

4 Continue with "Creating an Identity Injection Policy for Basic Authentication" on page 122.

Creating an Identity Injection Policy for Basic Authentication

This section explains how to enable single-sign by creating an Identity Injection policy that injects the user's authentication credentials into a header. The Web server uses the credentials in the authentication header to satisfy its login requirements.

1 In the Administration Console, click *Access Manager* > *Access Gateways* > *Edit* > *DAL* > *Dallistener* > *Protected Resources*.

2 In the *Protected Resource List*, click *sales_page*.

3 Click *Identity Injection* > *Manage Policies* > *New*.

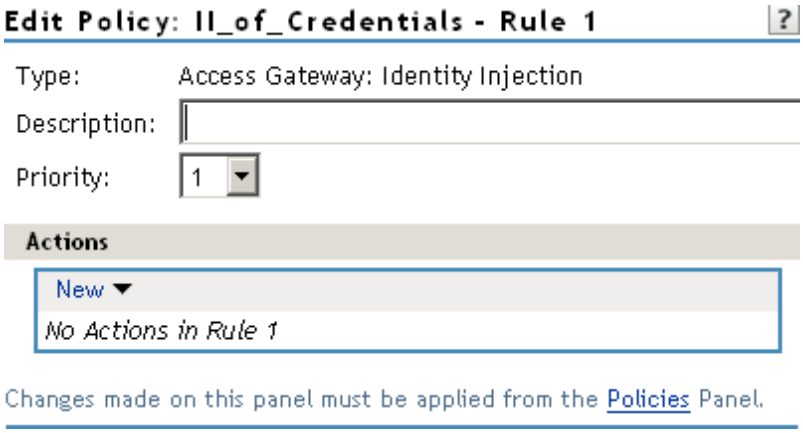
4 For the new policy, fill in the following fields:

Name: Specify *II_of_Credentials* for the name.

Type: Select *Access Gateway: Identity Injection* for the type.

5 Click *OK*.

The Edit Policy page opens so you can create a rule for the *II_of_Credentials* policy.

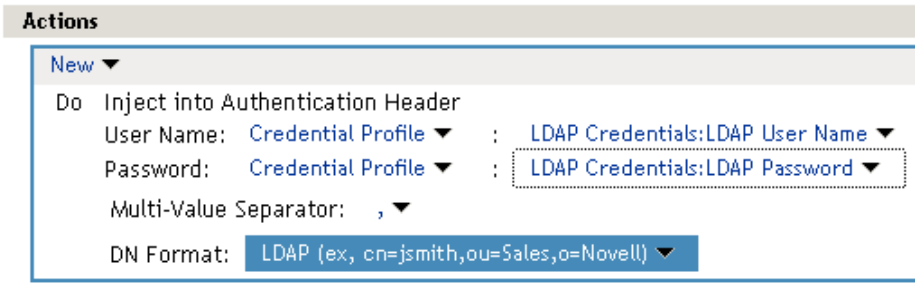


6 Click *New*, select *Inject into Authentication Header*, then select the following values:

User Name: Select *Credential Profile*. The *LDAP Credentials: LDAP User Name* value is automatically selected for you. This credential is the cn attribute of the user.

Password: Select *Credential Profile*. Click *LDAP Credentials: LDAP User Name*, then select *LDAP Credentials* > *LDAP Password*.

Your policy should look similar to the following:

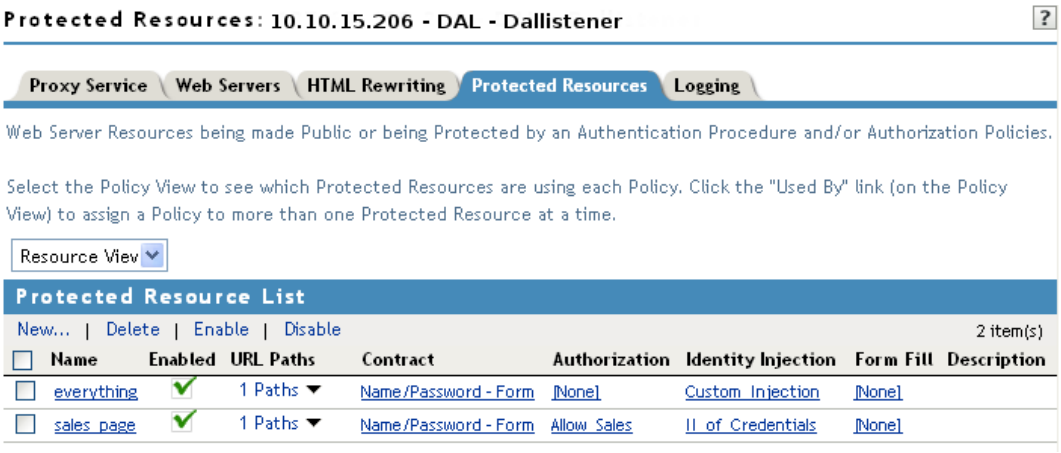


7 Click *OK* to close the policy editing page, then click *OK* to close the Rule List page.

8 In the Policy List page, click *Apply Changes*, then click *Close*.

9 Select the *II_of_Credentials* check box, click *Enable*, then click *OK*.

10 Click *OK* to return to the *Protected Resource List*. Your list should look similar to the following:



11 To save your configuration changes, click the *Access Gateways* link, then click *Update* > *OK*.

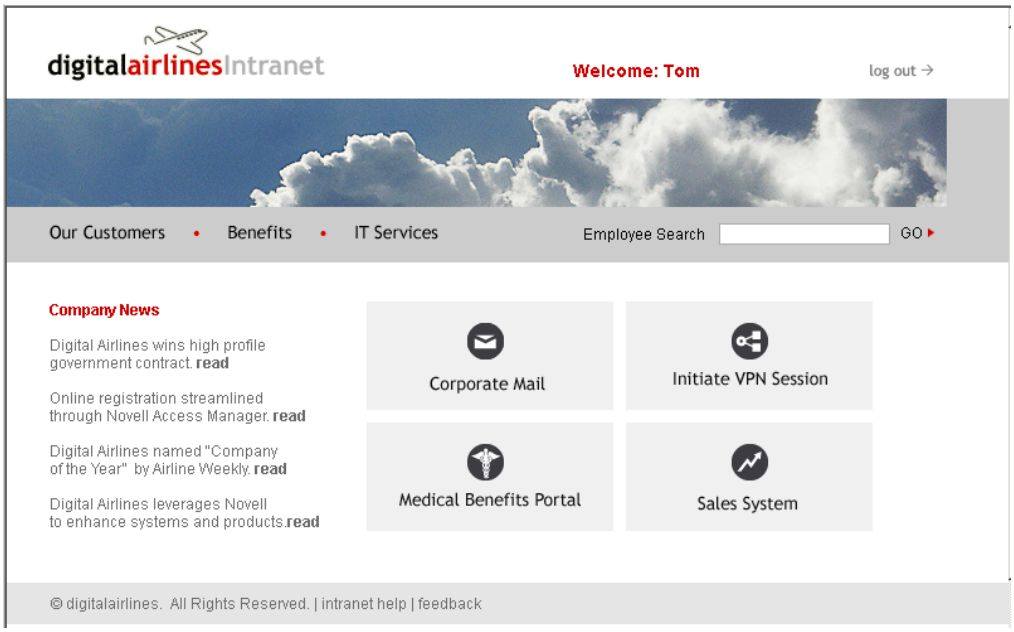
12 To test the configuration:

12a Open a new browser, then enter the URL of the Digital Airlines Web site you've created.

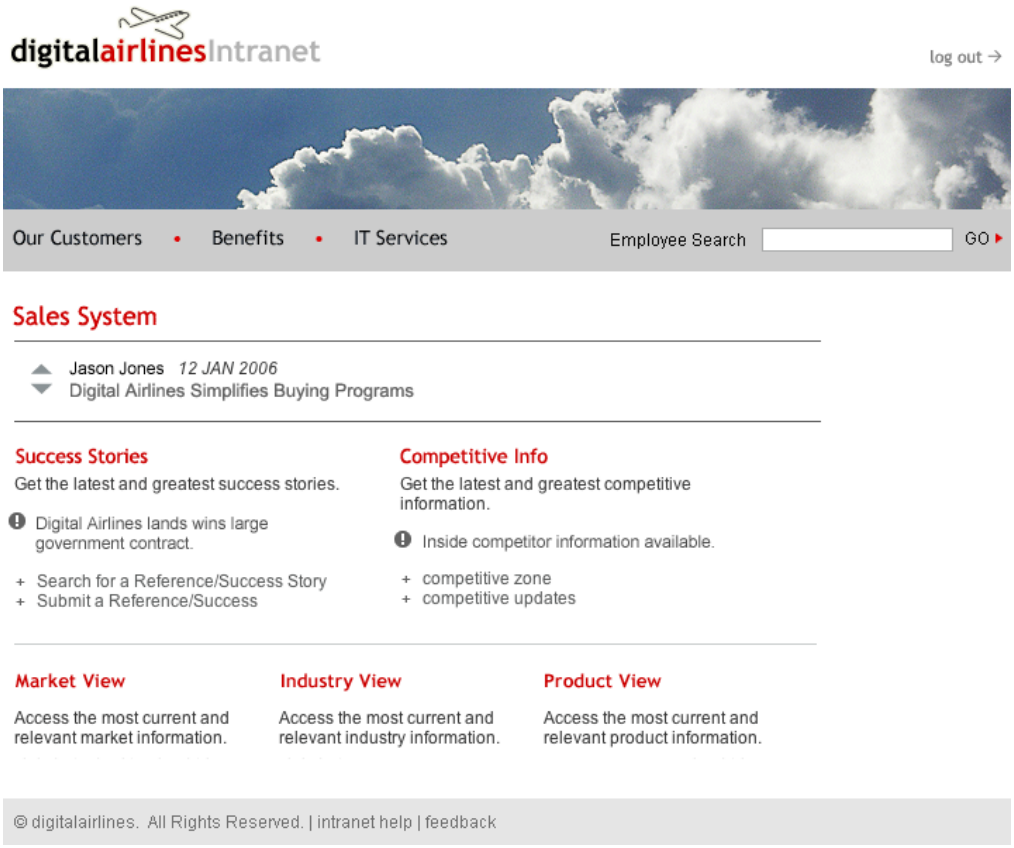
In this example, it is *am3bc.provo.novell.com*.

12b Log in as Tom.

The Digital Airlines site should appear with the *Sales System* button.



12c Click the *Sales System* button. You should have access to the Sales System site, as shown below:



For more information about Identity Injection policies, see "Creating Identity Injection Policies" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

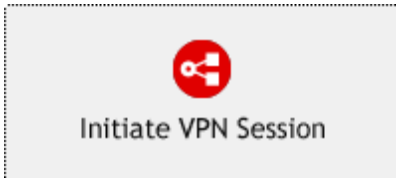
12d Close all sessions of the browser.

13 Continue with Section 7.4.5, "Initiating an SSL VPN Session," on page 125.

7.4.5 Initiating an SSL VPN Session

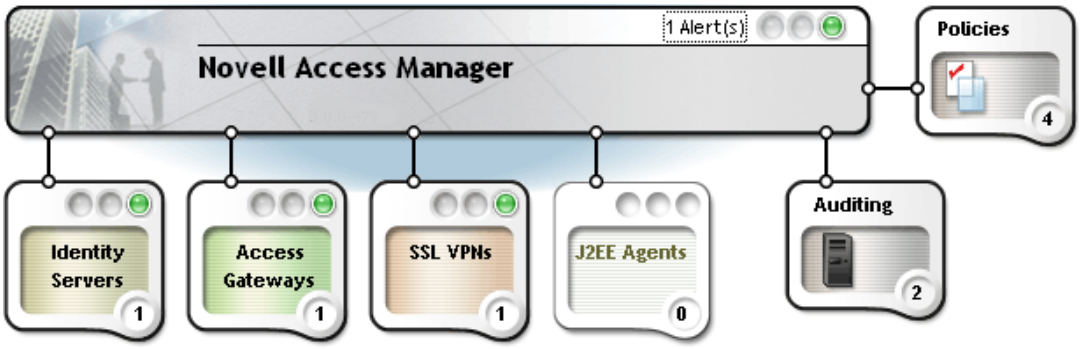
This section explains how to initiate an SSL Virtual Private Network (VPN) connection in the Digital Airlines example. The SSL VPN agent provides secure access to non-HTTP applications.

Figure 7-4 *GUI Button to Initiate an SSL VPN Session*



Before performing this task, you must have the SSL VPN agent installed on either your Identity Server or on your Linux Access Gateway. Your Access Manager console should appear similar to the green state shown in Figure 7-5:

Figure 7-5 *Access Console Indicating the Status of Access Manager Components*



For more information about installing the SSL VPN server, see "Installing SSL VPN" in the *Novell Access Manager 3.0 SP3 IR2 Installation Guide*.

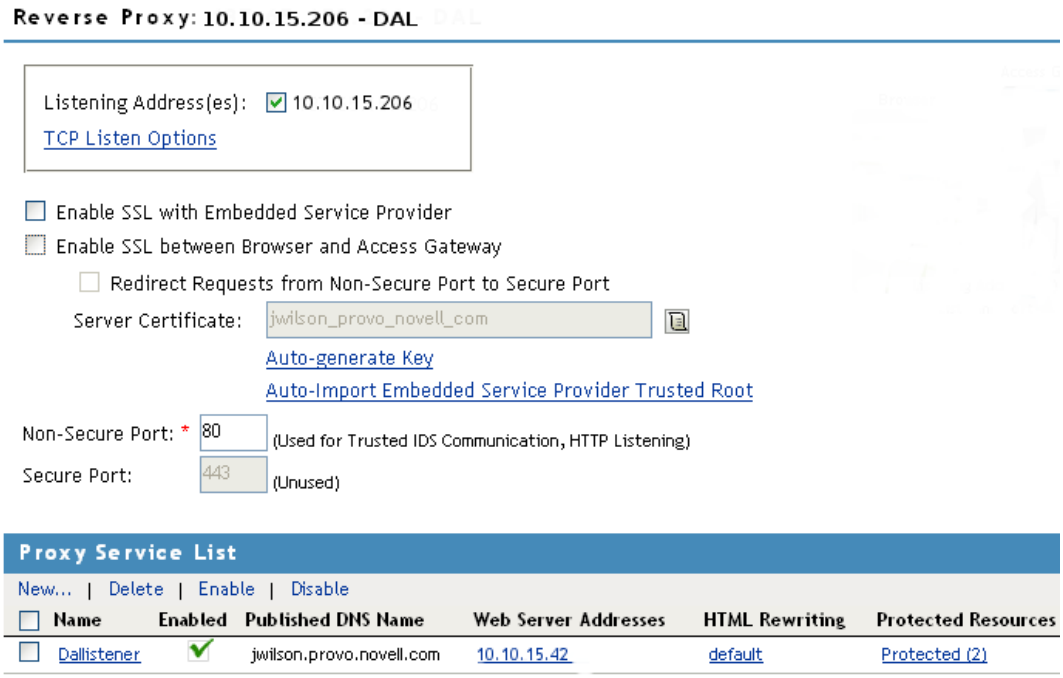
For the Digital Airlines example, you will perform the following tasks:

- "Configuring the SSL VPN as a Protected Resource" on page 126
- "Creating an SSL VPN Protected Resource and Identity Injection Policy" on page 127
- "Testing the SSL VPN Basic Configuration" on page 128
- "Configuring a Traffic Policy" on page 129

Configuring the SSL VPN as a Protected Resource

To configure the SSL VPN as protected resource, you must first create a reverse proxy for it.

1 In the Administration Console, click *Access Manager* > *Access Gateways* > *Edit* > *DAL*.



2 In the *Proxy Service List*, click *New*, then provide the following values:

Proxy Service Name: Specify *sslvpn*.

Multi-Homing Type: Select *Path-Based*. (For more information about accessing multiple resources, see "Using Multi-Homing to Access Multiple Resources" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.)

Path: Specify */sslvpn*.

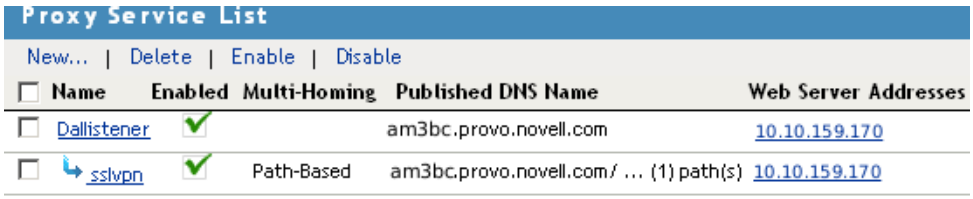
Web Server IP Address: Specify the IP address of SSL VPN server.

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*.

The Reverse Proxy window is displayed.



4 In the *Proxy Service List*, click *sslvpn* > *Web Servers*.

5 Change the *Connect Port* from *80* to *8080*, then click *OK*.

6 Continue with "Creating an SSL VPN Protected Resource and Identity Injection Policy" on page 127.

Creating an SSL VPN Protected Resource and Identity Injection Policy

1 In the *Proxy Service List*, select the *sslvpn*.

2 In the *Path List*, select the *SSLVPN* check box, then click *Enable SSL VPN*.

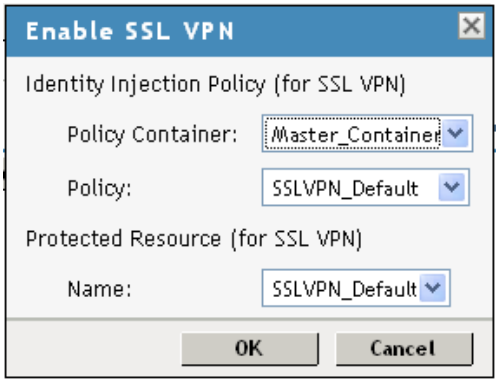
3 Fill in the following fields:

Policy Container: Select *Master_Container*.

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

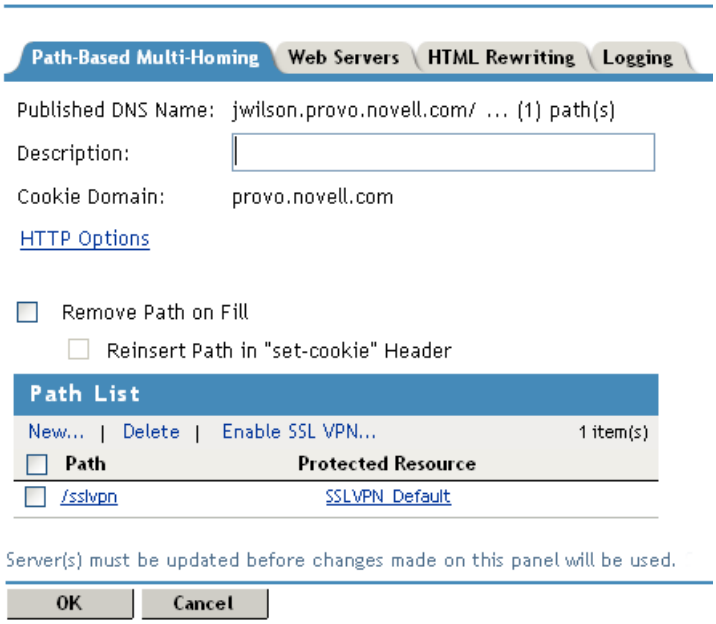
Name: Select *Create SSL VPN Default Protected Resource*.

Your configuration should look like the following:



4 Click *OK*.

The *Create SSL VPN Default Protected Resource* option creates a protected resource, creates a default SSL VPN identity injection policy, then assigns it to the protected resource. When it completes, the */sslvpn* Path should now indicate *SSLVPN_Default* as the Protected Resource.



5 Click *OK*.

6 Click the *Access Gateways* link, then click *Update* > *OK*.

Testing the SSL VPN Basic Configuration

Basic configuration of the SSL VPN is complete after it is protected behind your gateway and you have built your necessary identity injection policies. Test your basic configuration with the following procedure:

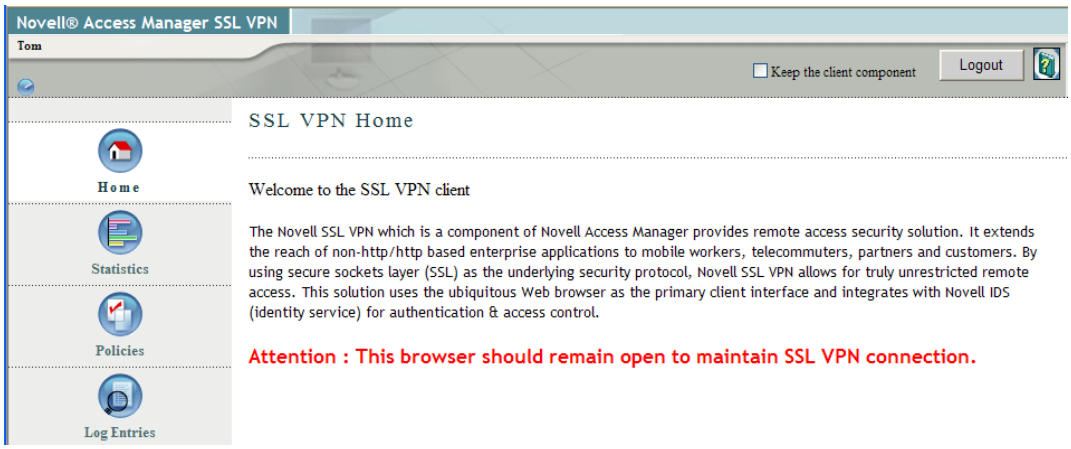
1 To access the SSL VPN servlet, open a new browser and enter *http://am3bc.provo.novell.com*.

2 Log in with any authorized username and password that is registered within your corporate domain, including the user you created in "Creating a New User with a Sales Role" on page 112.

3 Click the *Initiate VPN Session* link.

4 If requested, click *OK* to accept the certificate for the SSL VPN client.

5 Verify that the SSL VPN client downloads, installs, and runs:



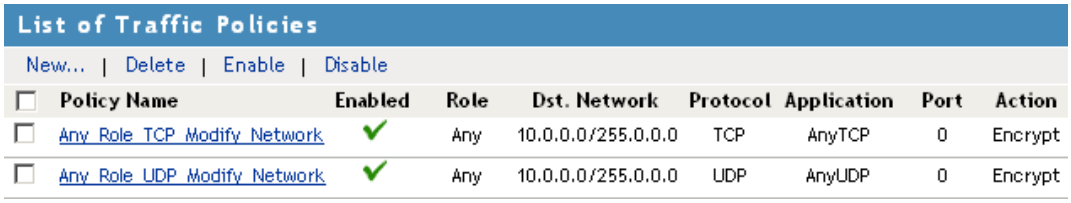
Notice that the user's first name ("Tom") is injected into the header of the SSL VPN browser.

6 Click *Logout*, then close the browser.

Configuring a Traffic Policy

Traffic policies allow you to control access to different networks and applications protected behind the SSL VPN. Simulate this by creating a rule that allows access to your network:

1 In the Administration Console, click *Access Manager* > *SSL VPNs* > *Edit* > *Traffic Policies*.



2 Click *New*, type *sales*, then click *OK*.

3 In the Traffic Policies list, select the *sales* check box, then click *Enable*.

4 Click the new, enabled sales policy, then provide the following values:

Role: *sales_role*. Specify this value in the *Role* field after clicking the + icon.

Destination Network: *10.0.0.0*. This field is usually prepopulated, or you can specify the IP address of the SSL network.

Network Mask: *255.0.0.0*. This field is usually prepopulated, or you can specify the value for your destination network.

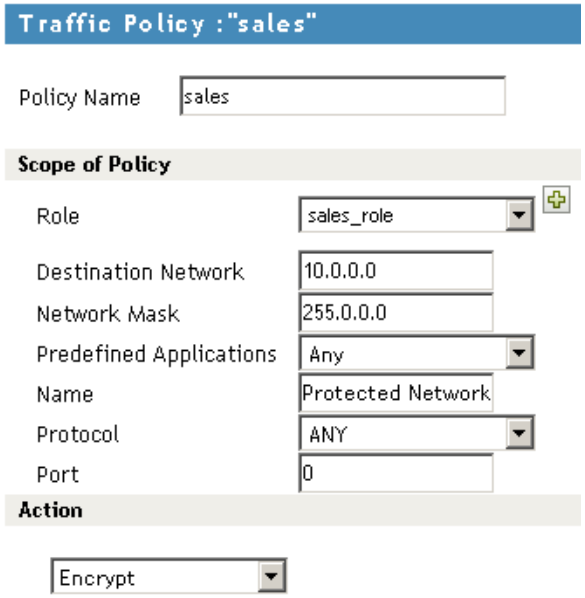
Predefined Application: *Any.* You can also select from drop-down list to specify your network application.

Name: *Protected Network*. You can also provide any descriptive name for the SSL network.

Protocol: *Any*. Specifies whether the protocol is *ICMP*, *UDP*, *TCP*, or *Any*.

Port: *Port*. Specifies the port number on which the service you select listens. The value of 0 allows all ports.

Action: *Encrypt*. Specifies whether the service can be encrypted or denied.



5 Click *OK* to save the configuration and return to the List of Traffic Policies page.

6 Click *OK* twice, then on the SSL VPNs page, click *Update*.

7 Test the traffic rule:

7a Open a new browser session and enter *http://am3bc.provo.novell.com/sslvpn/login*.

7b Log in as *admin* user of the Administration Console.

7c In the left navigation window, click *Policies*.

Notice that without a sales role, the *admin* user has no access to the Digital Airlines network. Access is granted only when you log in with your *sales* credentials created in "Creating a New User with a Sales Role" on page 112.

7d Log out of the SSL VPN session.

7e Open a new SSL VPN browser session and enter *http://am3bc.provo.novell.com/sslvpn/login*.

7f Log in as Tom. (See "Creating a New User with a Sales Role" on page 112.)

7g In the left navigation window, click *Policies*.

Notice that the user "*tom*" is now assigned a *sales_role* on the SSL VPN server.

For more information about Traffic Policies, see "Configuring Traffic Policies" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

7.5 Modifying the Digital Airlines Example

The Digital Airlines example is a relatively simple server-side Web application that consists of a predefined PHP framework and its associated database, HTML, and graphic files. Although creating more robust Web applications for your actual production environment is outside the scope of this document, you might want to demonstrate the capabilities of Access Manager by using an example more tailored to your company.

This section explains how you change the look and feel of the Digital Airlines example by replacing its graphics with those you create yourself:

- Section 7.5.1, "Prerequisites," on page 132
- Section 7.5.2, "Understanding the Example Files," on page 132
- Section 7.5.3, "Updating Static Graphics," on page 132
- Section 7.5.4, "Updating Mouse-Over Links," on page 135
- Section 7.5.5, "Deploying Your Updated Example Web Service," on page 135

7.5.1 Prerequisites

- Download and install the Digital Airlines example directory from the Novell Access Manager Demos Wiki site (http://developer.novell.com/wiki/index.php/Nam-demos).
- Create your own proprietary graphic files in GIF format to replace those in the default Digital Airlines example.
- Select a suitable PHP or HTML editor that enables you to open, view, and edit the example source files.

  Although you can edit files using a simple text-only editor, making changes to the example files is simpler if you use a more robust program that displays the source code integrated with your graphic files.

7.5.2 Understanding the Example Files

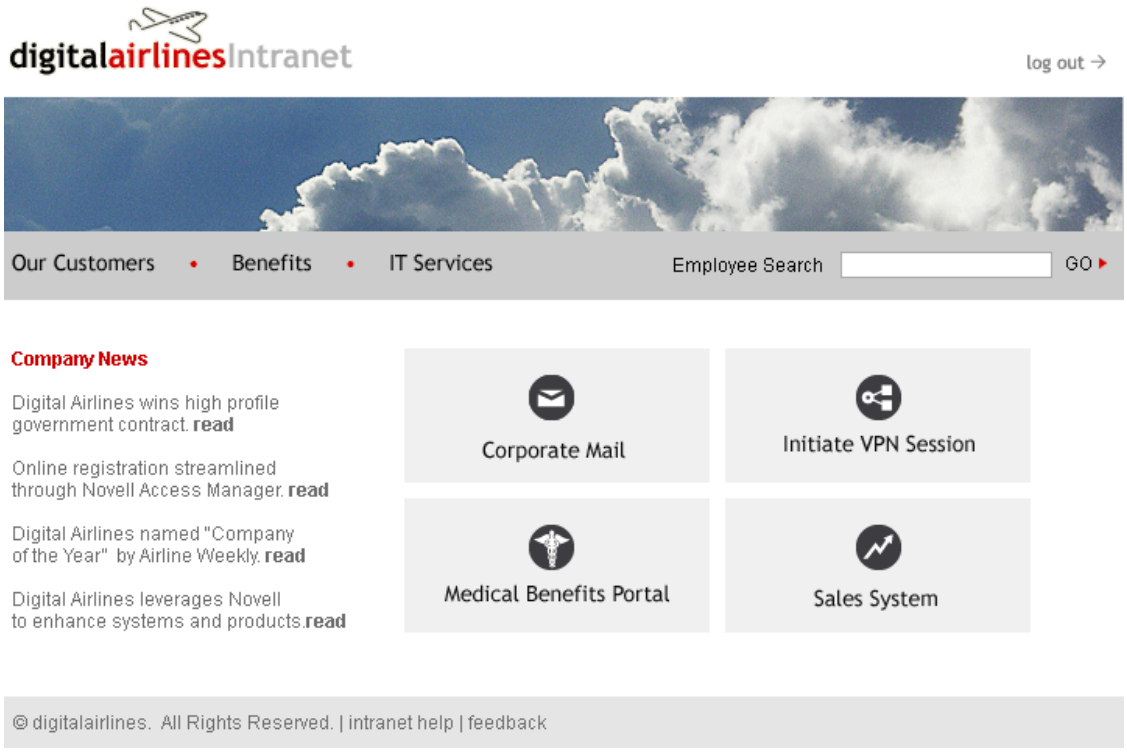
The files provided with the Digital Airlines example can be altered to meet your needs. The `index.php` and `sales.php` files in the htdocs directory are the master configuration files that define the visual appearance and functionality of the Web site. Other folders in the `htdocs` directory contain the image and database reference files required and specified by the PHP files.

Although you can change the functionality of this example by altering the PHP files, this document describes only how to integrate new graphic files into the existing database structure. By working through the Digital Airlines example, you should understand how to deploy Access Manager to protect your own Web services in a production environment.

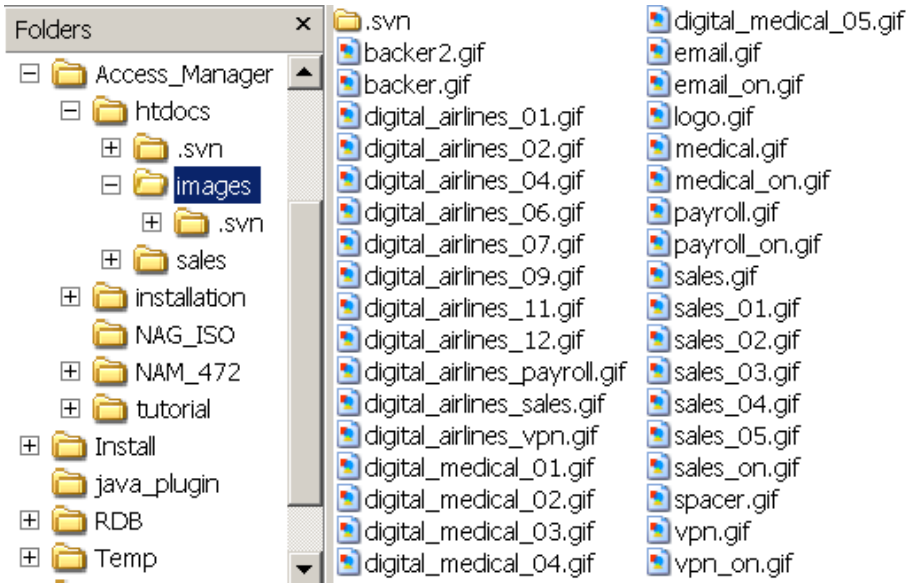
7.5.3 Updating Static Graphics

You can easily update any of the graphic files contained in the Digital Airlines example:

Figure 7-6 *Digital Airlines Composite GUI*



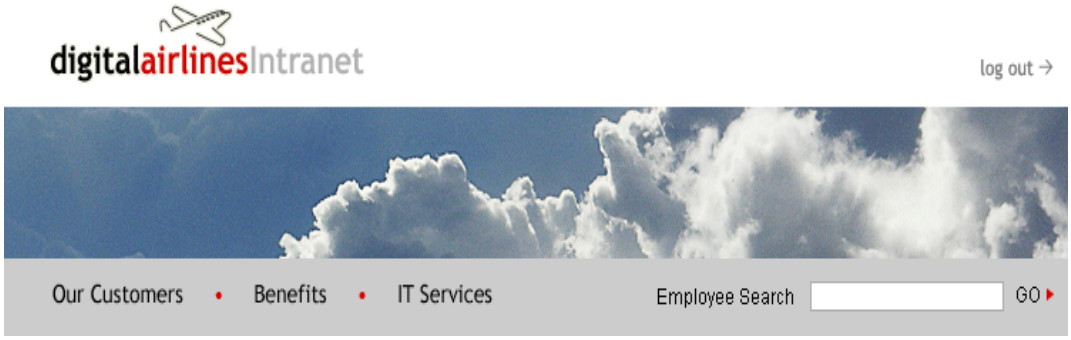
1 Navigate to the `htdocs` directory where your Digital Airlines components are located and open the `images` directory.



2 Open any of the GIF files to view the images you might want to replace.

For example, you might want to replace the Digital Airlines main header file with the look and feel of your own company:

Figure 7-7 *digital_airlines_01.gif*



3 Remember the name of this file, `digital_airlines_01.gif`.

4 Open the `index.php` file in an editor and search for `digital_airlines_01.gif`.

```
<div style="position:absolute; left:680px; top:42px;color:6a696a;font: 12px arial"> <a href="/plogout"></a></div>.
<table id="Table_01" width="747" height="700" border="0" cellpadding="0" cellspacing="0">.
        <tr>.
          <td colspan="5">.
                <img src="images/digital_airlines_01.gif" width="747" height="233" alt=""></td>.
        </tr>.
        <tr>.
```

5 In the PHP code, notice the dimensions of the graphic are 747 pixels wide and 233 pixels high.

6 Create your own main header graphic file (*`your_company`*`_01.gif`) with approximately the same dimensions as the Digital Airlines graphic (`digital_airlines_01.gif`).

NOTE: Although your replacement graphics do not need to be exactly the same size, try to create the new files as close to the original size as possible to avoid possible display problems.

---

7 Replace the old `digital_airlines_01.gif` with your new `your_company_01.gif`.

8 In the PHP code editor, replace the old `digital_airlines_01.gif` name with your new `your_company_01.gif` string.

```
<div style="position:absolute; left:680px; top:42px;color:6a696a;font: 12px arial"> <a href="/plogout"></a></div>.
<table id="Table_01" width="747" height="700" border="0" cellpadding="0" cellspacing="0">.
        <tr>.
          <td colspan="5">.
                <img src="images/your_company_01.gif" width="747" height="233" alt=""></td>.
        </tr>.
        <tr>.
```

The PHP code points to this GIF file and the Web service will display it in the proper location and format when the HTML page is called.

9 Save the `index.php` file.

10 Repeat this procedure for every graphic in your sample that you want to replace, except mouse-over links. For this procedure, see Section 7.5.4, “Updating Mouse-Over Links,” on page 135.

IMPORTANT: Check and update all of the sample graphics to give your own Web site a consistent look according to the design criteria of your company.

7.5.4 Updating Mouse-Over Links

Mouse-over links are dynamic links on your HTML Web page that change appearance when a user moves the mouse pointer over the link. Each of these links require two separate GIF files, one dormant file that displays normally on the Web page (Figure 7-8) and one active file, designated with the `_on` extension in its name, that is displayed when the mouse pointer hovers on the link (Figure 7-9).

Figure 7-8 *Dormant medical.gif*

Figure 7-9 *Active medical_on.gif*

The `index.php` file always defines where and how your GIF files are displayed on the active HTML Web page, as shown in the following code sample:

```
91        <tr>.
92                <td><a href="http://spd.provo.novell.com:8080/nidp" onMouseOut="MM_swapImgRestore()" .
93                onMouseOver="MM_swapImage('Image15','','images/medical_on.gif',1)">.
94                <img src="images/medical.gif" name="Image15" width="196" height="86" border="0"></a></td>.
95                <td>.
```

The following procedure explains how to update these mouse-over links with your own replacement graphics:

1. Follow the procedure outlined in Step 1 through Step 6 on page 134 for the mouse-over links that you want to update.

   Keep in the mind the pixel size requirements specified for your GIF files in `index.php`.
2. Name your new files *`[your_link]`*`.gif` and *`[your_link]`*`_on.gif`.
3. In the `htdocs/images` folder, replace the original dormant and active GIFs with your new *`[your_link]`*`.gif` and *`[your_link]`*`_on.gif` files.
4. In the PHP code editor, search for all instances of the `old medical.gif` and `medical_on.gif` files and replace with your new *`[your_link]`*`.gif` and *`[your_link]`*`_on.gif` files.
5. Save the `index.php` file.

7.5.5 Deploying Your Updated Example Web Service

After you have updated and saved your PHP and graphics files in the htdoc sample folder, deploy the Web service explained in Section 7.1, “Installation Overview and Prerequisites,” on page 97.

Creating Novell Audit Queries

8

The following instructions explain how to configure the Novell® Audit server that is installed on the Administration Console to use the MySQL open source database for queries. After you understand how to set up Novell Audit to use the MySQL database, you can adopt the process for the other databases and for remote Novell Audit servers.

- Section 8.1, "Setting Up the MySQL Database," on page 137
- Section 8.2, "Logging Events to the MySQL Database," on page 138
- Section 8.3, "Configuring Queries," on page 143

8.1 Setting Up the MySQL Database

- Section 8.1.1, "Prerequisites," on page 137
- Section 8.1.2, "Preparing MySQL for Novell Audit Connectivity," on page 137
- Section 8.1.3, "Installing the JDBC Driver," on page 138

8.1.1 Prerequisites

- You have downloaded the MySQL Community Server 5.0 and client from MySQL (http://dev.mysql.com/downloads/mysql/5.0.html#downloads). Select the version applicable to your platform.

  The instructions in this section are based on installing MySQL on SUSE Linux Enterprise Server 9, but most of the instructions are the same for all platforms.
- You have installed the MySQL server and client on the same machine.

  For more information, see "Installing and Upgrading MySQL" (http://dev.mysql.com/doc/refman/5.0/en/installing.html) in the *MySQL 5.0 Reference Manual*.
- You have set up security, if desired, for the `root` user and the default users.
- You know how to log in to the database. For Linux, use the following command:

  ```
  mysql -u <username> -p <password>
  ```

  If you haven't set up security, use the following command:

  ```
  mysql -u root
  ```

  For more information, see "Connecting to and Disconnecting from the Server" (http://dev.mysql.com/doc/refman/5.0/en/connecting-disconnecting.html) in the *MySQL 5.0 Reference Manual*.

8.1.2 Preparing MySQL for Novell Audit Connectivity

1. Log in as `root` to MySQL.

   The prompt changes to a `mysql>` prompt.
2. Use the following commands to create a new database called `naudit` and to create the `auditusr`, who is granted all rights to the new database:

```
create database naudit;
grant all on naudit.* to auditusr@'%' identified by 'auditpwd';
grant all on naudit.* to auditusr@localhost identified by
'auditpwd';
exit;
```

The semicolons mark the end of a command and must be included as part of the command.

3 Continue with Section 8.1.3, “Installing the JDBC Driver,” on page 138.

8.1.3 Installing the JDBC Driver

The Auditing and Logging plug-in installed in the Administration Console requires a JDBC driver to connect to the MySQL database.

1 Download the JDBC driver to your Administration Console from MySQL (http://dev.mysql.com/downloads/connector/j/5.0.html).

2 On your Administration Console machine, log in as `root`.

3 Change to the directory where you downloaded the driver and untar the file by using the following command:

```
tar -xzvf mysql-connector-java-5.0.7.tar.gz
```

4 Use the following command to copy the driver to its required location:

```
cp mysql-connector-java-5.0.7-bin.jar /var/opt/novell/tomcat4/
common/lib/
```

5 Change to the `/var/opt/novell/tomcat4/common/lib` directory.

6 Change the ownership of the driver by using the following commands:

```
chgrp novlwww mysql-connector-java-5.0.7-bin.jar
chown novlwww mysql-connector-java-5.0.7-bin.jar
```

7 Restart Tomcat by using the following command:

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

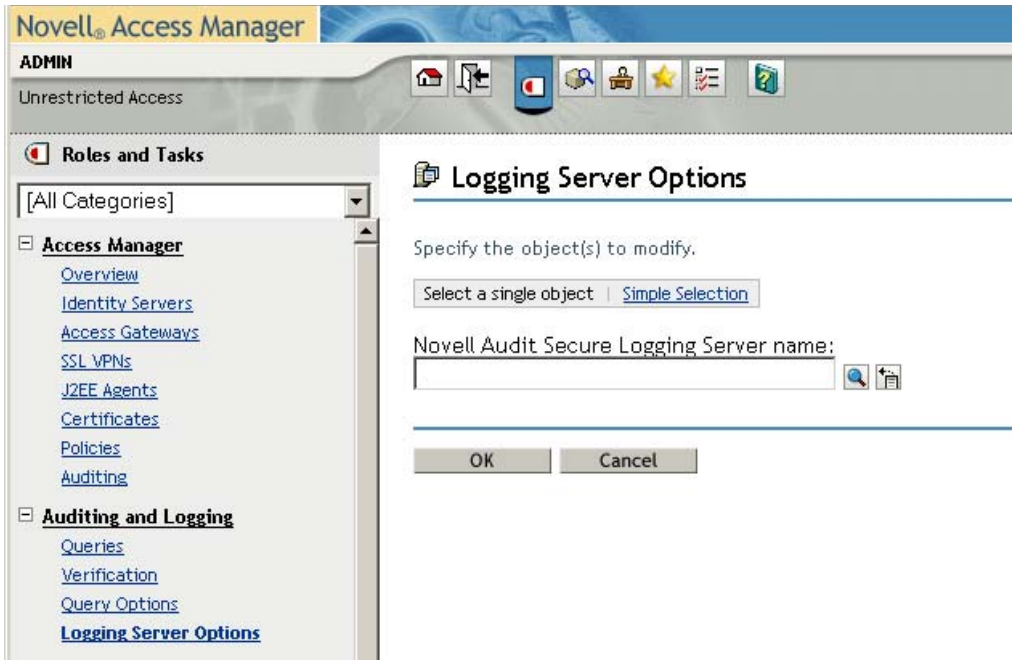
8.2 Logging Events to the MySQL Database

After you have created a MySQL database for the Novell Audit server and you have installed the driver, you can configure the Novell Audit Secure Logging Server so that it writes events to the MySQL server.

- Section 8.2.1, “Creating the MySQL Log Channel,” on page 138
- Section 8.2.2, “Configuring the Audit Server to Log Events to the MySQL Log Channel,” on page 140
- Section 8.2.3, “Configuring Access Manager Components to Log Audit Events,” on page 142

8.2.1 Creating the MySQL Log Channel

1 In the Administration Console, click *Auditing and Logging* > *Logging Server Options*.



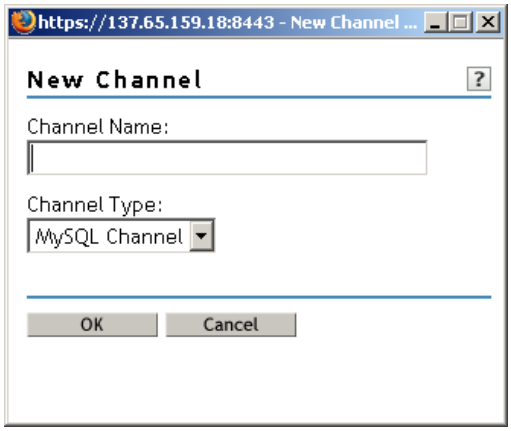
2 Use the *Object Selector* icon to find the Logging Services object and expand it.

3 Click the Logging Server object that has the hostname of your Administration Console prepended to it, for example `Jwilson1 Logging Server.Logging Services`.

4 Click *OK*.

5 On the Logging Server Options page, click the *Channels* tab.

6 Select *Container Name*, then click *Channel Actions* > *New*.

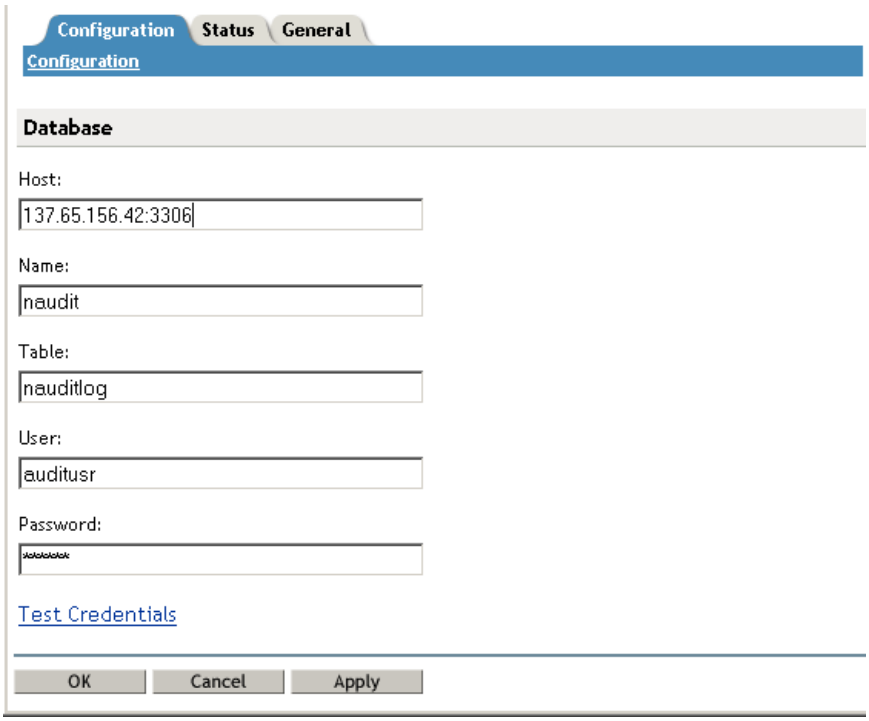


7 Fill in the following:

Channel Name: Specify *MySQL*.

Channel Type: Select *MySQL Channel*.

8 Click *OK*.



9 On the Configuration page, fill in the following:

Host: Specify the IP address of your MySQL server with a port of 3306. For example: *10.10.10.10:3306*.

Port 3306 is the default port for the MySQL 5.0 server. If you have configured your server to use a different port, enter it instead. If you are using a different version of MySQL, verify the port required by the JDBC driver.

Name: Specify *naudit*.

Table: Specify *nauditlog*.

User: Specify *auditusr*.

Password: Specify *auditpwd*.

10 Click *Test Credentials*, then enter the following in the *JDBC Class* field:

```
com.mysql.jdbc.Driver
```

11 Click *OK*.

You should receive a `Database test connection was successful` message. If you do not receive this message, verify your configuration information.

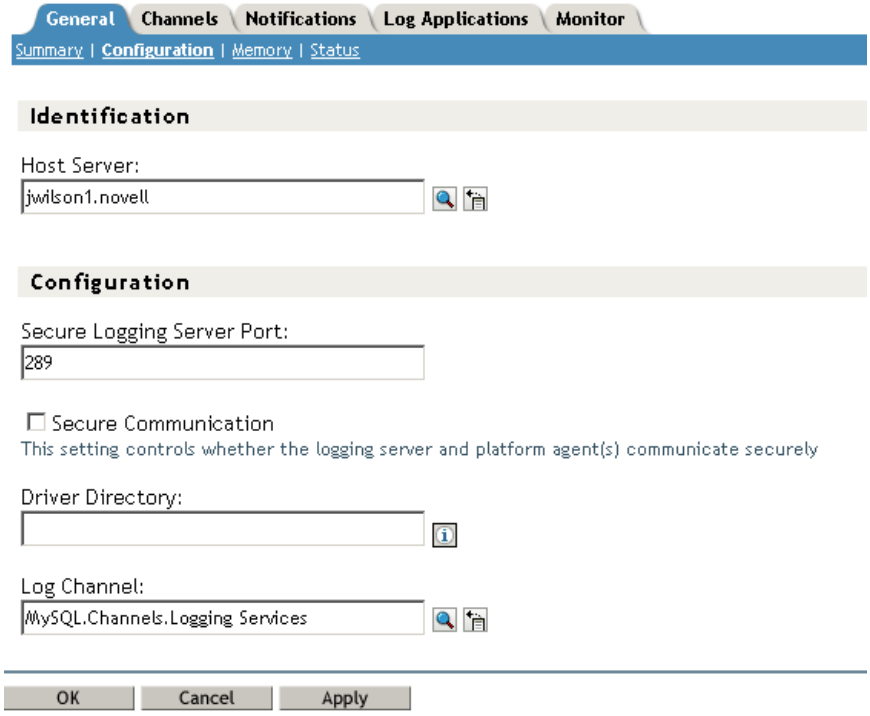
12 Click *OK*.

13 Continue with Section 8.2.2, “Configuring the Audit Server to Log Events to the MySQL Log Channel,” on page 140.

8.2.2 Configuring the Audit Server to Log Events to the MySQL Log Channel

1 On the Logging Server Options page, click the *General* tab, then click *Configuration*.

2 In the *Log Channel* field, click the *Object Selector* icon, expand the Channels object, then select the *MySQL* object.



The *Log Channel* field should now contain *MySQL.Channels.Logging Services* as its value.

3 To save the changes, click *Apply*.

4 Click *OK*.

5 To update the audit server with this new channel, complete the following steps from a terminal window on your Administration Console:

5a Stop the audit server by using the following command:

```
/etc/init.d/novell-naudit stop
```

5b Start the audit server by using the following command:

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

Starting the audit server causes the nauditlog table in the MySQL database to be created. The start -d option causes the console to appear. Leave it running for now so you can see when events start occurring.

If you close the console by pressing Ctrl+C, you close the console and stop the audit server. You need the audit server to be running for the rest of these instructions to work.

6 Verify that the table was created in the database by using the following steps:

6a Log in to your MySQL server.

6b Change to the naudit database by using the following command:

```
use naudit;
```

6c To display the tables in the database, use the following command:

```
show tables;
```

```
mysql> show tables;
+------------------+
| Tables_in_naudit |
+------------------+
| nauditlog        |
| simple           |
+------------------+
2 rows in set (0.00 sec)

mysql>
```

The *nauditlog* table should be in the list. If it is not, repeat Step 5.

6d To view the columns in the table, use the following command:

```
describe nauditlog;
```

The *nauditlog* table should have 24 rows.

```
+-----------------+--------------+------+-----+---------+-------+
| Field           | Type         | Null | Key | Default | Extra |
+-----------------+--------------+------+-----+---------+-------+
| SourceIP        | int(11)      | YES  |     | NULL    |       |
| ClientTimestamp | int(11)      | YES  | MUL | NULL    |       |
| ClientMS        | int(11)      | YES  |     | NULL    |       |
| ServerTimestamp | int(11)      | YES  |     | NULL    |       |
| SessionID       | int(11)      | YES  |     | NULL    |       |
| Component       | varchar(255) | YES  |     | NULL    |       |
| EventID         | int(11)      | YES  | MUL | NULL    |       |
| Severity        | int(11)      | YES  |     | NULL    |       |
| Grouping        | int(11)      | YES  |     | NULL    |       |
| Originator      | varchar(255) | YES  |     | NULL    |       |
| OriginatorType  | int(11)      | YES  |     | NULL    |       |
| Target          | varchar(255) | YES  |     | NULL    |       |
| TargetType      | int(11)      | YES  |     | NULL    |       |
| SubTarget       | varchar(255) | YES  |     | NULL    |       |
| Text1           | varchar(255) | YES  |     | NULL    |       |
| Text2           | varchar(255) | YES  |     | NULL    |       |
| Text3           | varchar(255) | YES  |     | NULL    |       |
| Value1          | int(11)      | YES  |     | NULL    |       |
| Value2          | int(11)      | YES  |     | NULL    |       |
| Value3          | int(11)      | YES  |     | NULL    |       |
| MIMEType        | int(11)      | YES  |     | NULL    |       |
| DataSize        | int(11)      | YES  |     | NULL    |       |
| Data            | mediumblob   | YES  |     | NULL    |       |
| Signature       | varchar(255) | YES  |     | NULL    |       |
+-----------------+--------------+------+-----+---------+-------+
24 rows in set (0.01 sec)
```

7 Continue with Section 8.2.3, “Configuring Access Manager Components to Log Audit Events,” on page 142.

8.2.3 Configuring Access Manager Components to Log Audit Events

The database is ready to receive events, and the Novell Audit Secure Logging Server is ready to send events to the database. The next step is to configure Access Manager to send events to the

server, which channels them to the database. For more information about these events, see "Enabling Auditing" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

1. To enable general Access Manager events, complete the following steps:
   - **1a** In the Administration Console, click *Access Manager* > *Auditing*.
   - **1b** In the Management Console Audit Events section, select the *Select All* option.
   - **1c** Click *Apply*.
2. To enable Identity Server events, complete the following steps.
   - **2a** In the Administration Console, click *Access Manager* > *Identity Servers* > *Edit* > *Logging*.
   - **2b** Scroll to the Novell Audit Logging section, then select *Enable*.
   - **2c** For events, select either the *Select All* option or at least the following: *Login Provided*, *Server Started*, *Server Stopped*, *Server Refreshed*.
   - **2d** Click *OK*.
   - **2e** On the Identity Servers page, click *Update* > *OK*.
3. To enable Access Gateway event, complete the following steps:
   - **3a** In the Administration Console, click *Access Gateways* > *Edit* > *Novell Audit*.
   - **3b** For events, select either the *Select All* option or at least the following: *Access Denied*, *URL Accessed*, and *Access Allowed*.
   - **3c** Click *OK* twice.
   - **3d** On the Access Gateways page, click *Update* > *OK*.
4. Generate a few events by logging in to Access Manager and accessing a resource.

   The audit event configuration changes to the Identity Server and the Access Gateway generated a few events, but logging in and accessing a resource generates a few more.
5. To verify that events are being logged in the nauditlog table, complete the following steps:
   - **5a** Log in to your MySQL server.
   - **5b** Change to the naudit database by using the following command:
     ```
     use naudit;
     ```
   - **5c** To display two columns of data, use the following command:
     ```
     select EventID, Originator from nauditlog;
     ```
6. Continue with Section 8.3, "Configuring Queries," on page 143.

8.3 Configuring Queries

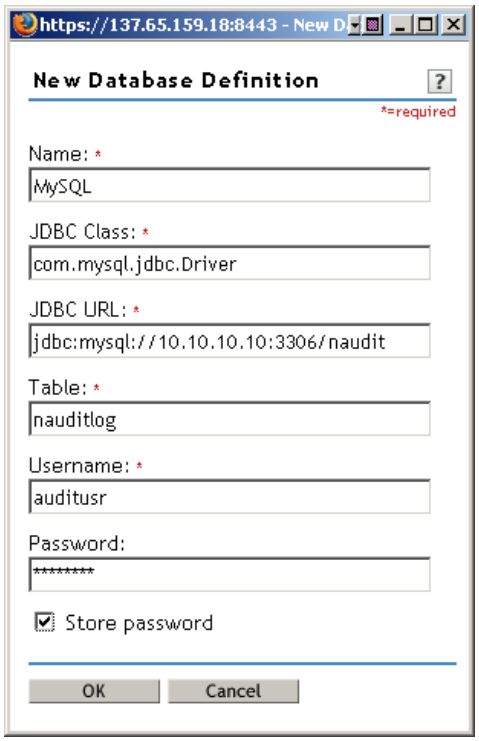
The Queries option in the Auditing and Logging plug-in allows you to use SQL queries to retrieve information about the events stored in the database. The following sections explain how to configure and use this feature.

- Section 8.3.1, "Enabling Queries to the MySQL Database," on page 144
- Section 8.3.2, "Configuring the Query Event List and Display," on page 144
- Section 8.3.3, "Performing a Query," on page 145

8.3.1 Enabling Queries to the MySQL Database

1 In the Administration Console, click *Auditing and Logging* > *Query Options*.

2 Click *New*.



3 Fill in the following fields:

Name: Specify *MySQL*.

JDBC Class: Specify *com.mysql.jdbc.Driver*.

JDBC URL: Specify *jdbc:mysql://<IP address>:3306/naudit*.

Replace *<IP address>* with the IP address of your MySQL server, for example: *jdbc:mysql://10.10.10.10:3306/naudit*.

Table: Specify *nauditlog*.

Username: Specify *auditusr*.

Password: Specify *auditpwd*.

Store Password: Select this option so that the password is stored.

4 Click *OK*.

5 Continues with Section 8.3.2, “Configuring the Query Event List and Display,” on page 144.

8.3.2 Configuring the Query Event List and Display

1 On the Query Options page, click the *Product Events* tab.

2 Click the *Object Selector* icon, and find the Logging Server object that has the host name of your Administration Console prepended to it, for example `Jwilson1 Logging Server`.

For this example, the Novell Audit Secure Logging Server DN field displays the following name:

```
Jwilson1 Logging Server.Logging Services
```

3 Click *Update*.

4 Click the *Global Options* tab.

5 Select *RFC822 Local* for the *Date/Time format*.

6 Click *OK*.

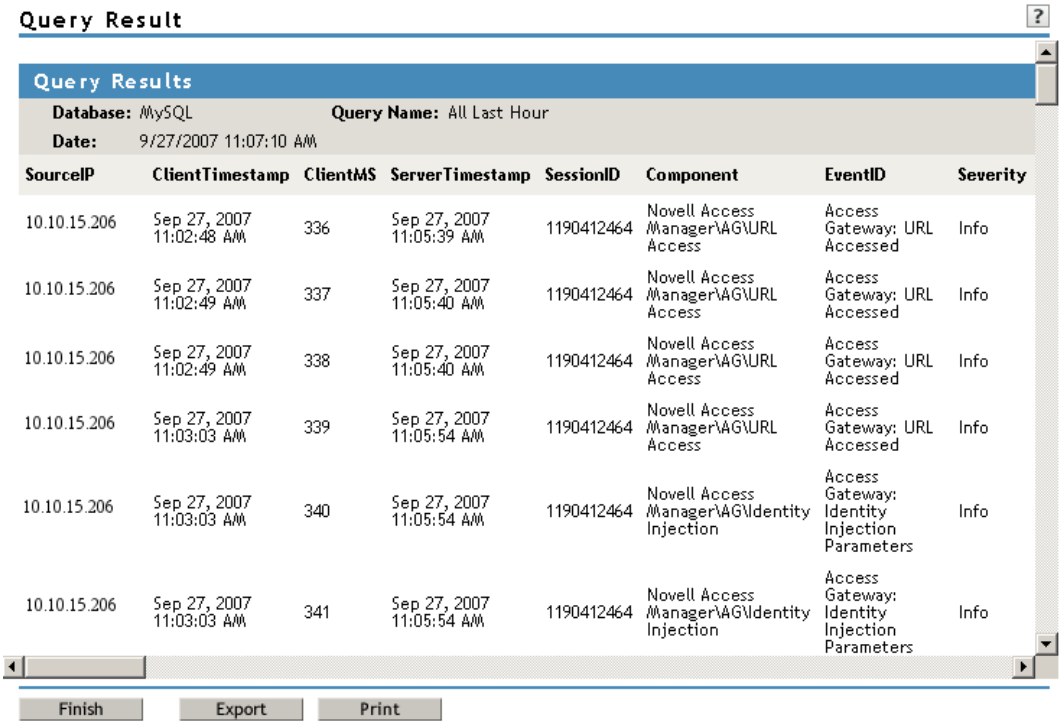
7 Continue with Section 8.3.3, "Performing a Query," on page 145.

8.3.3 Performing a Query

1 Click *Queries* under *Auditing and Logging*.

2 Select *All Last Hour*, then click *Run Query*.

A display similar to the following should appear.



For more information about the fields that are possible on each event row, see "Access Manager Audit Events and Data" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

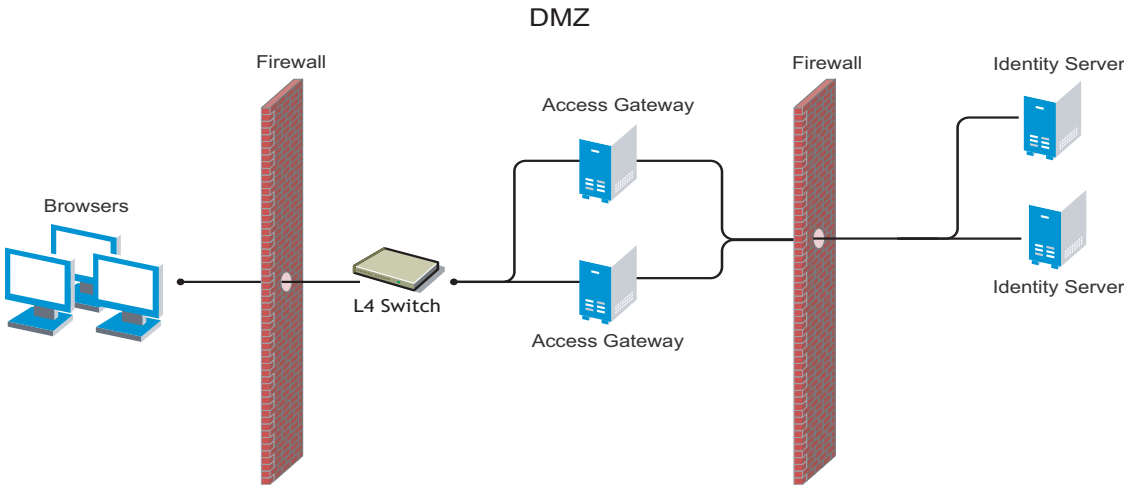
For more information about how to use queries and create your own, see the *Novell Audit 2.0 Administration Guide* (http://www.novell.com/documentation/novellaudit20/novellaudit20/data/bookinfo.html).

Protecting an Identity Server with an Access Gateway

9

For security reasons, you might want to set up your Access Manager configuration so that the Identity Server is a resource protected by an Access Gateway. This configuration reduces the number of ports you need to open between the outside world and your network. Figure 9-1 illustrates such a configuration.

Figure 9-1 *Identity Servers behind an Access Gateway*



With this configuration, you do not need an L4 switch to add multiple Identity Servers to a cluster configuration. When the Identity Server is configured to be a protected resource of the Access Gateway, the Access Gateway uses its Web server communication channel. Each Identity Server in the cluster must be added to the Web server list, and the Access Gateway uses its Web server load balancing and failover policies for the clustered Identity Servers.

This configuration has been tested with the Access Gateways plugged directly into the L4 switch.

The following features are not supported in this configuration:

- The Identity Server cannot respond to Identity Provider introductions.
- Federation to an external service provider cannot be supported with this configuration.
- The proxy service that is protecting the Identity Server cannot be configured to use mutual SSL. For example with this configuration, X.509 authentication cannot be used for any proxy service. To perform X.509 authentication (which is a form of mutual SSL), a user's browser must have direct access to the Identity Server.

To configure Access Manager in this manner, you must perform the following changes to the basic configuration.

1. Change the port of the Base URL of the Identity Server to 443. (This configuration has not been tested with port 80.) See Section 1.3, “Creating a Basic Identity Server Configuration,” on page 13.

If you are using path-based multi-homing, the domain name of the Base URL must match the public DNS of the proxy service set up in the Access Gateway.

If you are using domain-based multi-homing, the domain name of the Base URL can be different than the Access Gateway, but your DNS server must resolve the name to the IP address of the Access Gateway.

2 (Conditional) If you are using domain-based multi-homing, create a wildcard certificate to be used by the Identity Server and the Access Gateway.

For example, `*.novell.com`, where the Identity Server DNS is `idp.novell.com` and the Access Gateway DNS is `esp.novell.com`.

If you are using path-based multi-homing, you can use the same certificate for the Identity Server and the Access Gateway.

3 Set up a proxy service on the Access Gateway for the Identity Server. See "Creating a Reverse Proxy and Proxy Service" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

3a When creating the proxy service, set the following fields to the specified values:

Published DNS Name: Specify the same name you have specified for the domain name of the Base URL of the Identity Server. Your DNS server must be set up to resolve this name to the Access Gateway.

Web Server IP Address: Specify the IP address of the Identity Server. If the cluster configuration for the Identity Server contains more than one Identity Server, provide the IP address of one of the servers here. This must be the actual IP address of the Identity Server and not the VIP address if the Identity Server is behind an L4 switch.

Host Header: Specify *Web Server Host Name.*

Web Server Host Name: Specify the domain name of the Base URL of the Identity Server. This entry matches what you specify in the *Published DNS Name* field.

If proxy service is not the first proxy service of the reverse proxy, you can use either domain-based or path-based multi-homing.

3b (Conditional) For a domain-based proxy service, set the *Multi-Homing Type* field to *Domain-Based*.

3c (Conditional) For a path-based proxy service, set the *Multi-Homing Type* field to *Path-Based* and set the *Path* field to `/nidp`.

On the Path-Based Multi-Homing page, do not select the *Remove Path on Fill* option. The Identity Server needs the `/nipd` path.

4 Configure a protected resource for the proxy service. See "Configuring Protected Resources" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

Set the *Contract* field to *None*. The Identity Server needs to be set up as a public resource.

Set the *URL Path* of the protected resource to `/nidp/*`.

5 Set up the Access Gateway to use SSL between the browsers and the Access Gateway. See "Configuring SSL Communication with the Browsers and the Identity Server " in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.

6 Set up SSL between the proxy service that is protecting the Identity Server and the Identity Server. See "Configuring SSL between the Proxy Service and the Web Servers" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*. Use the following settings:

- Select the *Connect Using SSL* option
- Configure a *Web Server Trusted Root*.

- Do not configure an *SSL Mutual Certificate*.
- Set the *Connect Port* to 8443.

7 (Conditional) If the cluster configuration for the Identity Server contains more than one Identity Server, configure the following options:

7a Click *Access Manager > Access Gateways > Edit > [Name of Reverse Proxy] > [Name of Proxy Service] > Web Servers*.

7b Specify the IP addresses of the other Identity Servers in the *Web Server List*.

If the Identity Servers are behind an L4 switch, you need to add the IP address of each Identity Server and not the VIP address.

7c Click *TCP Connect Options*, then configure the following options.

Policy for Multiple Destination IP Addresses: (Linux only) For the Identity Servers, select *Round Robin*. This is the configured behavior for the NetWare Access Gateway.

Enable Persistent Connections: Make sure this option is selected. After the user has established an authenticated session with an Identity Server, you want that user to continue using the same Identity Server as long as that server is running.

8 Configure HTML rewriting.

8a Click *Access Manager > Access Gateways > Edit > [Name of Reverse Proxy] > [Name of Proxy Service] > HTML Rewriting*

8b Make sure the *Enable HTML Rewriting* option is selected.

8c In the *HTML Rewriter Profile List*, click *New*, then specify a name for the profile and select *Word* for the *Search Boundary*.

8d Specify the following URLs in the *And Requested URL Is Not* section. The following URLs use `ag76.provo.novell.com/nidp` as the DNS name of the reverse proxy for the Identity Server.

```
ag76.provo.novell.com/nidp/idff/soap
ag76.provo.novell.com/nidp/idff/soap/
ag76.provo.novell.com/nidp/idff/soap/*
ag76.provo.novell.com:443/nidp/idff/soap
ag76.provo.novell.com:443/nidp/idff/soap/
ag76.provo.novell.com:443/nidp/idff/soap/*
```

8e Click *OK*.

8f Use the up-arrow icon to move your profile to the top of the list.

9 Configure the Pin List so that the Identity Server pages are not cached. Click *Access Gateways > Edit > Pin List*. In the list, create a *URL Mask* of `/nidp/*` and set the *Pin Type* to *Bypass*. See "Configuring a Pin List" in the *Novell Access Manager 3.0 SP3 IR2 Administration Guide*.