Setup Guide

Access Manager 3.2

May 2012

Legal Notice

About This Guide

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

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

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 *NetIQ Access Manager 3.2 Identity Server Guide* and the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide* as the sources for additional or advanced 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/TLS)
- 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.

Documentation Updates

For the most recent version of the *Setup Guide*, visit the NetIQ Access Manager Documentation Web site (https://www.netiq.com/documentation/novellaccessmanager32/).

Additional Documentation

- *NetIQ Access Manager 3.2 SP1 Installation Guide*
- *NetIQ Access Manager 3.2 Administration Console Guide*
- *NetIQ Access Manager 3.2 Identity Server Guide*
- *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*
- *NetIQ Access Manager 3.2 SSL VPN Server Guide*
- *NetIQ Access Manager 3.2 Policy Guide*
- *NetIQ Access Manager 3.2 J2EE Agent Guide*

NOTE: Contact namsdk@novell.com for any query related to Access Manager SDK.

Contents

1 Setting Up a Basic Access Manager Configuration

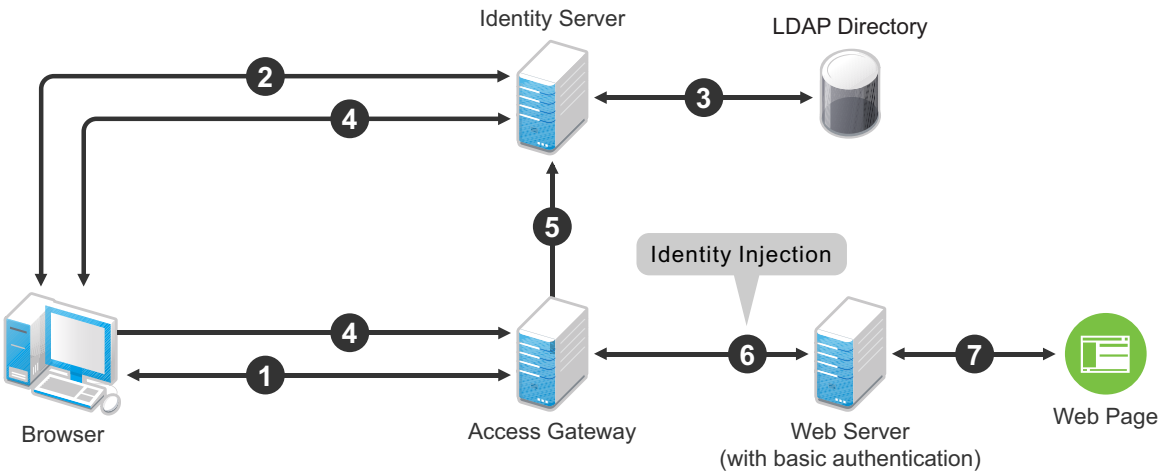
The initial setup for NetIQ Access Manager consists of installing the components and setting up the Identity Server and the Access Gateway to protect resources running on an HTTP Web server. Access Manager can also be configured to protect other resources such as applications on J2EE servers and non-HTTP applications. These should be set up after you have created a basic setup. For J2EE server applications, see the *NetIQ Access Manager 3.2 J2EE Agent Guide*. For non-HTTP applications, see the *NetIQ Access Manager 3.2 SSL VPN Server Guide*

This tutorial describes the following topics and tasks:

1.1 Understanding Access Manager Configuration

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

Figure 1-1 *Basic Process Flow*

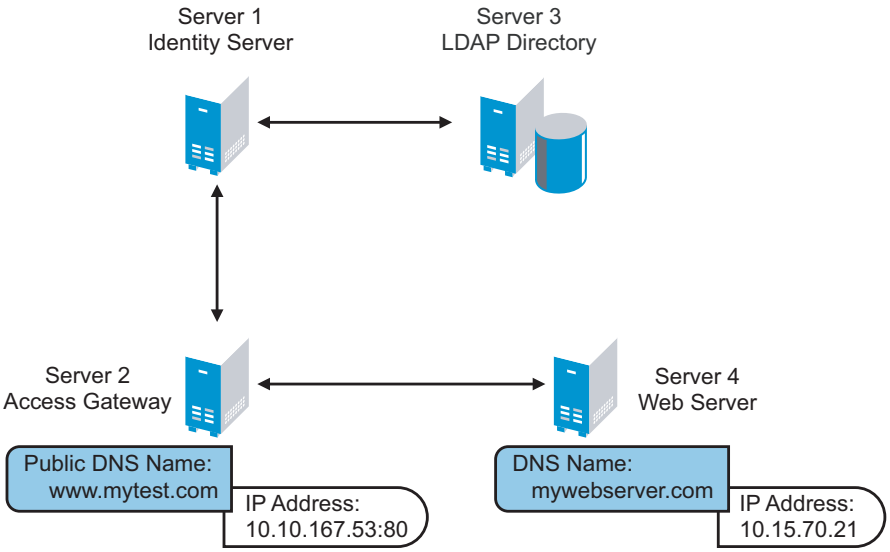


1. The user sends a request to the Access Gateway for access to a protected resource.
2. The Access Gateway redirects the user to the Identity Server, which prompts the user for a username and password.

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 through the browser in a query string.
5. The Access Gateway retrieves the user's credentials from the Identity Server through the SOAP channel in the form of a SOAP message.
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 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 2, "Enabling SSL Communication," on page 27.

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 *NetIQ Access Manager 3.2 SP1 Installation Guide*.
- ❒ An installed Identity Server. See "Installing the NetIQ Identity Server" in the *NetIQ Access Manager 3.2 SP1 Installation Guide*.
- ❒ An installed Access Gateway. See "Installing the Access Gateway Appliance" in the *NetIQ Access Manager 3.2 SP1 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 6.2.3, "Configuring Name Resolution," on page 115.
- ❒ 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 6, "Digital Airlines Example," on page 111.
- ❒ A client workstation with a browser with browser pop-ups enabled.

1.3 Creating a Basic Identity Server Configuration

After you log in to the Administration Console, click *Devices* > *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.

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 *NetIQ Access Manager 3.2 Identity Server 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 *NetIQ Access Manager 3.2 SP1 Installation Guide*.

2 In the Administration Console, click *Devices* > *Identity Servers*.

3 Select the check box next to the Identity Server, then click *New Cluster*.

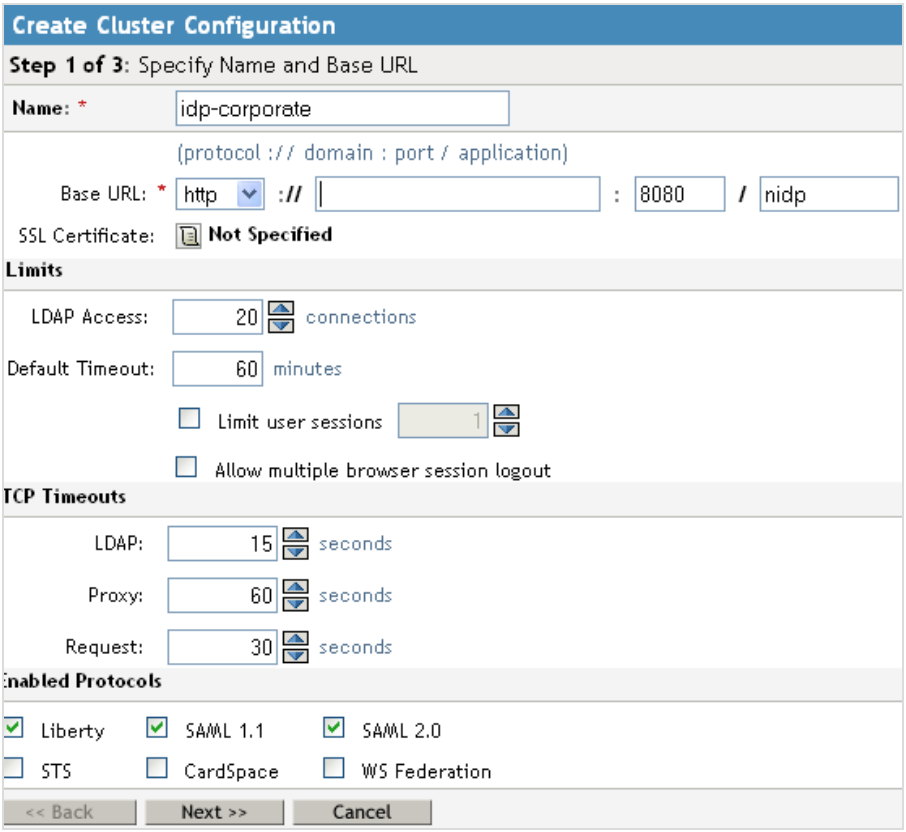
Selecting the server is one way to assign it to the cluster configuration.

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.

5 Click *OK*.

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



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

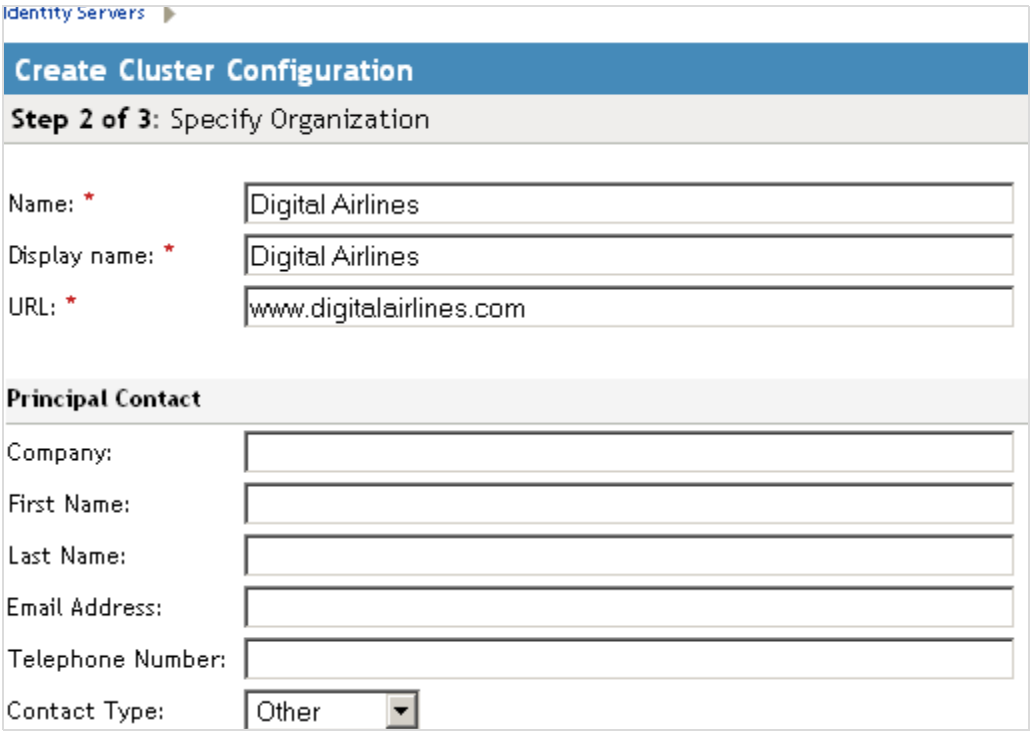
Name: The name by which you want to refer to the Identity Server configuration. This field is populated with the name you provided in the *New Cluster* dialog box. You can change the name here, if necessary.

Base URL: The application path for the Identity Server. The Identity Server protocols 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.

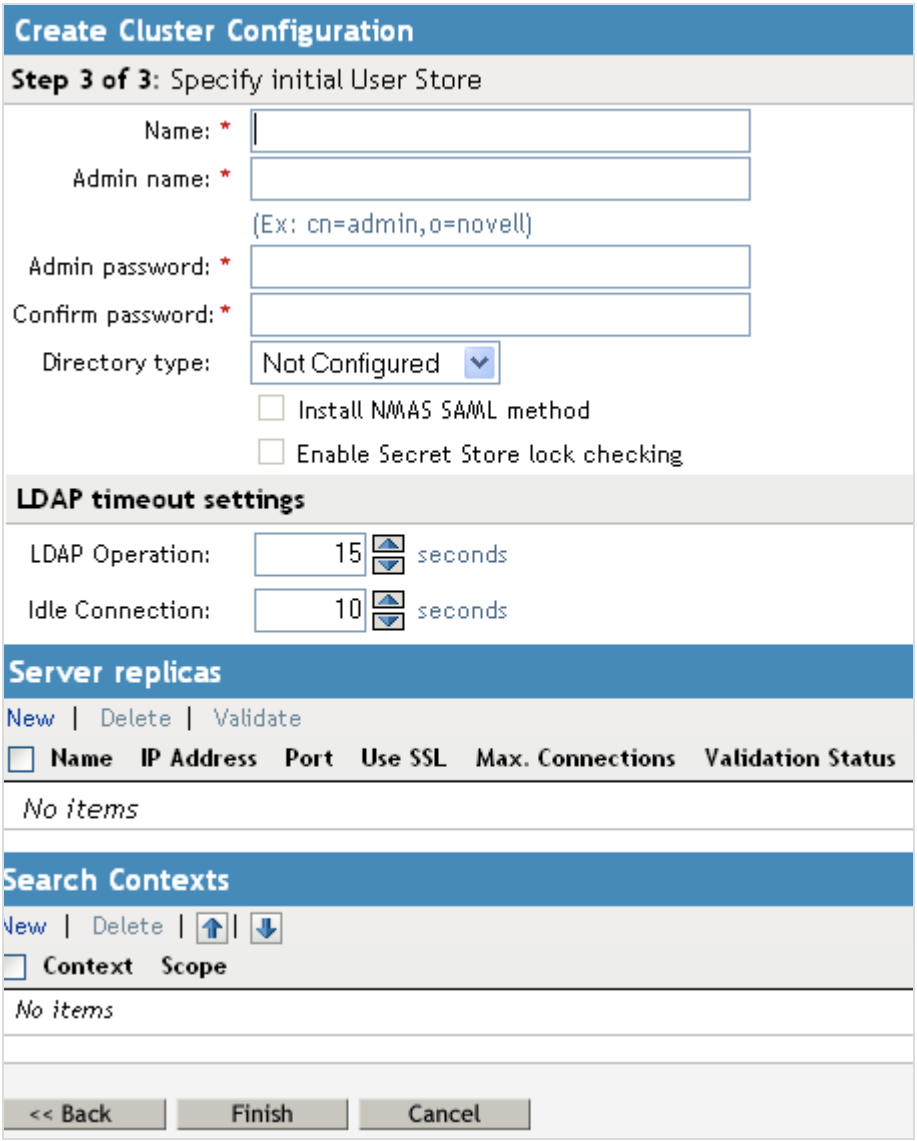
Display Name: The display name for the organization. This can be the same as the name of the organization.

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.

For more information about the options on this page and configuring for load balancing and failover, see "Configuring Identity User Stores" in the *NetIQ Access Manager 3.2 Identity Server Guide*.

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.

For information about adding multiple replicas for load balancing and failover, see "Configuring the User Store " in the *NetIQ Access Manager 3.2 Identity Server Guide*.

10 Select *Use secure LDAP connections*. The port changes to 636, which is the secure LDAP port.

This is the only configuration we recommend for the connection between the Identity Server and the LDAP server in a production environment. If you use port 389, usernames and passwords are sent in clear text on the wire.

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.
- Make sure that the specified admin user can log into the user store.
- Check for network communication problems between the Identity Server and the LDAP server.
- Enable verbose logging on the Identity Server, then search for the IP address or name of the user store in the log file (Linux: `catalina.out`; Windows: `stdout.log`) and identify errors.

  For logging information, see "Enabling Component Logging" in the *NetIQ Access Manager 3.2 Identity Server Guide*.

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.

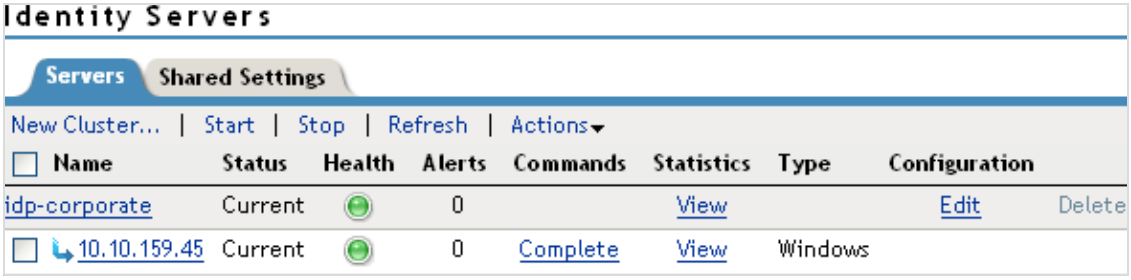
If the search context you specify finds more that one user with the same username, the Identity Server cannot authenticate these users. A username must be unique within a search context.

18 Click *Finish* to save the server configuration.

19 Restart Tomcat as prompted.

If your Administration Console is installed on the same machine as your Identity Server, your connection is broken. Refresh the page and log in to the Administration Console.

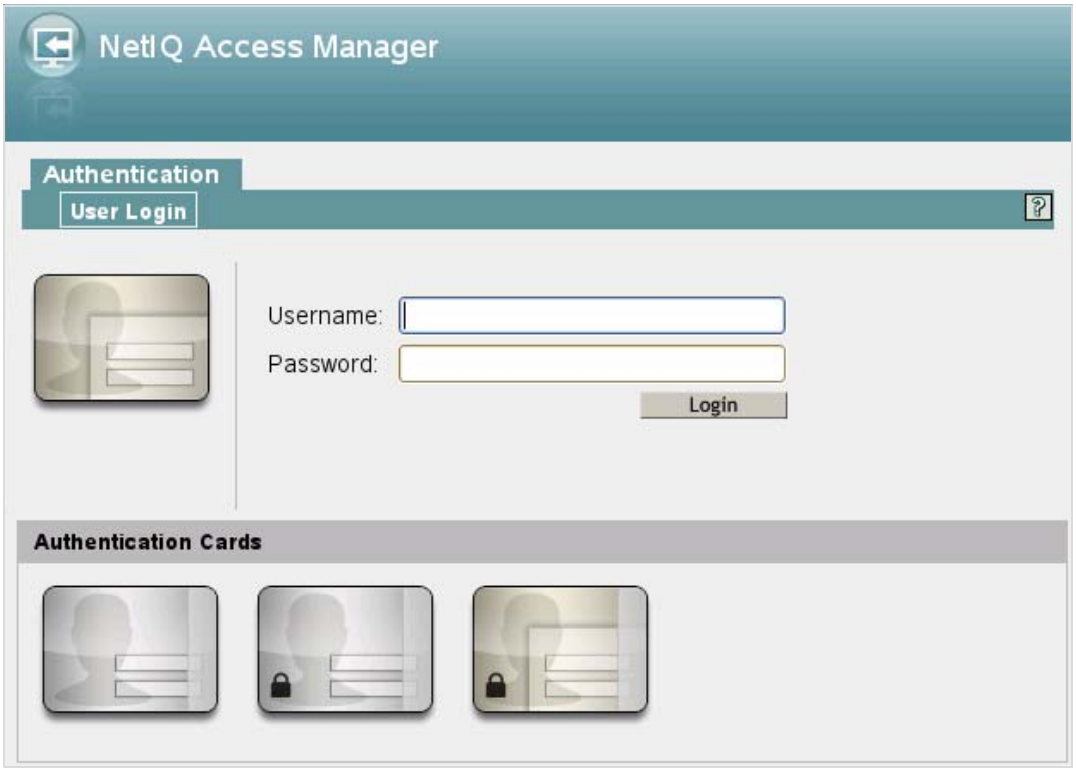
The Health status icons for the configuration and the Identity Server should turn green.



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 *NetIQ Access Manager 3.2 Identity Server Guide*.

20 (Optional) Verify the configuration:

20a In a browser, enter the Base URL of the Identity Server as the URL.



20b Select a card without the locking icon.

Cards with a locking icon require HTTPS and SSL. In this basic setup, you configured the Identity Server to use HTTP.

20c Log in using the credentials of a user in the LDAP server.

20d (Conditional) 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 17.
- To use the Digital Airlines sample Web pages, continue with Chapter 6, "Digital Airlines Example," on page 111.

To install an Access Gateway, see "Installing the Access Gateway Appliance" or "Installing the Access Gateway Service" in the *NetIQ Access Manager 3.2 SP1 Installation Guide*.

1.4 Configuring the Access Gateway

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

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.

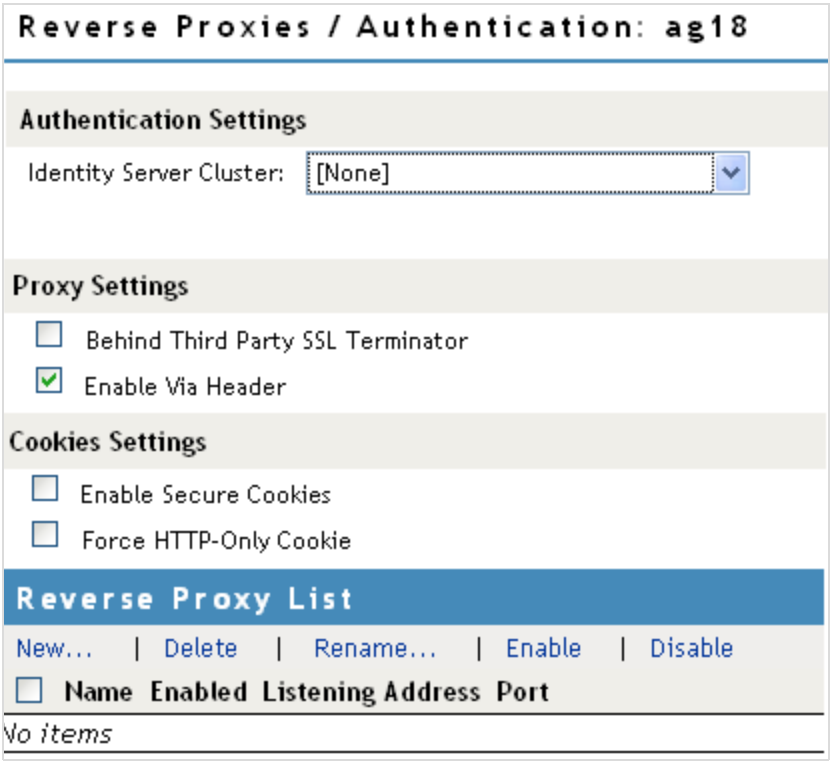
To create a reverse proxy, you must create at least one proxy service with a protected resource. You must supply a name for each of these components. Reverse proxy names and proxy service names must be unique to the Access Gateway because they are configured for global services such as IP addresses and 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`.

What You Need To Know	Example	Your Value
Name of the Identity Server cluster	idp-corporate	_____
DNS name of the Access Gateway	mytest.com	_____
Web server information		
IP address	10.15.70.21	_____
DNS name	mywebserver.com	_____
Names you need to create		
Reverse proxy name	mycompany	_____
Proxy service name	company	_____
Protected resource name	public	_____

This first reverse proxy is used for authentication. You need to configure the proxy service to use the DNS name of the Access Gateway as its *Published DNS Name*, and the Web server and the resource on that Web server need to point to the page you want displayed to the users when they first access your Web site. You can use Access Gateway configuration options to allow this first page to be a public site with no authentication required until the users access the links on the page, or you can require authentication on this first page. The following configuration steps have you first configure the protected resource as a public resource, then you modify the configuration to require authentication.

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

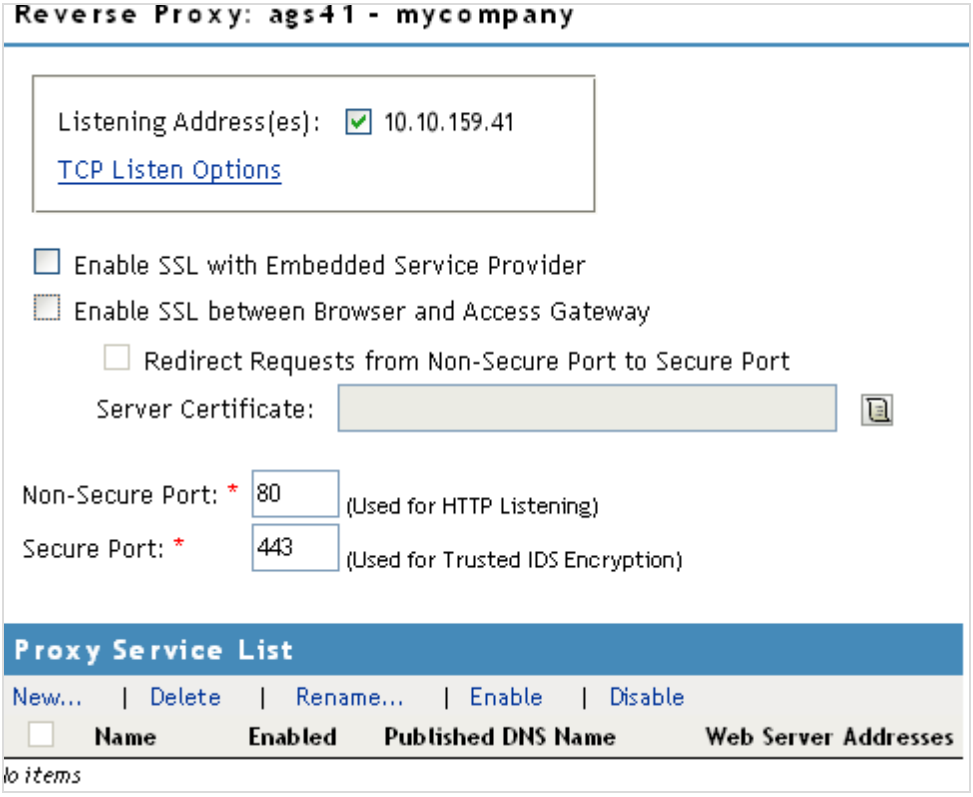


2. In the *Identity Server Cluster* option, select the configuration you have assigned to the Identity Server.

   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*.

The Reverse Proxy configuration page appears.



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.

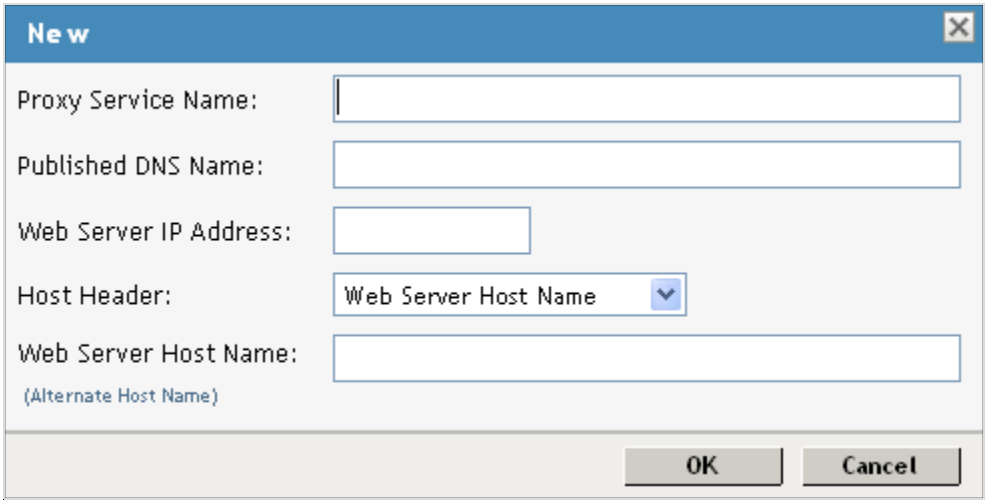
This basic configuration does not set up SSL. For SSL information, see Chapter 2, "Enabling SSL Communication," on page 27.

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. For this first proxy server, the DNS name must resolve to the Access Gateway IP address that you selected as the listening address. For the example in Figure 1-2 on page 10, 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 10, 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 10 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.

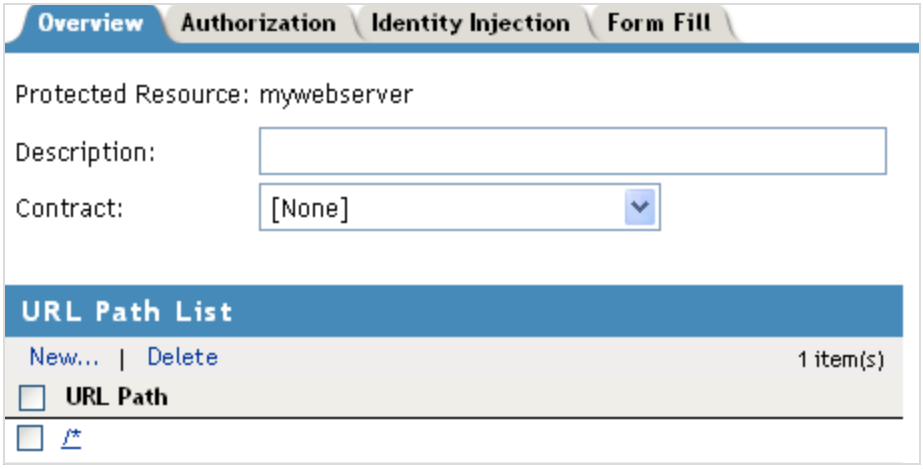
1.4.2 Configuring a Public Protected Resource

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 next to 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 *Devices* > *Access Gateways*.

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 *Devices* > *Identity Servers* > *Update*, then click *OK*.

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

12 (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 10, 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.

13 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 17 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 23

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 or a Linux Access Gateway Service, use YaST to verify the time settings. For a Windows Access Gateway Service, use the Date and Time option in the Control Panel. If you have a Network Time Protocol server, configure the Access Manager machines to use it.

For an Access Gateway Appliance, complete the following steps:

1 In the Administration Console, click *Devices* > *Access Gateways*, then click *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 To save the changes to browser cache, click *OK*.

5 To apply your changes, click *Devices* > *Access Gateways*, then click *Update* > *OK*.

6 Continue with "Enabling Trusted Authentication" on page 23.

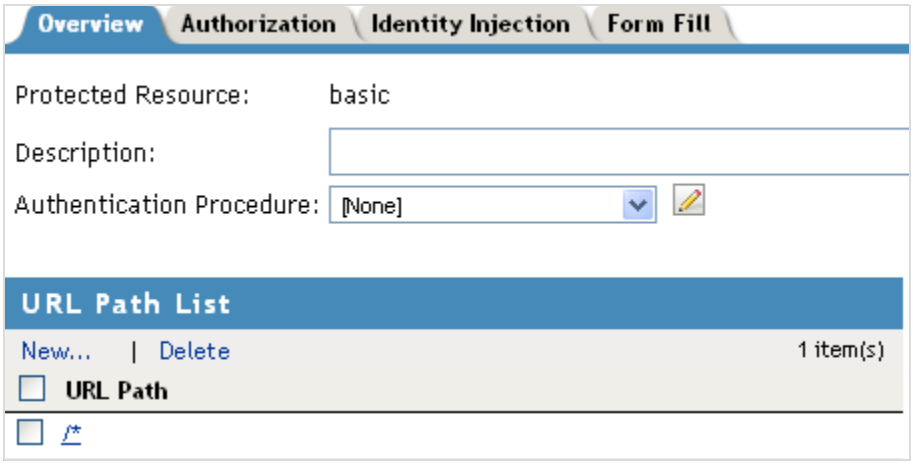
1.5.2 Enabling Trusted Authentication

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 *Devices* > *Access Gateways*, then click *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* for the *Authentication Procedure*:

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 17 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 10, 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 *Devices* > *Access Gateways*, then click *Update* > *OK*.

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

8a Specify the published DNS name to this resource in the browser. For the example illustrated in Figure 1-2 on page 10, 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 10).

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.

If you receive an error, see "Common Authentication Problems" on page 122.

9 Continue with Section 1.6, "Setting Up an Identity Injection Policy," on page 24.

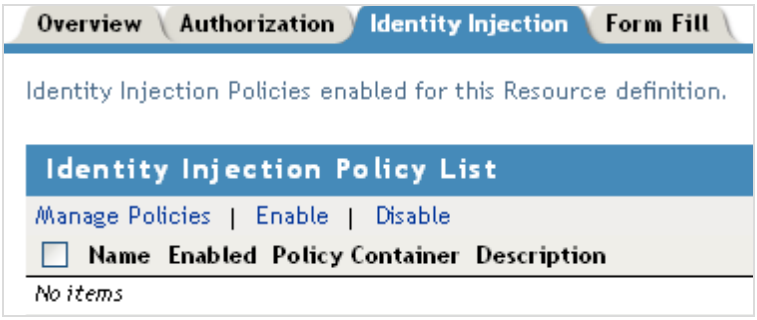
1.6 Setting Up an Identity Injection Policy

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. 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, which is the `basic` directory that your Web server has been configured to require basic authentication before allowing access.

1. In the Administration Console, click *Devices* > *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 10:
   - **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*.

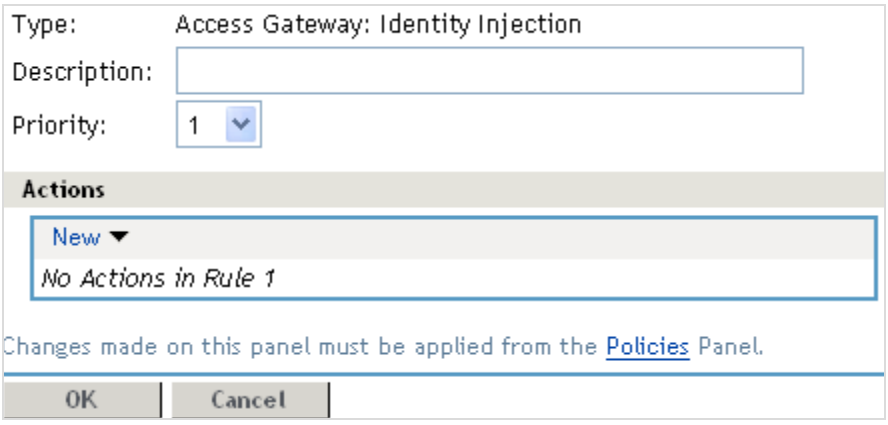


On a new installation, the list is empty because no policies have been created.

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.

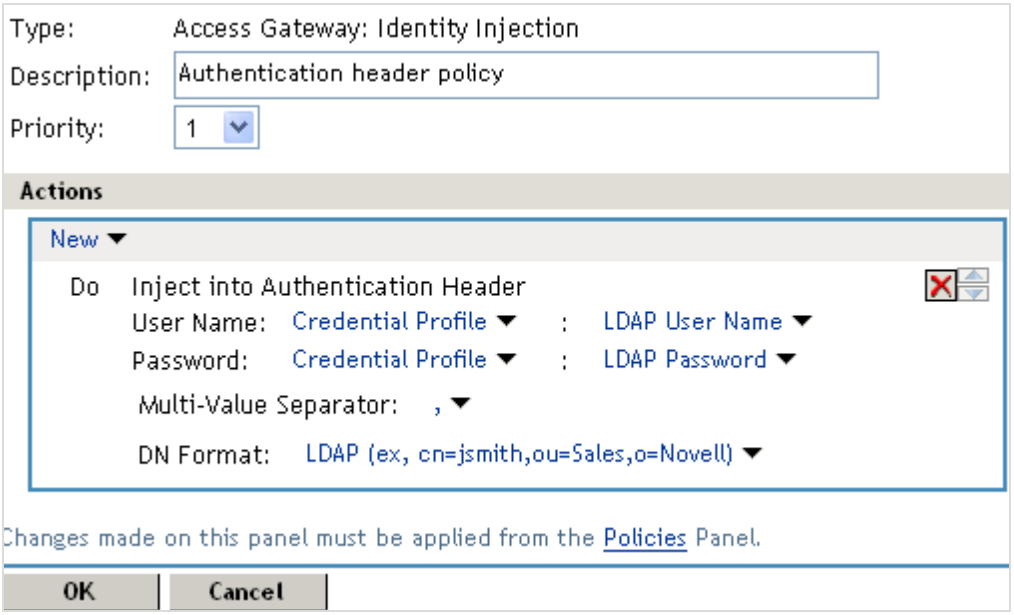
8 In the *Actions* section, click *New* > *Inject into Authentication Header*.

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 *Devices* > *Access Gateways*, 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 that uses 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 Identity Manager User Application, see "Configuring Access Manager for UserApp and SAML" (http://www.novell.com/coolsolutions/appnote/19981.html).

2 Enabling SSL Communication

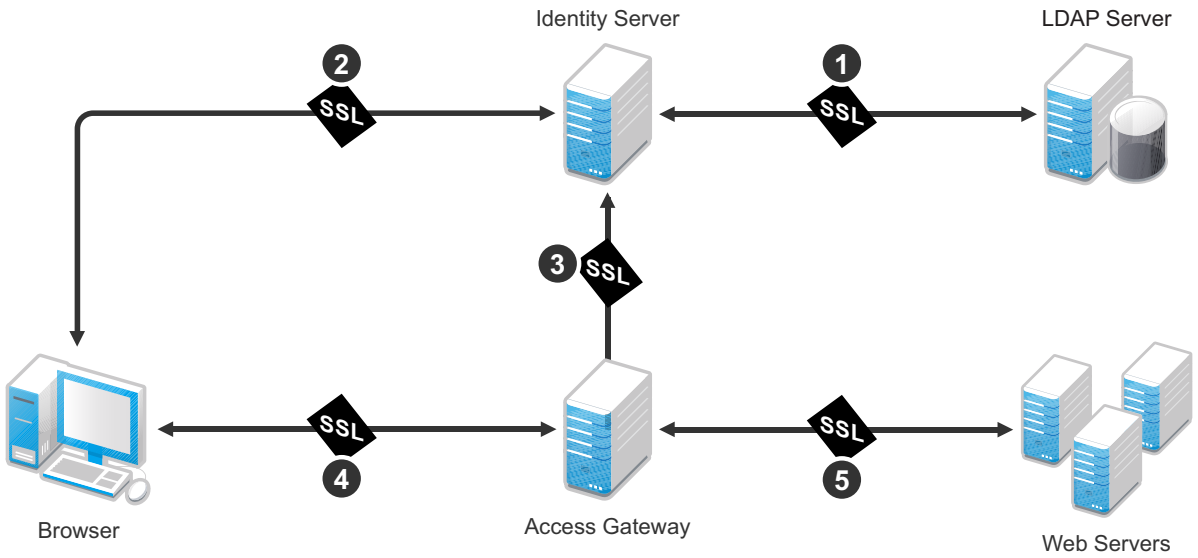
Because the Identity Server handles authentication, it must be configured for SSL before any of the other Access Manager components. You can then configure the Access Gateway to use SSL in its connections to the Identity Server, to the browsers, and to its Web servers.

SSL impacts the performance of Access Manager components. Instead of enabling Access Manager components for SSL, you can front the components with an SSL terminator or accelerator. The SSL terminator offloads the handling of the SSL traffic, and the Access Manager components can be configured to use HTTP. For some tips on using such a device, see Section 2.4, “Using an SSL Terminator,” on page 41.

2.1 Identifying the SSL Communication Channels

Access Manager has five communication channels that can be configured for SSL. Figure 2-1 illustrates these channels.

Figure 2-1 *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 11). 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 2.2, "Using Access Manager Certificates," on page 28
- Section 2.3, "Using Externally Signed Certificates," on page 36

2.2 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 2.2.1, "Configuring Secure Communication on the Identity Server," on page 28
- Section 2.2.2, "Configuring the Access Gateway for SSL," on page 31

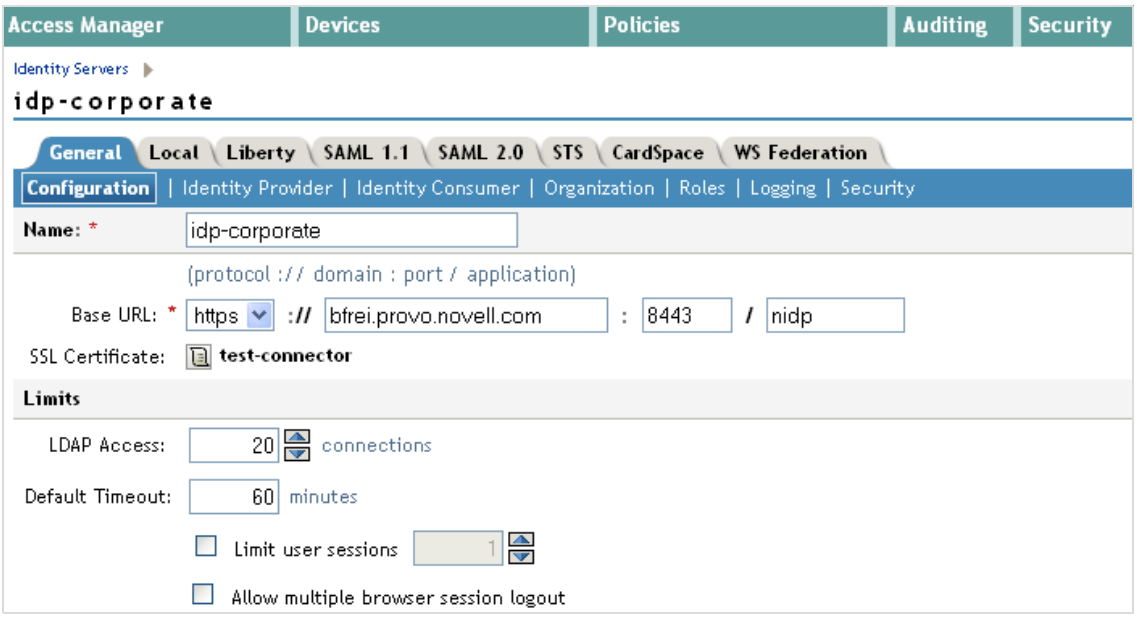
2.2.1 Configuring Secure Communication on the Identity Server

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:

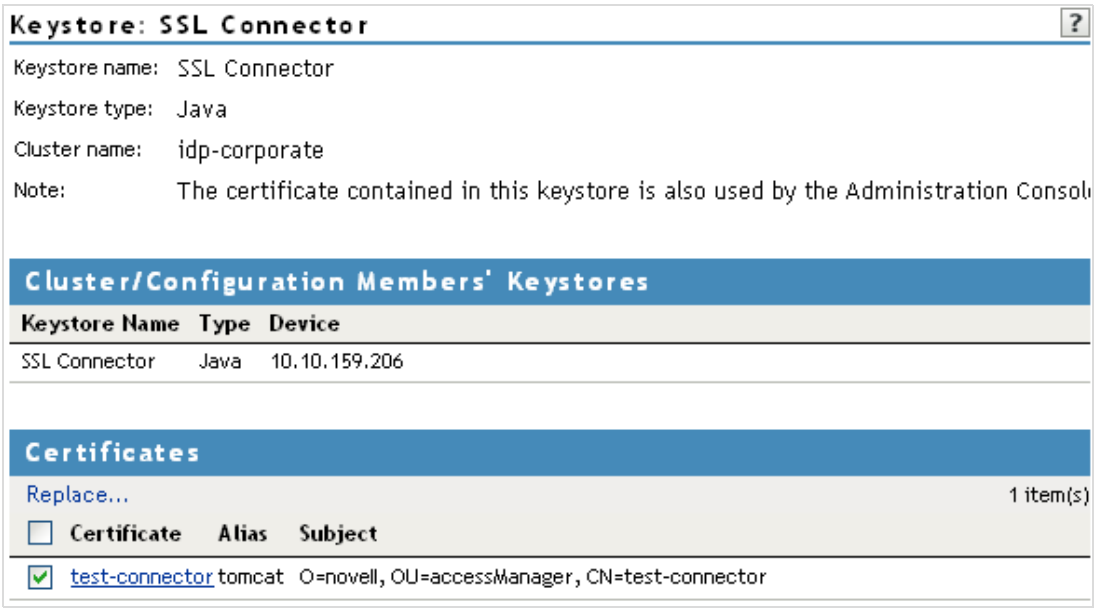
1. In the Administration Console, click *Devices* > *Identity Servers*.
2. In the Configuration column, click *Edit*.
3. Change *Protocol* to HTTPS (the system changes the port to 8443), click *Apply*, then click *OK* at the warning.
4. Copy the domain name of your Identity Server configuration to the clipboard, or take note of the name. It must match the common name of the new certificate.



5 Click the *SSL Certificate* icon, then click *OK* at the warning if you clicked *Apply* when you changed the protocol to HTTPS.

If you did not click *Apply*, then click *Cancel* and click *Apply* before returning to this option

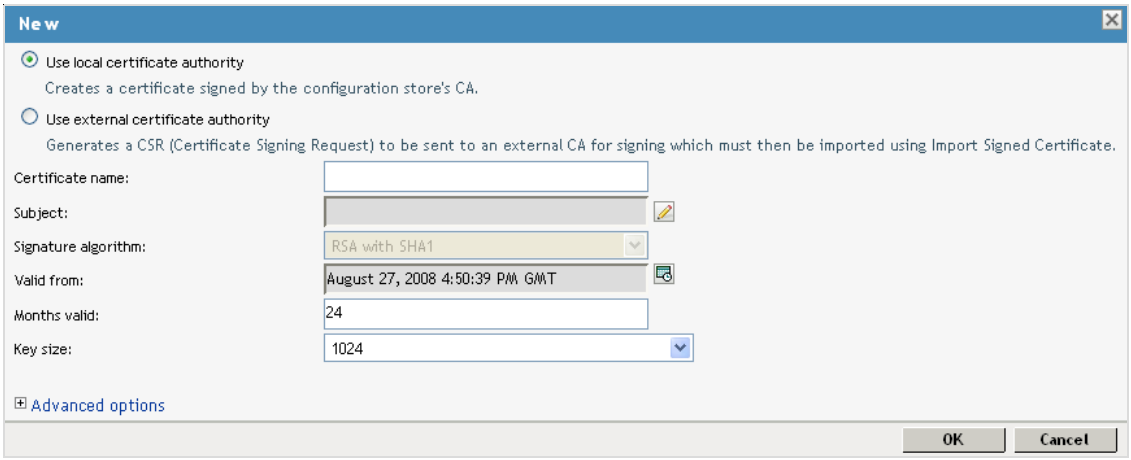
The Keystore configuration page appears.



6 In the *Certificates* section, click *Replace*.

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

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



9 Click *Use local certificate authority*.

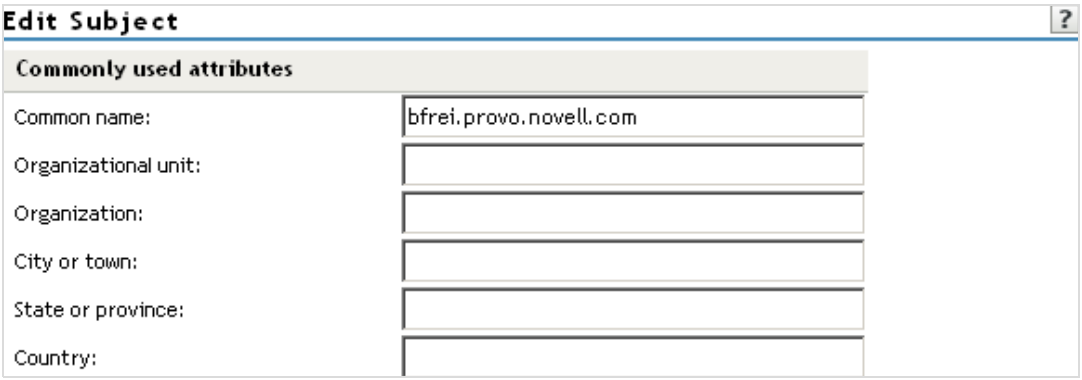
This option creates a certificate signed by the local CA (or Organizational CA), and creates the private key.

10 Fill in the following fields:

Certificate name: A 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 *NetIQ Access Manager 3.2 Administration Console 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.



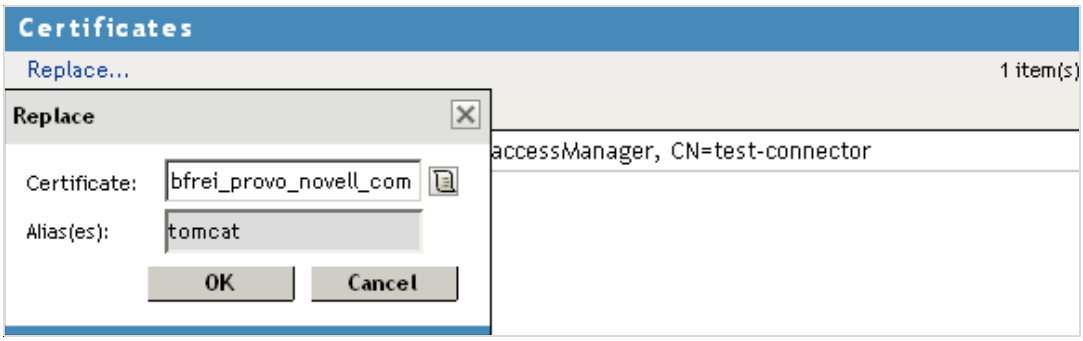
If you are going to be using Windows CardSpace, fill in values for the other common attributes.

11 Click *OK*.

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

The new certificate is displayed on the Select Certificate page.

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



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

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

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

- If your Identity Server and Administration Console are on the same machine, you need to log in to the Administration Console again.
- If your Identity Server is on another machine, click *OK*.

17 To verify the health of the Identity Server, click *Devices* > *Identity Servers*.

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

If you do not receive the option to update the Access Gateway, select the Access Gateway, then click *Actions* > *Service Provider* > *Restart Service Provider* > *OK*.

Restarting the service provider reestablishes the trust between the Access Gateway and the new base URL for the Identity Server.

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

19a Enter the URL to a protected resource on the Access Gateway.

19b Complete one of the following:

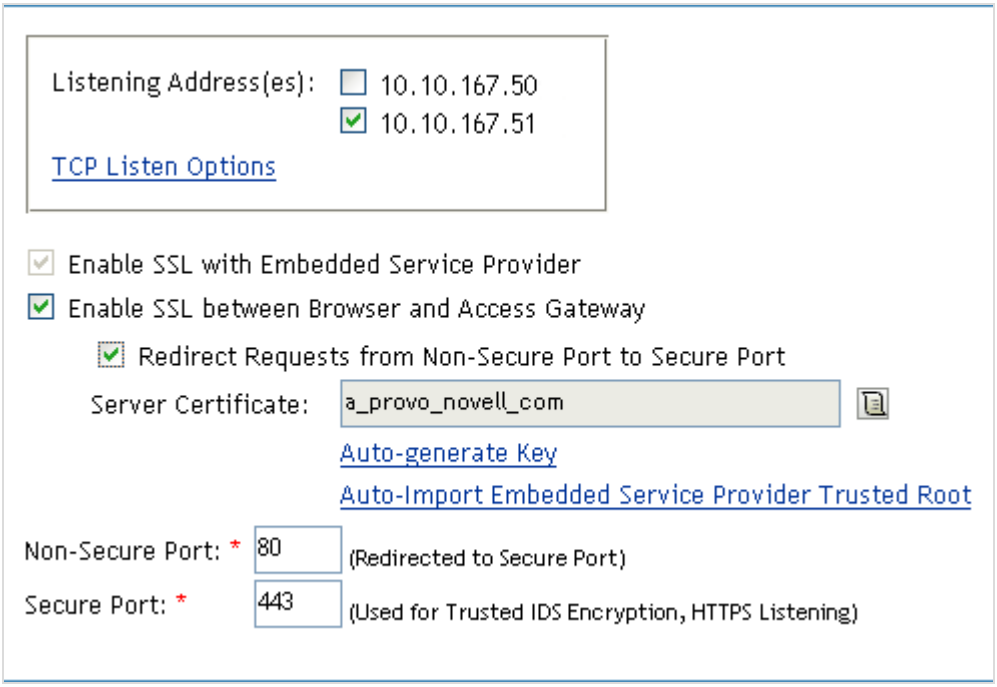
- If you can access the site, the trusted relationship has been reestablished. Continue with Section 2.2.2, "Configuring the Access Gateway for SSL," on page 31.
- If you receive a 100101043 or 100101044 error, the trusted relationship has not been established. For information on how to solve this problem, see "Troubleshooting 100101043 and 100101044 Liberty Metadata Load Errors" in the *NetIQ Access Manager 3.2 Identity Server Guide*.

2.2.2 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 Access Gateway

1 In the Administration Console, click *Devices* > *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 "Enabling SSL between the Reverse Proxy and Its Web Servers" on page 34.

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 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 Authentication Procedure from an HTTP contract to an HTTPS contract.

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

The *Name/Password - Form* contract is capable of using either HTTP or HTTPS.

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

7 Click the *Configuration Panel* link near the bottom of the page, 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 *Devices* > *Identity Servers*, then click *Update* > *OK*.

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 *NetIQ Access Manager 3.2 Identity Server Guide*.

Enabling SSL between the Reverse Proxy and Its Web Servers

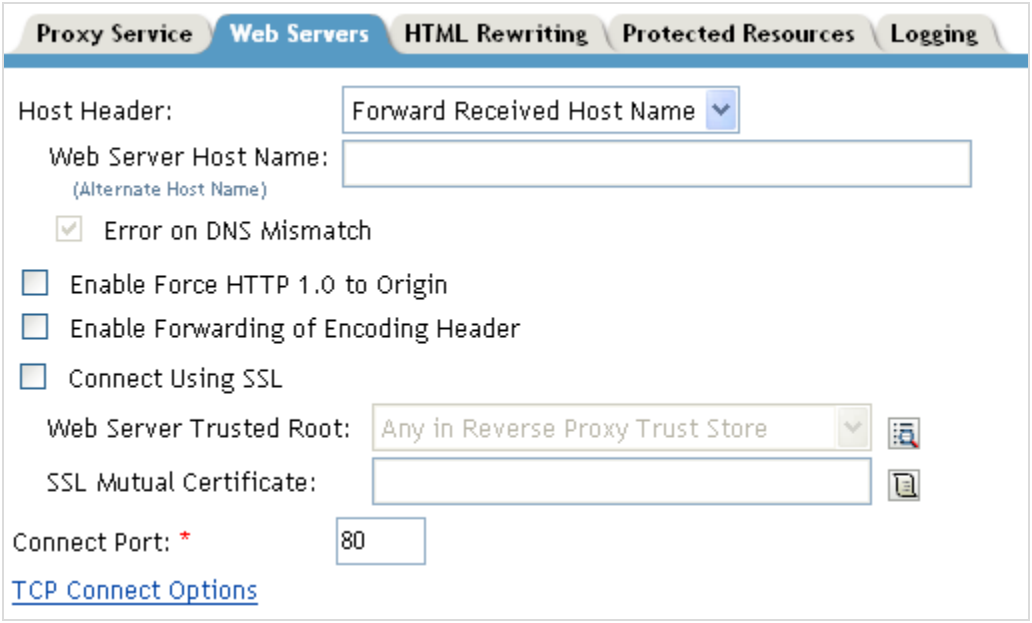
To enable SSL between the reverse proxy and the Web servers, you must have already performed the following tasks:

- ❒ Enabled SSL between the Access Gateway and the browsers. See Section 1.4.1, "Configuring a Reverse Proxy," on page 17 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 *Devices* > *Access Gateways* > *Edit* > *[Name of Reverse Proxy]* > *[Name of Proxy Service]* > *Web Servers*.

   The Web Servers configuration page appears.



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 17 and select the *Enable SSL between Browser and Access Gateway* field.

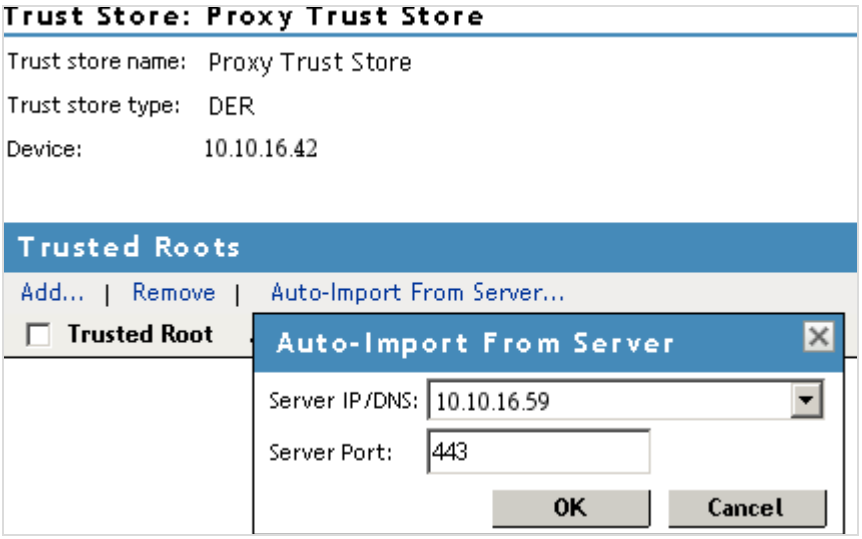
3. In the *Connect Port* field, specify the port that your Web server uses for SSL communication.

4. Configure how you want the certificate verified. The Access Gateway supports different options. Select one of the following:

   - **Do not verify:** Select this option if you do not want to verify the *Web Server Trusted Root* certificate. Continue with Step 10.
   - To verify the certificate authority of the Web server certificate, select *Any in Reverse Proxy Trust Store*. When this option is selected, the public certificate of the certificate authority must be added to the proxy trust store.

     IMPORTANT: For an Access Gateway Service, this option is a global option. If you select this option for one proxy service, all proxy services on an Access Gateway Service are flagged to verify the public certificate. This verification is done even when other proxy services are set to *Do not verify*.

5 Click the *Manage Reverse Proxy Trust Store* icon. The auto import screen appears.



6 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.

7 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.

8 Specify an alias, then click *OK*.

All the displayed certificates are added to the trust store.

9 Click *Close*.

10 (Optional) For mutual authentication:

10a Select the certificate. Click the *Select Certificate* icon, select the certificate you created for the reverse proxy, then click *OK*.

10b Import the trusted root certificate of the CA that signed the proxy service's certificate to the Web servers assigned to this proxy service.

See your Web server documentation for instructions.

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

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

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

14 (Optional). Test this configuration from a client browser:

14a Enter the published DNS name as the URL in the browser.

14b Click the links that require authentication for access.

2.3 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 2.3.1, "Obtaining Externally Signed Certificates," on page 36
- Section 2.3.2, "Configuring the Identity Server to Use an Externally Signed Certificate," on page 38
- Section 2.3.3, "Configuring the Access Gateway to Use an Externally Signed Certificate," on page 40

2.3.1 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 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 36
- "Getting a Signed Certificate" on page 37
- "Importing the Signed Certificates and Root Certificate" on page 38

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	novell	_____
Organization	test	_____
City or town	Provo	_____
State or province	UTAH	_____
Country	US	

To create a signing request for the Identity Server:

1. In the Administration Console, click *Security* > *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: `novell`

   Organization: `test`

   City or town: `Provo`

   State or province: `UTAH`

   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.

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 for testing while you wait for the official certificate. Companies such as VeriSign offer trial signed certificates for testing.

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. If CA requires that you select a server platform, select eDirectory if available. If eDirectory is not a choice, select unknown or server not listed.
5. Click *Next*, then copy the signed certificate and paste it into a new text file or at the bottom of the signing request file.
6. Click *Back*, and repeat Step 2 through Step 5 for the Access Gateway.
7. Follow the instructions of the vendor to download the root certificate of the Certificate Authority and any intermediate CA certificates.

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. Either click *Browse* and locate the root certificate file or select *Certificate data text* and paste the certificate in the text box.
4. Click *OK*.

   The trusted root is added and is now available to add to trusted root stores.
5. (Conditional) Repeat Step 2 through Step 4 for any intermediate CA certificates.
6. In a text editor, open the signed certificate for the Identity Server.
7. In the Administration Console, click *Access Manager* > *Certificates*, then click the name of certificate signing request for the Identity Server.
8. Click *Import Signed Certificate*, then select *Certificate data text (PEM/Based64)*.
9. Paste the text for the signed certificate into the data text box. Copy everything from

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

   through

   ```
   -----END CERTIFICATE-----
   ```
10. Click *Add trusted root*, then either click *Browse* and locate the root certificate file or select *Certificate data text* and paste the certificate in the text box.
11. (Conditional) For any intermediate CA certificates, click *Add intermediate certificate*, then either click *Browse* and locate the intermediate certificate file or select *Certificate data text* and paste the certificate in the text box.
12. 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 *NetIQ Access Manager 3.2 Administration Console Guide*.
13. Repeat Step 6 through Step 12 for the Access Gateway certificate.

2.3.2 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 *Devices* > *Identity Servers.*
2. In the Configuration column, click *Edit*.
3. Change *Protocol* to HTTPS (the system changes the port to 8443), click *Apply,* then click *OK* at the warning.
4. In the *SSL Certificate* line, click the *Browse* icon.
5. In the *Certificates* section, click *Replace*, then click the *Browse* icon.
6. Select the Identity Server certificate, then click *OK* twice.
7. At the prompt to restart Tomcat, select to restart Tomcat now.

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

- If your Identity Server and Administration Console are on the same machine, you need to log in to the Administration Console again.
- If your Identity Server is on another machine, click *OK*.

9 Wait for the Identity Server health to turn green.

10 Click *Access Gateway* > *Edit* > *Service Provider Certificates* > *Trusted Roots*.

11 In the *Trusted Roots* section, click *Add*, then click the *Browse* icon.

12 Select the trusted root certificate of the certificate authority that signed the Identity Server certificate.

13 (Conditional) If you imported intermediate certificates for the CA, select them also.

14 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.

---

15 Click *Close*, then click *Access Gateways*.

16 Update the Access Gateway.

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

17a Enter the Base URL of the Identity Server in a browser.

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

17b 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.

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

18a Enter the URL to a protected resource on the Access Gateway.

18b 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 *NetIQ Access Manager 3.2 Identity Server Guide*.

2.3.3 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 2-1 on page 27) and between the Access Gateway and the browsers (channel 4 in Figure 2-1 on page 27).

1. In the Administration Console, click *Devices* > *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. Click *Auto-Import Embedded Service Provider Trusted Root*, then click *OK*.

   This adds the trusted root of the Access Gateway certificate to the trusted root store of the Identity Server.
7. Specify an *Alias* for the certificate, then click *OK* > *Close*.
8. On the Reverse Proxy page, click *OK*.
9. On the Server Configuration page, click *Reverse Proxy* / *Authentication*.
10. In the *Embedded Service Provider* section, click *Auto-Import Identity Server Configuration Trusted Root* and follow the prompts.

    This imports the trusted root certificate of the Identity Server into the trusted root store of the embedded service provider.
11. Click *OK* twice to return to the Access Gateways page.
12. On the Access Gateways page, click *Update*.
13. 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.

    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 *NetIQ Access Manager 3.2 Identity Server Guide*.

2.4 Using an SSL Terminator

An SSL terminator is a method of offloading the processor-intensive public key encryption algorithms involved in SSL transactions to a hardware terminator or accelerator. This can be a separate card that plugs into a PCI slot in a computer that contains one or more coprocessors able to handle the SSL processing, or it can be a dedicated (and expensive) hardware device.

The most processing-intensive part of an SSL session is the stage where the SSL server (the Identity Server or Access Gateway) is required to decrypt the SSL session key (an asymmetric key) that has been sent to it from the SSL client (usually a Web browser). This is known as the SSL handshake. Typically a hardware SSL terminator offloads the processing of the SSL handshake while leaving the server software to process the less intense symmetric cryptography of the actual SSL data exchange. The terminator can also act as a proxy and handle all SSL operations, which allows the server that is behind the terminator use unencrypted connections.

The performance benefits to the Access Manager servers are very high, often resulting in faster performance and higher throughput.

Although the Access Manager configuration settings are the same for any SSL terminator, the process for configuring the terminator for rewriting varies with the hardware. The following explanations use the Citrix Netscaler SSL terminator to explain the required rewriter configuration. For more information about this SSL terminator, see the following documents:

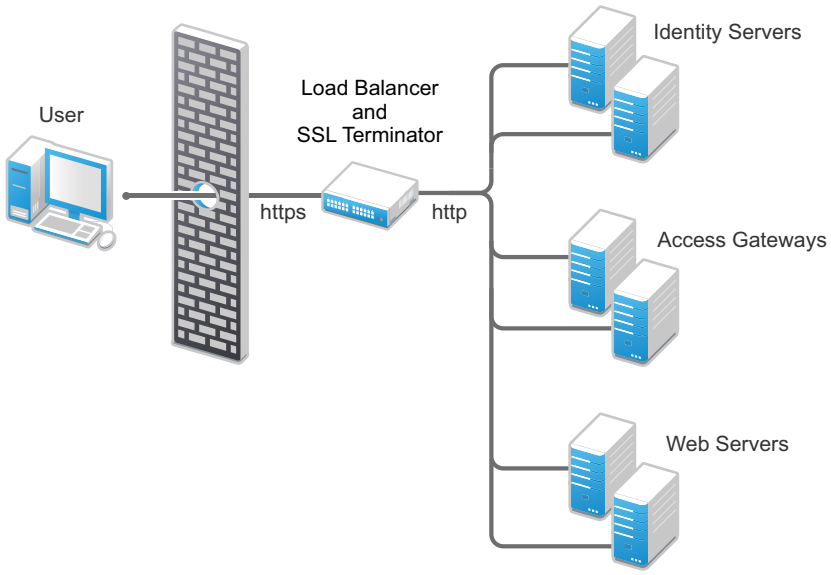
- Citrix NetScaler Traffic Management Guide (http://support.citrix.com/servlet/KbServlet/download/23213-102-645234/NS-TrafficMgmt-Guide.pdf) was used for general information about the device.
- SharePoint Deployment Guide (http://www.citrix.com/site/resources/dynamic/accessAnswers/SharePoint_Deployment_Guide.pdf) was used for the actual setup of the SSL terminator.

The following sections describe the required network configuration, the required Access Manager components, and the terminator and Access Gateway configuration process.

- Section 2.4.1, “Required Setup,” on page 42
- Section 2.4.2, “Configuring the SSL Terminator,” on page 42
- Section 2.4.3, “Configuring the Access Gateway,” on page 43

2.4.1 Required Setup

The following diagram illustrates the sample setup that was used for the configuration steps.



This setup has the following features:

- The Citrix Netscaler SSL terminator is configured to load balance (it provides the L4 switch functionality) and to offload the SSL traffic.
- The Identity Servers and the Access Gateways are accessible only through the SSL terminator via HTTP.
- The Identity Servers and the Access Gateways communicate to each other through the SSL terminator.
- The Identity Server cluster is configured to use HTTP on port 80. For information on translating the default 8080 port to 80, see "Translating the Identity Server Configuration Port" in the *NetIQ Access Manager 3.2 Identity Server Guide*.

2.4.2 Configuring the SSL Terminator

The configuration instructions assume that the SSL virtual servers have been created for the Access Gateways and Identity Servers on the SSL terminator. This sample configuration uses the logical name of "Access Manager Access Gateway" for the Access Gateway virtual server, and "Access Manager Identity Server" for the Identity Sever virtual server. The virtual server setup details are available in the documentation links referenced in Section 2.4, "Using an SSL Terminator," on page 41.

To enable the rewrite functionality:

1 Configure the SSL terminator to rewrite information in the HTTP header to be HTTPS:

The string used within the quotes is the virtual server name of the SSL virtual server. Each Access Manager component set has a different name for the virtual server.

1a At the command line, enter the following command for the Access Gateway:

```
set ssl vserver "Access Manager Access Gateway" -sslRedirect ENABLED -
redirectPortRewrite ENABLED
```

The "Access Manager Access Gateway" string needs to be replaced with the name you have specified for the Access Gateway virtual server.

Enabling SSL Redirect (-sslRedirect) causes the SSL terminator to convert any HTTP 302 redirect responses from back-end servers to HTTPS redirects.

1b At the command line, enter the following command for the Identity Server.

```
set ssl vserver "Access Manager Identity Server" -sslRedirect ENABLED -
redirectPortRewrite ENABLED
```

The "Access Manager Identity Server" string needs to be replaced with the name you have specified for the Identity Server virtual server.

2 Create a policy to scan the HTTP data (as opposed to headers) as it passes through the SSL terminator and replace references to http:// with references to https://.

At the command line, enter the following commands:

```
add rewrite action httpRewriteAction replace_all "http.res.body(50000)"
"\"https://\"" -pattern "http://"

add rewrite policy HttpToHttpsRewrite "http.res.body(50000).contains(\"http://
\")" httpRewriteAction
```

The (50000) value references the number of bytes to scan. This number can be tweaked for the size of the page; 50000 was from the Citrix support examples.

3 Bind the policy to the Identity Server virtual server.

At the command line, enter the following command:

```
bind lb vserver "Access Manager Identity Server" -policyName HttpToHttpsRewrite
-priority 100 -gotoPriorityExpression END -type RESPONSE
```

This command rewrites all Identity Server generated references of http to the https scheme. For example, the following entry in the default login (login.jsp) page includes an HTML form with an action tag that indicates where the credentials are to be posted. The page includes the following line:

```
<form name="IDPLogin" enctype="application/x-www-form-urlencoded"
method="POST" action="<%= (String) request.getAttribute("url") %>"
AUTOCOMPLETE="off">
```

When the JSP is executed, the following is sent back to the browser by the Identity Server:

```
<form name="IDPLogin" enctype="application/x-www-form-urlencoded"
method="POST" action="http://idp126.lab.novell.com/nidp/idff/sso?sid=4"
AUTOCOMPLETE="off">
```

With the policy defined above, the action tag is rewritten to the following:

```
<form name="IDPLogin" enctype="application/x-www-form-urlencoded"
method="POST" action="https://idp126.lab.novell.com/nidp/idff/sso?sid=4"
AUTOCOMPLETE="off">
```

2.4.3 Configuring the Access Gateway

With the SSL terminator rewriting HTTP to HTTPS for the Identity Server, the only changes required on the Access Manager side are for the Access Gateway. There are three particular cases where the Access Gateway must have its scheme rewritten:

- All Web pages rendered through the Access Gateway must have their schemes rewritten from HTTP to HTTPS.

Because of the complexity of Web pages, many SSL terminators have issues rewriting all references in a Web page from HTTP to HTTPS. The Access Gateway must take responsibility for this work.

By default, the Access Gateway rewriter does not rewrite the scheme if the proxy service and back-end Web servers use the same protocol. In this case, all traffic into the proxy is HTTP and all traffic to the back-end Web servers is also HTTP, which implies that no scheme rewriting takes place. Because the browser expects all links to reference HTTPS schemes, the Access Gateway must be configured to automatically rewrite all HTTP references on Web pages to HTTPS.

- The Liberty Authentication request generated by the Access Gateway must have the target URL rewritten to HTTPS.

  When a user accesses an Access Gateway protected resource, a corresponding Liberty authentication request is generated by the Embedded Service Provider and is sent to the Identity Server via the browser. This authentication request includes multiple attributes, including information about the trusted Liberty service provider generating the request, a target URL where the user must be redirected to post authentication, and the contract to be executed at the Identity Server. The target URL is embedded in this authentication request and references an HTTP resource. The Access Gateway must be able to rewrite this HTTP request to HTTPS. The following example was sent by the Access Gateway to the Identity Server via the browser.

```
HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=AF5484F1CD4D218C5404A17A0DA86E5A; Path=/nesp; secure
Location: http://idp126.lab.novell.com/nidp/idff/
sso?RequestID=idQgvQqocG6fgFrkeiUG6jlRD.LMk&MajorVersion=1&MinorVersion=2&Issu
eInstant=2010-05-
18T13%3A53%3A26Z&ProviderID=https%3A%2F%2Flag129.lab.novell.com%3A443%2Fnesp%2
Fidff%2Fmetadata&RelayState=MA%3D%3D&consent=urn%3Aliberty%3Aconsent%3Aunavail
able&ForceAuthn=false&IsPassive=false&NameIDPolicy=onetime&ProtocolProfile=htt
p%3A%2F%2Fprojectliberty.org%2Fprofiles%2Fbrws-
art&target=http%3A%2F%2Flag129.lab.novell.com%3A443%2Fformfill%2Fphpinfo.phpen
tRef=u&AuthnContextStatemscell%2Fsecure%2Fname%2Fpassword%2Furi
Date: Tue, 18 May 2010 13:53:26 GMT
Content-Length: 0
Via: 1.1 lag129.lab.novell.com (Access Gateway 3.1.1-265_eng_600589-
7AA324FFCBA4D4ED)
```

  The target parameter embedded within the authentication request references HTTP in the following line:

  http%3A%2F%2Flag129.lab.novell.com%3A443%2Fformfill%2Fphpinfo.php

  This needs to be rewritten to use the HTTPS scheme, for example:

  https%3A%2F%2Flag129.lab.novell.com%3A443%2Fformfill%2Fphpinfo.php

- The Location HTTP header in the 302 redirects must have its scheme rewritten from HTTP to HTTPS. There are two cases where the Access Gateway sends 302 redirects back to the browser:
  - When a non-authenticated user tries to access a protected resource, a series of HTTP redirects are generated by the Access Gateway that redirect the user to the Embedded Service Provider or to the Identity Server server requesting the user's credentials. Browsers execute on these 302 redirect status codes and generate corresponding requests to the URL defined in the Location HTTP header. The scheme on the Location header must be HTTPS and not the default HTTP.
  - When the back-end Web server sends a 302 redirect to the browser, the Access Gateway must interpret the URL and make any rewrites it deems necessary (such as scheme and path-based multi-homing path injection). Because the proxy and back-end Web server schemes are both HTTP in the setup, the Location header is not rewritten by default.

The Location header rewriting is handled by the SSL terminator. You have already enabled this rewriting in Step 1a on page 42.

To configure the Access Gateway to rewrite Web page references and the target URL:

1. In the Administration Console, click *Devices* > *Access Gateways* > *Edit* > *Reverse Proxy / Authentication*.
2. In the Proxy Settings section, select *Behind Third Party SSL Terminator*, then click *OK*.
3. Click *OK*, then update the Access Gateway.

3 Clustering and Fault Tolerance

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.
- **User 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.

  NOTE: This is not applicable for the Administration Console.

  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:

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

3.1.1 Prerequisites

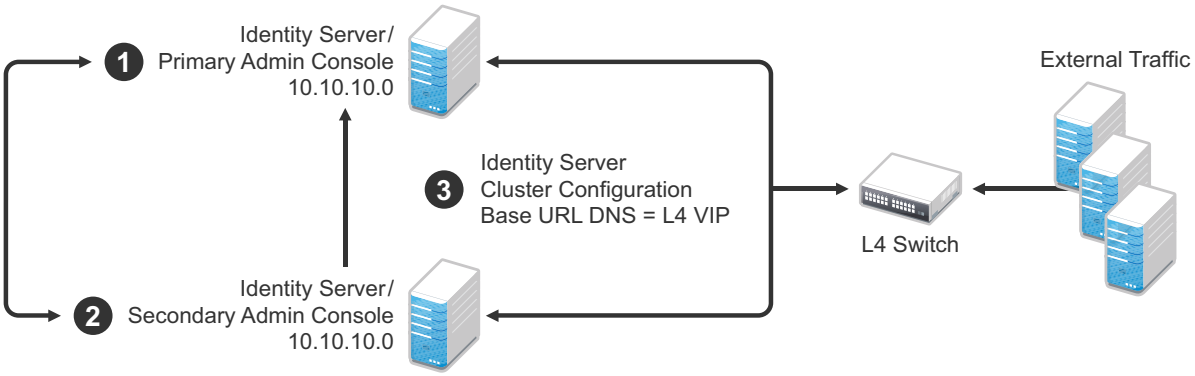
- ❒ The administration consoles must have their time synchronized. The easiest way to ensure this is to configure the machines to use the same network time server for time synchronization.
- ❒ Secondary consoles should be installed on the same operating system as the primary console. In other words, if your primary console is installed on Windows, all secondary consoles should also be installed on Windows. If your primary console is installed on Linux, all secondary console should be installed on Linux.
- ❒ If you are going to install your clustered Identity Servers on the same machines as your primary and secondary consoles, the Administration Consoles cannot be configured as a virtual group on an L4 switch. For more information, see "Managing Administration Consoles Installed on Clustered Identity Servers" on page 48.

Managing Administration Consoles Installed on Clustered Identity Servers

You can install the primary Administration Console and the Identity Server on the same machine, even when the Identity Server is going to be assigned to a cluster of Identity Servers. You can install a secondary Administration Console on another member of the Identity Server cluster. The 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) must pass through an L4. Figure 3-1 illustrates this configuration, showing Identity Servers on the same machine as Administration Consoles.

Figure 3-1 *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 NetIQ Identity Server" in the *NetIQ Access Manager 3.2 SP1 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 11.)

3.1.2 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 *NetIQ Access Manager 3.2 SP1 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 need 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, Access Gateway, and J2EE Agent with the following command:

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

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 *NetIQ Access Manager 3.2 Identity Server Guide*.

3.1.3 Understanding How the Consoles Interact with Each Other and Access Manager Devices

The primary and secondary consoles use eDirectory synchronization to keep their configuration databases current.

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.

Access Manager devices use the secondary console only when the primary console is down. Therefore, if a secondary console goes down while the primary console is running, the devices are notified. But they continue to run by using the primary console for configuration information. The secondary console can be down for as long as required to fix the problem without affecting the other Access Manager devices.

When the primary console goes down, all of the devices discover this and switch to using the secondary console. This can take a few minutes, because each device has its own trigger for checking in with the Administration Console. After the device has switched to using the secondary console, it continues to run just as it did when it was communicating with the primary console. When the primary console comes back online, all of the devices discover this and switch back to using the primary console. Again, this can take a few minutes.

Not all tasks are available from the secondary console:

- "Tasks Requiring the Primary Console" on page 50
- "Tasks Available from the Secondary Console" on page 50

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.

- **Linux:** Enter the following command:

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

- **Windows:** Enter the following commands:

  ```
  net stop Tomcat7
  net start Tomcat7
  ```

For more information about backup and restore, see "Backing Up and Restoring" in the *NetIQ Access Manager 3.2 Administration Console Guide*.

Tasks Available from the Secondary Console

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.

3.2 Clustering Identity Servers

A cluster of Identity Servers should reside behind a Layer 4 (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 3.1, "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.

IMPORTANT: Using a DNS round robin setup instead of an L4 switch for load balancing is not recommended. The DNS solution works only as long as all members of the cluster are working and in a good state. If one of them goes down and traffic is still sent to that member, the entire cluster is compromised and all devices using the cluster start generating errors.

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

3.2.1 Configuration Notes

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 unless you have enabled session failover. For more information about this feature, see "Configuring Session Failover" in the *NetIQ Access Manager 3.2 Identity Server Guide*.

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 Service Configuration

If your L4 switch can perform both SSL and non-SSL health checks, you should configure the L4 switch only for the services that you are using in your Access Manager configuration. For example, if you configure the SSL service and the non-SSL service on the L4 and the base URL of your Identity Server configuration is using HTTP rather than HTTPS, the health check for the SSL service fails. The L4 switch then assumes that all the Identity Servers in the cluster are down. Therefore, make sure you enable only the services that are also enabled on the Identity Server.

A Note about Alteon Switches

When you configure an Alteon switch for clustering, direct communication between real servers must be enabled. If direct access mode is not enabled 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.

3.2.2 Prerequisites

- ❒ An L4 server is 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 *NetIQ Access Manager 3.2 Identity Server Guide* for information about creating an Identity Server configuration. See "Assigning an Identity Server to a Cluster Configuration" in the *NetIQ Access Manager 3.2 Identity Server 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 *NetIQ Access Manager 3.2 Identity Server Guide*), you must configure the L4 switch to load balance on ports 8445 (identity provider) and 8446 (identity consumer).

3.2.3 Setting Up a Cluster

1. Install the additional Identity Servers.

   During the installation, choose option 2, *Install NetIQ 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.

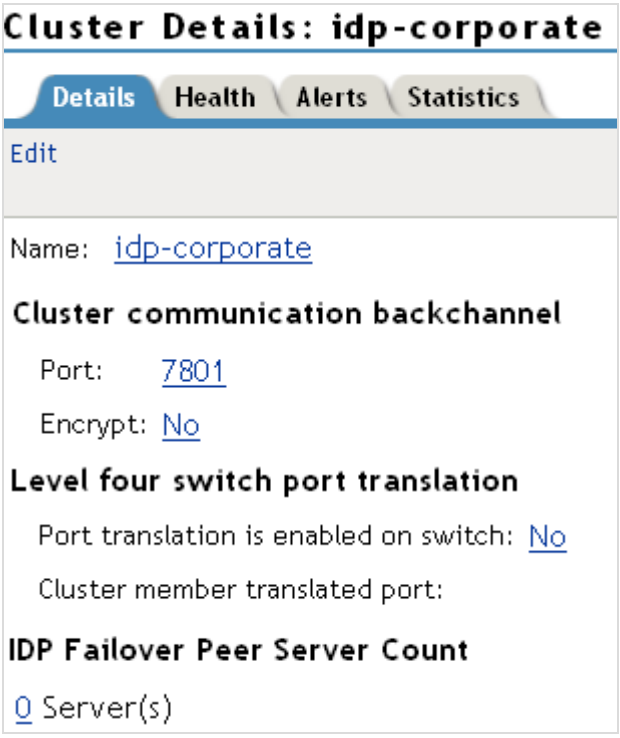
2. Assign the Identity Servers to the same cluster configuration.

   For more information about assigning servers to a configuration, see "Assigning an Identity Server to a Cluster Configuration" in the *NetIQ Access Manager 3.2 Identity Server 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 11.)

4. In the Administration Console, click *Devices* > *Identity Servers*, then click the configuration name you created for the cluster.

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: Provides an alternative to using iptables when you want to use port 443 on the L4 switch and port 8443 for cluster communication. This option only works if firewalls do not separate the Identity Servers from each other and the L4 switch supports port translation. To use this option, configure the base URL to use port 443, then configure the following options:

- **Port translation is enabled on switch:** Indicates that L4 switch has been configured to support port translation and that incoming traffic is using a different port than the cluster members.
- **Cluster member translated port:** Specifies the port the cluster members are configured to use. The default port that should be used for HTTPS is 8443.

If you have firewalls separating your Identity Servers or your L4 switch does not support port translation, you can use iptables to translate the port. For more information on iptables, see "Translating the Identity Server Configuration Port" in the *NetIQ Access Manager 3.2 Identity Server Guide*.

IDP Failover Peer Server Count: Enables session failover. For more information about this feature, see "Configuring Session Failover" in the *NetIQ Access Manager 3.2 Identity Server Guide*.

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 152, 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

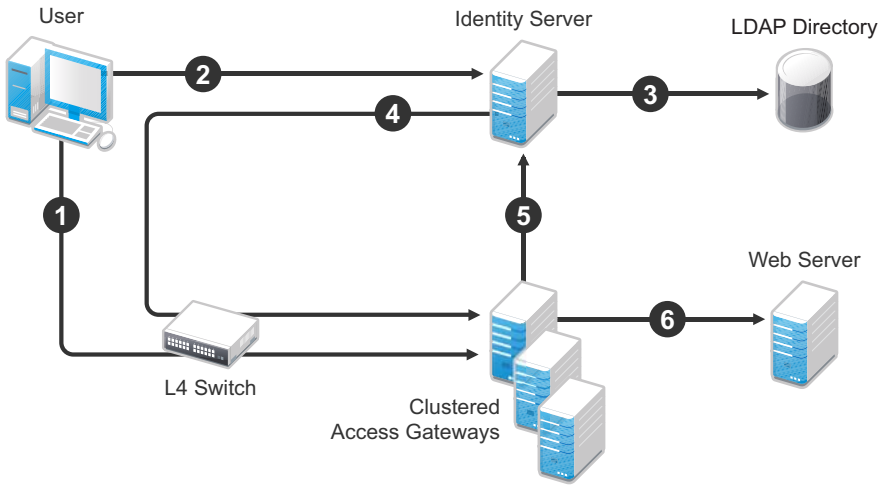
```
Current virtual servers settings:
  1: 149.44.174.220, enabled, dname idp
    virtual ports:
      8443: rport 8443, group 1, pbind clientip, frags
          real servers:
             1: 149.44.171.116,  weight 1,  enabled, backup none
             2: 149.44.174.51,   weight 1,  enabled, backup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

3.3 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 3-2 illustrates the flow of a user request when the Access Gateways are clustered behind an L4 switch.

Figure 3-2 *Clustering 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's session was established 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.

IMPORTANT: Using a DNS round robin setup instead of an L4 switch for load balancing is not recommended. The DNS solution works only as long as all members of the cluster are working and in a good state. If one of them goes down and traffic is still sent to that member, the entire cluster is compromised and starts generating errors.

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

3.3.1 Prerequisites

- ❒ An L4 switch is 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 is installed.

  When you install a 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.

3.3.2 Designing the Membership Type for a Cluster

You can create a cluster of all Gateway Appliances or of all Gateway Services. The Gateway Services cluster can contain both Linux and Windows versions of the Access Gateway Service. When you create a cluster of Access Gateways that are of the same type, you can guarantee that the user experience is always the same, regardless of which Access Gateway the user establishes a connection to. For a list of the differences between the Access Gateway Appliance and the Access Gateway Service, see “Feature Comparison of Different Types of Access Gateways” in the *NetIQ Access Manager 3.2 SP1 Installation Guide*.

3.3.3 Configuring a Cluster

1. In the Administration Console, click *Access Managers* > *New Cluster*.
2. Fill in the following fields:

   Cluster Name: Specify a display name for the cluster.

   Type: Select the type of cluster you want to create: Gateway Appliance or Gateway Service.

   Primary Cluster Server: Select the server that is to be the primary server in the cluster.
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. You cannot create a cluster that contains Access Gateway Appliances and Access Gateway Services. The cluster can contain only one type of Access Gateway.

   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. Click *OK*.

5 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.

6 (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 you create the cluster configuration for newly added servers, the listening address is always the IP address of eth0. If this is not the address where 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.

7 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. When you update the servers one at time, your site remains up. For more information on the *Update* and *Update All* options, see "Configuration Options" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

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 and the changes have been saved only in browser cache, the changes are lost and are not applied to the servers that are still in an *Update* status.

3.4 Clustering SSL VPN Servers

You can cluster the high-bandwidth SSL VPN servers to provide load balancing and fault tolerance capabilities and act as a single server. 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. Whenever a user accesses the virtual IP address (port 8080) assigned to the L4 switch, the system routes the user to one of the SSL VPN servers in the cluster, as traffic necessitates.

Clustering enables the following features:

- Cluster configuration synchronization for all members of the cluster.
- 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 processes the request.
- Load balancing among the cluster members.
- Transparent failover.

A cluster can be set up to function with an L4 switch or the Access Gateway to handle load balancing. A cluster can be set up to function with an L4 switch or by using the Access Gateway. You can have a cluster of servers in both HTTP and HTTPS. For more information on configuring the SSL VPN cluster by using the Access Gateway, see "Clustering SSL VPNs by Using the Access Gateway without an L4 Switch" in the *NetIQ Access Manager 3.2 SSL VPN Server Guide*.

This section has the following information:

For more information about SSL VPN clusters, see "Clustering the High-Bandwidth SSL VPN Servers" in the *NetIQ Access Manager 3.2 SSL VPN Server Guide*.

3.4.1 Prerequisites

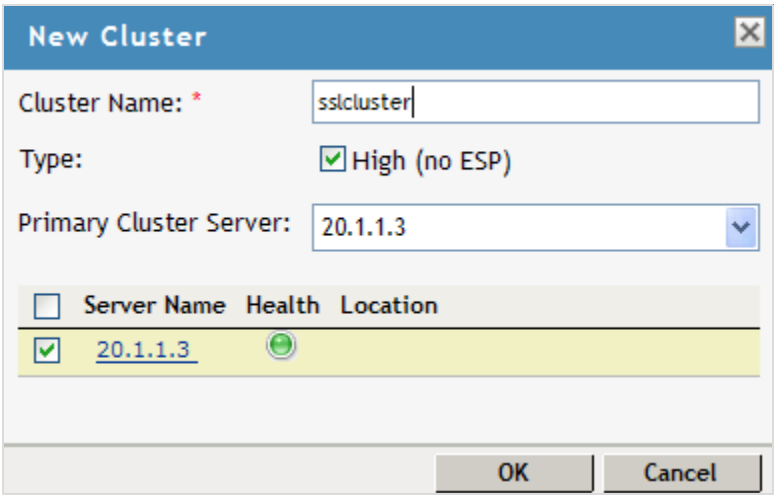
- ❒ An L4 switch is installed. The LB algorithm can be anything (hash/sticky bit), defined at the Real server level.
- ❒ Persistence (sticky) sessions are enabled on the L4 switch. You usually define this at the virtual server level.
- ❒ All SSL VPN servers must be running the high-bandwidth version and imported into the same administration console. The health status of all the imported servers must be green or yellow.
- ❒ The traffic policies must be imported into the SSL VPN servers before they are clustered.
- ❒ An SSL VPN Server configuration is created for the cluster, and all the SSL VPN servers are assigned to this configuration.

  The base URL DNS name of this configuration must be the virtual IP address of the L4 server. The L4 switch balances the load between the SSL VPN servers in the cluster.
- ❒ The following ports are open on the L4 switch for SSL VPN communication:
  - 8080 (for HTTP communication)
  - 8443 (for HTTPS communication)
  - 7777 (for Stunnel over TCP and OpenVPN over UDP)
  - 7778 (for OpenVPN over TCP)
- ❒ All members of an SSL VPN cluster should belong to either an ESP-enabled SSL VPN or a Traditional SSL VPN.

3.4.2 Creating a Cluster of SSL VPN Servers

To create a new SSL VPN server cluster, you start by creating a cluster configuration with a primary server.

1. In the Administration Console, click *Devices* > *SSL VPNs* > *Servers*.
2. Select the SSL VPN server that you want to add to the cluster, then click *New Cluster*.

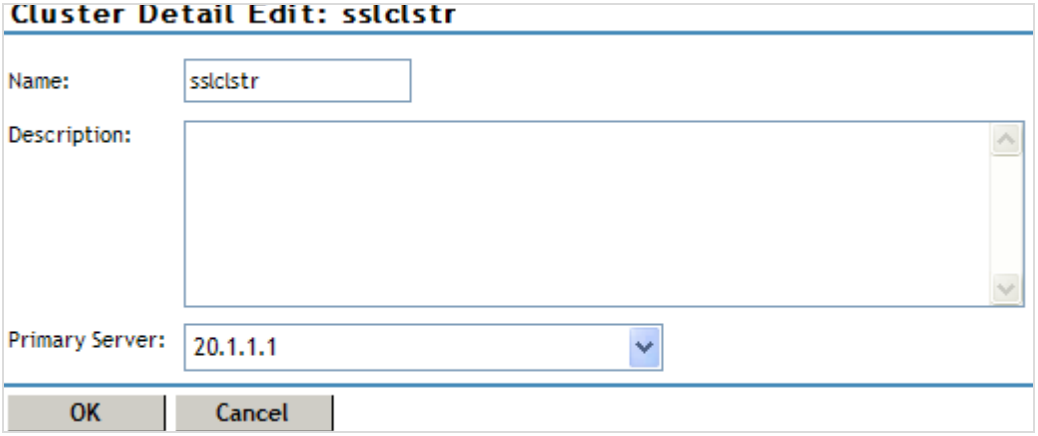


3 Specify a name for the cluster configuration. If you selected the server in the previous step, the IP address of the server is displayed in the *Primary Server* drop-down list. If you have not selected a server in the previous step, you can now select the server or servers that you want to assign to this configuration.

4 Click *OK*.

5 Click the cluster configuration name that you created.

6 On the Cluster Details page, click *Edit*.



7 Fill in the following fields as required:

Name: Specifies the name of the SSL VPN server cluster configuration. You can modify the name of the cluster if you want.

Description: Specify a brief description of the SSL VPN cluster.

Primary Server: Specify the IP address of the primary server in the SSL VPN server cluster.

The *Cluster Members* section displays the IP address and other details of the SSL VPN servers that are assigned to the cluster.

8 Click *OK*.

The status icons for the configuration and the SSL VPN Server should turn green. It might take several seconds for the SSL VPN server to start and for the system to display a green light.

3.5 Configuration Tips for the L4 Switch

When you use an L4 switch to cluster the 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 3.5.1, “Sticky Bit,” on page 60
- Section 3.5.2, “Network Configuration Requirements,” on page 60
- Section 3.5.3, “Health Checks,” on page 61
- Section 3.5.4, “Real Server Settings Example,” on page 65
- Section 3.5.5, “Virtual Server Settings Example,” on page 65

3.5.1 Sticky Bit

Each L4 switch has a slightly different method and terminology for the sticky bit or persistence bind. This bit allows a client that 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.

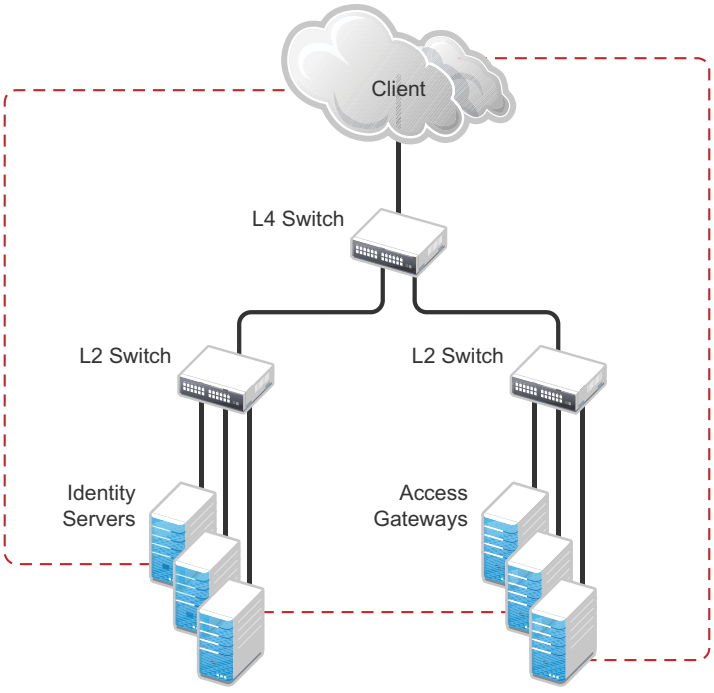
3.5.2 Network Configuration Requirements

When you set 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 you install 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 you use 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 be connected to separate ports in the L4 switch. If there is a connection in your network that allows 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 because networking protocols are configured to select the most direct route. Such a configuration causes communication problems because all traffic must be routed through the L4 switch. Figure 3-3 illustrates this problem.

Figure 3-3 *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 lines.

Figure 3-3 shows each cluster type with its own L2 switch. An Access Gateway cluster and an Identity Server cluster cannot share the same L2 switch because they can see the MAC address for each other. Networking protocols are configured to use the most direct route for the communication, and the MAC address is more direct than going up to the L4 switch and back down. Such a configuration causes communication problems because all traffic between the clusters needs to be routed through the L4 switch. Using a separate L2 switch for each cluster type prevents them from gaining access to the MAC address and forces communication to take place through the L4 switch.

3.5.3 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 the Identity Servers and Access Gateways:

- "Health Checks for the Identity Server" on page 61
- "Health Checks for the Access Gateway" on page 62

Health Checks for the 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 that 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 switch 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
```

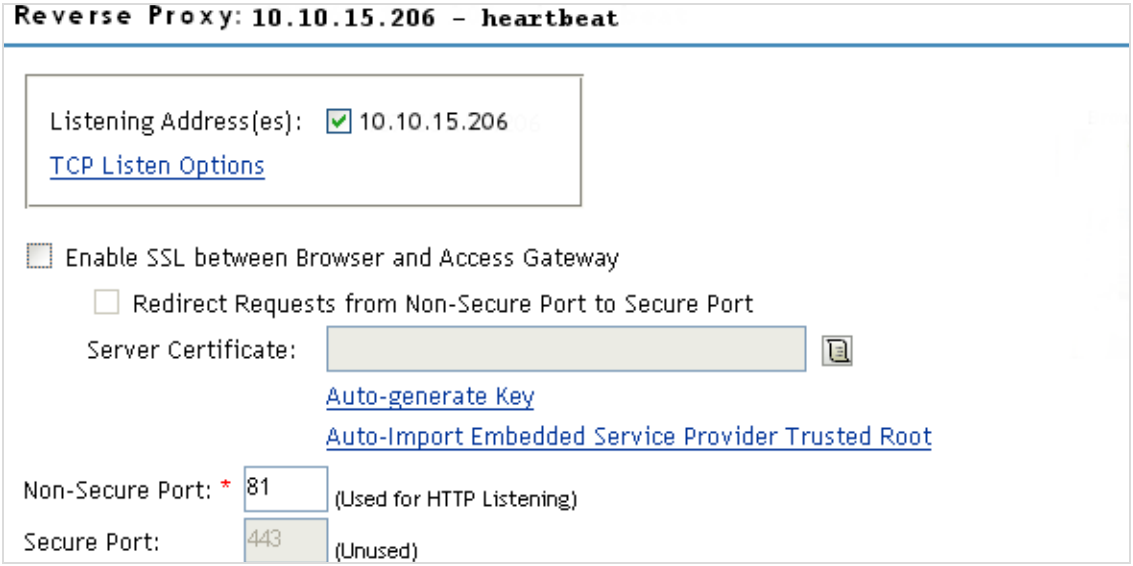
For an L4 switch to support an HTTPS query for the health of the Access Gateway, the switch must support an L7 health check. For a Foundry switch, the L7 health check script string should look similar to the following when the hostname is ag1 and the IP address is 10.10.172.

```
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
```

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. The following instructions configure this reverse proxy to use port 81, because port 80 on the specified IP address is reserved for redirects to the SSL port.

To create a reverse proxy for the health check:

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.

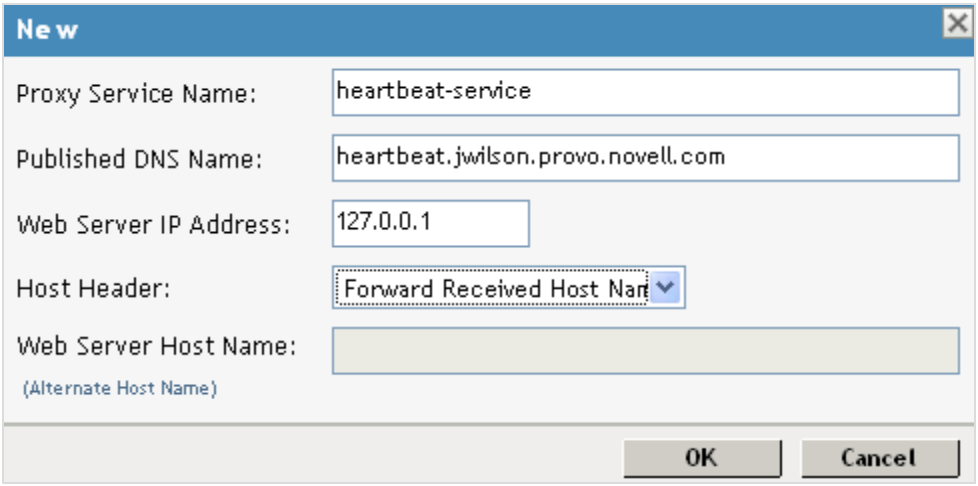


3 Change the *Non-Secure Port* to 81.

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.



5 Configure the following fields:

Proxy Service Name: Specify a name that identifies the purpose of this proxy service.

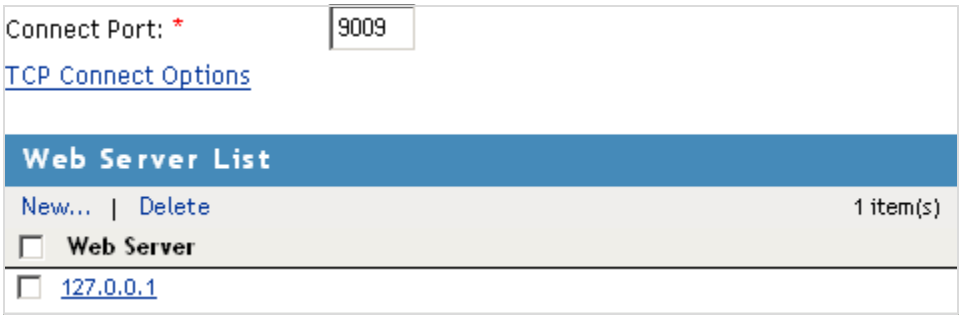
Published DNS Name: Specify a second DNS name that resolves to the VIP of the Access Gateways on the L4 switch. For example, if the DNS name is jwilson.provo.novell.com for the Access Gateways, you could use heartbeat.jwilson.provo.novell.com for the second name.

Web Server IP Address: Specify the internal address:127.0.0.1.

Host Header: Select *Forward Received Host Name*. This field is not used.

6 Click *OK*.

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



8 Change the *Connect Port* value on the Web Servers page to 9009.

The service provider (ESP) in the Access Gateway that provides the heartbeat service listens on 127.0.0.1:9009.

9 Click *Protected Resources*.

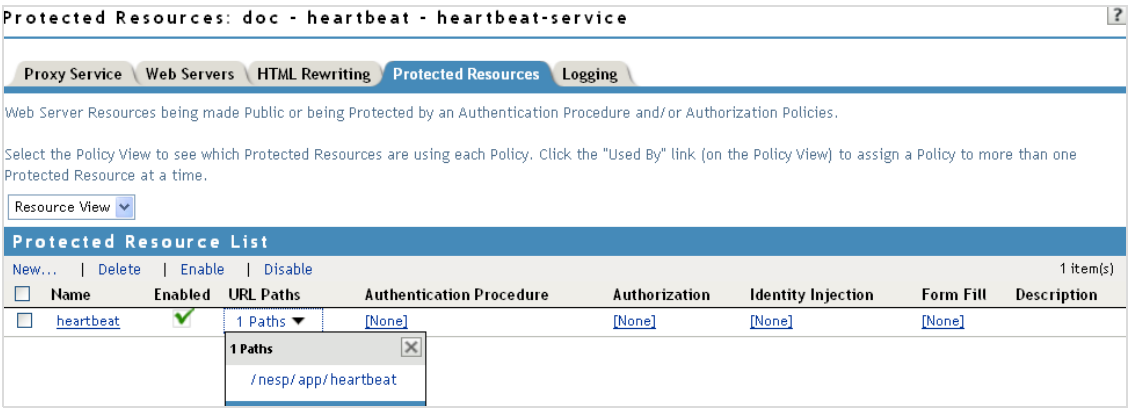
10 Click *New*, then specify a name.

11 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.

12 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.

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

14 Add a line similar 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
```

3.5.4 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 152, 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
```

3.5.5 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
```

3.6 Using a Software Load Balancer

Instead of using an L4 switch, you can cluster the Identity Servers and the Access Gateways behind a software load balancer that runs in Layer 7. Each manufacturer uses slightly different terminology, but the basic steps are quite similar. You need to create the following types of objects:

- Pools to specify how load balancing occurs, such as round robin.

- Persistence classes to be used within the pools to enable the sticky bit or to keep state so that a connection is sent to the same device.
- Monitors to be used within the pools for monitoring the health heartbeat of the device.
- Virtual servers to set up the ports and protocols for the pools.
- Traffic IP groups where the virtual IP addresses are set up and tied to the virtual servers.

Because the software actually runs in Layer 7, it does not require any special networking setup and it runs on standard server hardware.

As an example, the following instructions explain how to configure the Zeus ZXTM Load Balancer with HTTP and HTTPS for the Identity Server and Access Gateway. For more information about this product, see Zeus Technology (http://www.zeus.com/).

1. Create two persistence classes, one for HTTPS and one for HTTP.

   ```
   HTTP > J2EE Session Persistence
   HTTPS > SSL Session ID
   ```

2. Create four monitors, two for the Identity Servers and two for the Access Gateways.

   2a. Use the following paths to specify a path for HTTP and a path for HTTPS:

   Identity Server: `/nidp/app/heartbeat`

   Access Gateway: `/nesp/app/heartbeat`

   2b. Configure the following parameters for the monitors:

   HTTP: timeout=10 seconds, use_ssl=no, host_header: <domain>, body_regex: Success

   HTTPS: timeout=10 seconds, use_ssl=yes, host_header: <domain>, body_regex: Success

   Replace <*domain*> with the DNS name of the Access Manager device

3. Create four pools, one for each monitor. Configure each pool with the following parameters:

   ```
   Load _balancing: Round Robin
   persistence: <new class created>
   max_reply_time: 10
   ```

   For an HTTP resource, replace <*new class created*> with the HTTP class you created. For an HTTPS resource replace <*new class created*> with the HTTPS class you created.

4. Create four virtual servers, one for each port. Configure each with the following parameters:

   ```
   Protocol: <scheme>
   Port: <port>
   Pool: <pool created>
   ```

   Replace <*scheme*> with HTTP or HTTPS.

   Replace <*port*> with one of the following values: 80,8080,443, or 8443.

   Replace <*pool created*> with one of the pools you created in Step 3.

5. Create two traffic manager groups, one for the Identity Servers and one for the Access Gateway.

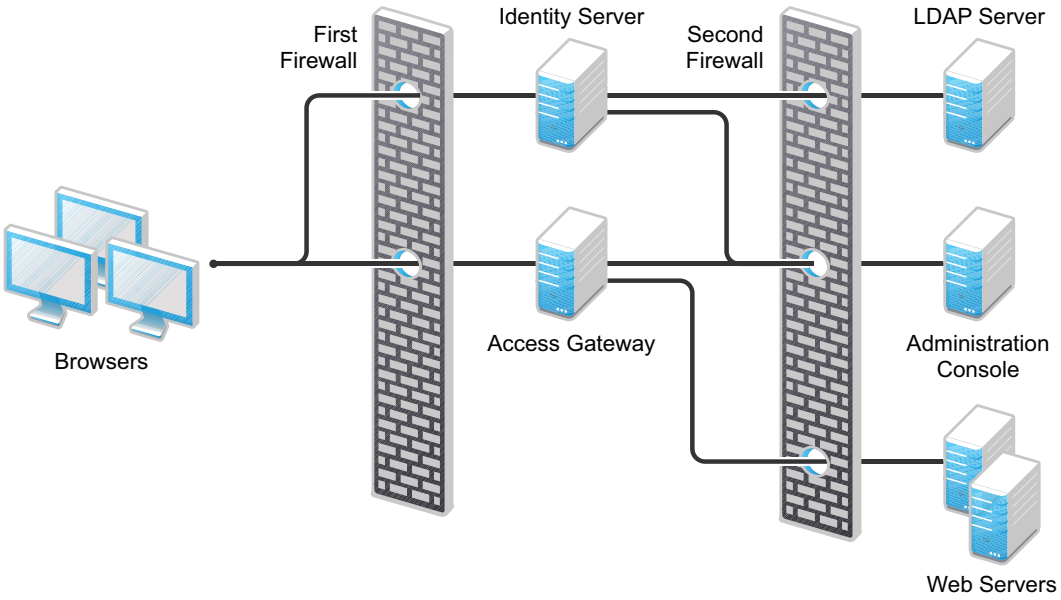
   This is where the virtual IP address is set up.

6. Start the traffic groups.

4 Setting Up Firewalls

Access Manager is not a firewall; it should be used with firewalls. Figure 4-1 illustrates a simple firewall setup for a basic Access Manager configuration of an Identity Server, an Access Gateway, and an Administration Console.

Figure 4-1 *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 4.1, “Required Ports,” on page 67
- Section 4.2, “Sample Configurations,” on page 76

4.1 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 4-1 *When a Firewall Separates an Access Manager Component from a Global Service*

Component	Port	Description
NTP Server	UDP 123	Access Manager components must have time 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 Linux 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.
Remote Windows Administration Workstation	Configurable	If you use RDP or VNC for remote administration and want to use it for remote administration of Access Manager components, you need to open the ports required by your application from the remote administration workstation to your Access Manager components. You need to open ports for console access and for file sharing. For console access, VNC usually uses TCP 5901 and RDP uses TCP 3389. For file sharing, UDP 135-139 are the default ports.

Table 4-2 *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 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 an Access Gateway Appliance	ICMP	During an import, the Access Gateway Appliance 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 Novell 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	TCP 524	Required to synchronize the configuration data store.
	TCP 636	Required for secure LDAP communication.
	TCP 427	Used for SLP (Service Location Protocol) communication.
	TCP 8080, 8443	Used for Tomcat communication.
Browsers	TCP 8080	For HTTP communication from the browsers to the Administration Console.
	TCP 8443, 2443, 2080.	For HTTPS communication from the browsers to the Administration Console. **NOTE**: 2443 and 2080 are optional ports required when the Administration Console and Identity Server are collocated.
	TCP 8028, 8030	To use iMonitor or DSTrace from a client to view information about the configuration store on the Administration Console.

Table 4-3 *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. The default ports for the Identity Server are TCP 8080 and 8443. They are configurable. You need to open the port that you configured for the Base URL of the Identity Server.
	TCP 80 or 443	For communication from the Identity Server to the Embedded Service Provider of the Access Gateway. This is the reverse proxy port that is assigned to be Embedded Service Provider (see the Reverse Proxy /Authentication page). This is usually either port 80 or 443.

Component	Port	Description
ESP Enabled SSL VPN	TCP 8080 or 8443	For authentication communication from the SSL VPN server to the Identity Server. TCP 8080 and 8443 are the default ports for the Identity Server. They are configurable. You need to open the port of the Base URL of the Identity Server. Also for communication from the Identity Server to the Embedded Service Provider of the SSL VPN server. This is the *Embedded Service Provider Base URL* on the Configuration page. The default values are TCP 8080 and 8443.
Traditional SSL VPN	N/A. The traditional SSL VPN server 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 *NetIQ Access Manager 3.2 Identity Server Guide*.
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	TCP 8443 or 443	For HTTPS communication. You can use iptables to configure this for TCP 443. See "Translating the Identity Server Configuration Port" in the *NetIQ Access Manager 3.2 Identity Server Guide*.
	TCP 7801, 7802	For back-channel communication with cluster members. You need to open two consecutive ports for the cluster, for example 7801 and 7802. The initial port (7801) is configurable. See"Configuring a Cluster with Multiple Identity Servers" in the *NetIQ Access Manager 3.2 Identity Server Guide*.
LDAP User Stores	TCP 636	For secure LDAP communication from the Identity Server to the LDAP user store.

Component	Port	Description
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, 3080, 3443	For HTTP communication from the browser to the Identity Server. You can use iptables to configure this for TCP 80. See "Translating the Identity Server Configuration Port" in the *NetIQ Access Manager 3.2 Identity Server Guide*. **NOTE**: 3080 and 3443 are optional ports. These are required when the SSL VPN and Identity Server are collocated.
	TCP 8443	For HTTPS communication from the browser to the Identity Server. You can use iptables to configure this for TCP 443. See "Translating the Identity Server Configuration Port" in the *NetIQ Access Manager 3.2 Identity Server Guide*.
CRL and OCSP Servers	Configurable	If you are using x.509 certificates that include an AIA or CRL Distribution Point attribute, you need to open the port required to talk to that server. Ports 80/443 are the most common ports, but the LDAP ports 389/636 can also be used.
Active Directory Server with Kerberos	TCP 88, UDP 88	For communication with the KDC on the Active Directory Server for Kerberos authentication.

Table 4-4 *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. The default ports are TCP 8080 and 8443, which are configurable. You need to open the port of the Base URL of the Identity Server.
	TCP 80 or 443	For communication from the Identity Server to the Embedded Service Provider of the Access Gateway. This is the reverse proxy port that is assigned to be Embedded Service Provider (see the Reverse Proxy /Authentication page). This is usually either port 80 or 443.
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.

Component	Port	Description
	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.
ESP Enabled SSL VPN	N/A. The ESP enabled SSL VPN server never communicates directly with the Access Gateway.	
Traditional SSL VPN	TCP 8080	(Access Gateway Appliance) For HTTP communication from the Access Gateway to the SSL VPN.
	TCP 8443	(Access Gateway Appliance) 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	TCP 7801, 7802	For back-channel communication with cluster members. You need the first port plus 1. The initial port (7801) is configurable. It is set by the Identity Server cluster configuration that the Access Gateway trusts. See“Configuring a Cluster with Multiple Identity Servers” in the *NetIQ Access Manager 3.2 Identity Server Guide*.
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.
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 4-5 *When a Firewall Separates the Traditional 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.	
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.	
SSL VPN Server	TCP 8900	For communication between the cluster members. This is a default port. You can use any other free port.
Browsers	TCP 8080	For HTTP communication.
	TCP 8443	For HTTPS communication.
SOCKS server	TCP 7777	For SOCKS communication from the SSL VPN to the SOCKS server. This is the default port for access to the SSL VPN, but it can be configured to use TCP 443.
OpenVPN	UDP 7777	For OpenVPN server communication. This is the default port for access to the SSL VPN, but it can be configured to use UDP 443.
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: On SLES 11 SP1 (or a higher version), you can edit this file or use YaST to configure UDP ports and internal networks.

Table 4-6 *When a Firewall Separates the ESP-Enabled SSL VPN from a Component*

Component	Port	Description
Identity Server	TCP 8080 or 8443	For authentication communication from the SSL VPN server 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.
		For communication from the Identity Server to the Embedded Service Provider of the SSL VPN server. This is the *Embedded Service Provider Base URL* on the Configuration page. The default values are TCP 8080 and 8443.
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.
ESP-Enabled SSL VPN	TCP 7801 and 8900	For communication between the cluster members. 8900 is a default port. You can use any other free port instead of 8900.
J2EE Agent	N/A. The SSL VPN never communicates with the J2EE Agent.	
Browsers	TCP 8080	For HTTP communication.
	TCP 8443	For HTTPS communication.
SOCKS server	TCP 7777	For SOCKS communication from the SSL VPN to the SOCKS server. This is the default port for access to the SSL VPN, but it can be configured to use TCP 443.
OpenVPN	TCP 7777	For OpenVPN server communication. This is the default port for access to the SSL VPN, but it can be configured to use UDP 443.
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.

Component	Port	Description
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: On SLES 11 SP1 (or a higher version), you can edit this file or use YaST to configure UDP ports and internal networks.

Table 4-7 *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 *NetIQ Access Manager 3.2 Identity Server 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.	

Component	Port	Description
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.

4.2 Sample Configurations

4.2.1 The Access Gateway and Identity Server in 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.

See, Figure 4-1 on page 67.

Table 4-8 *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.	
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 *NetIQ Access Manager 3.2 Identity Server 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 *NetIQ Access Manager 3.2 Identity Server Guide*.

Port	Purpose
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 *NetIQ Access Manager 3.2 Identity Server 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 *NetIQ Access Manager 3.2 Identity Server 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:

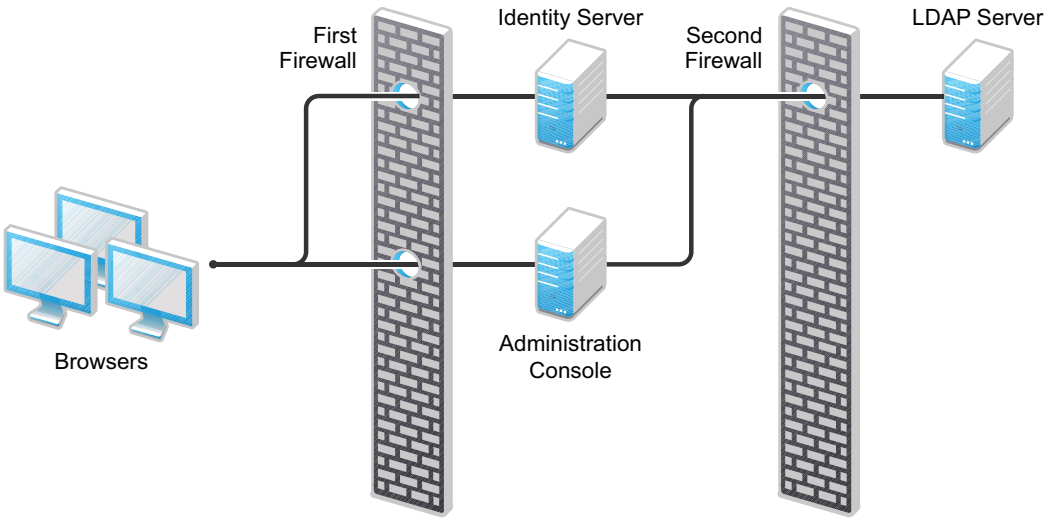
Table 4-9 *Ports to Open in the Second Firewall*

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.

4.2.2 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.

Figure 4-2 *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.

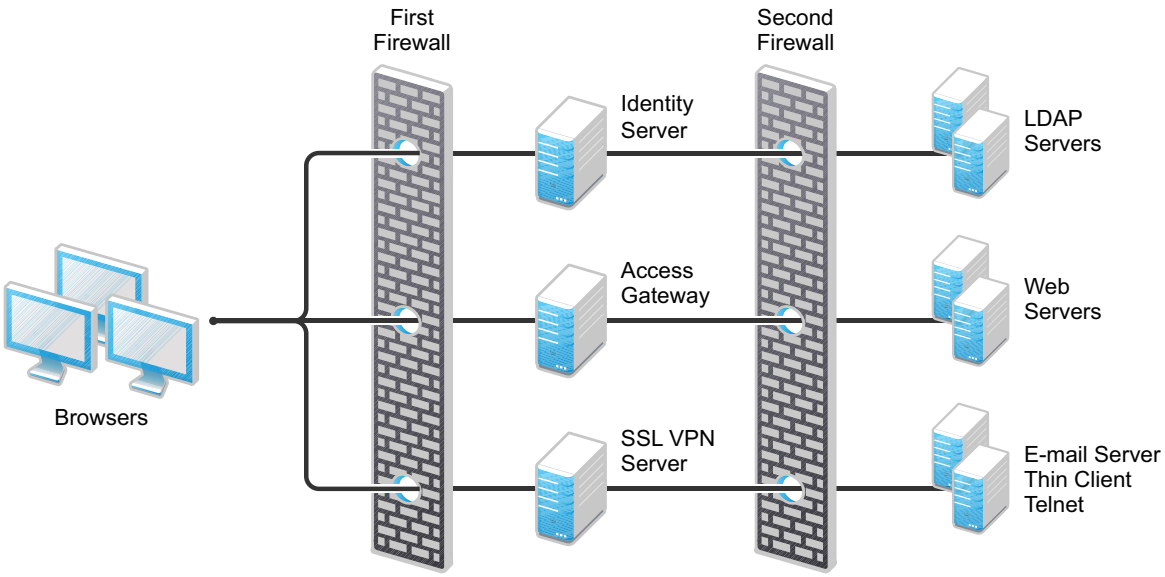
Table 4-10 *Ports to Open in the Second Firewall*

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.

4.2.3 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 4-3 *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 4-11 *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.

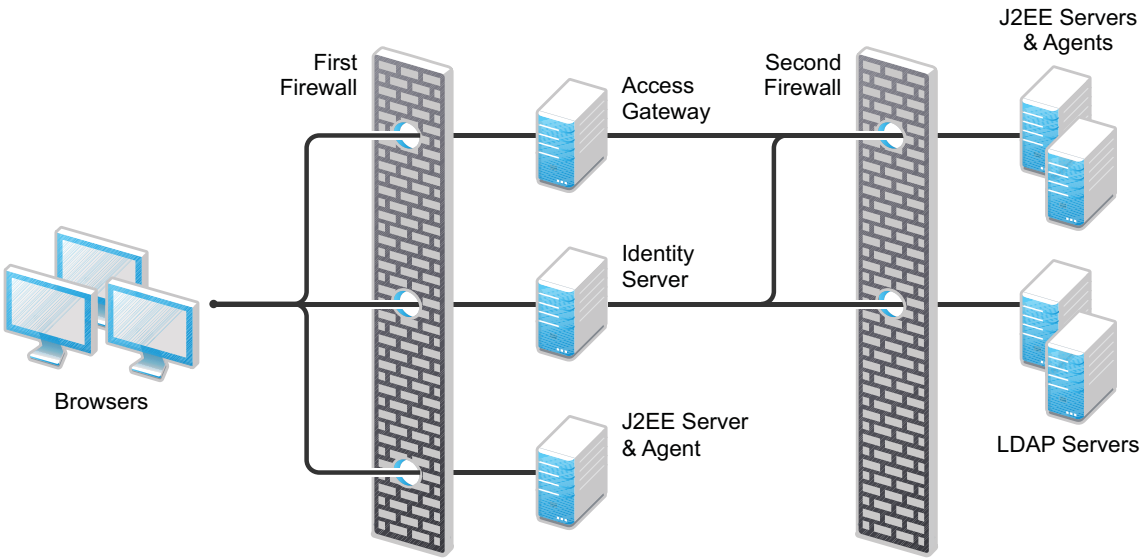
Table 4-12 *Ports to Open in the Second Firewall for SSL VPN*

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

4.2.4 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 4-4 *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 4-13 *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 4-14 *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.
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.

5 Setting Up Federation

Federation allows a user to associate two accounts with each other. This allows the user to log into one account and access 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.

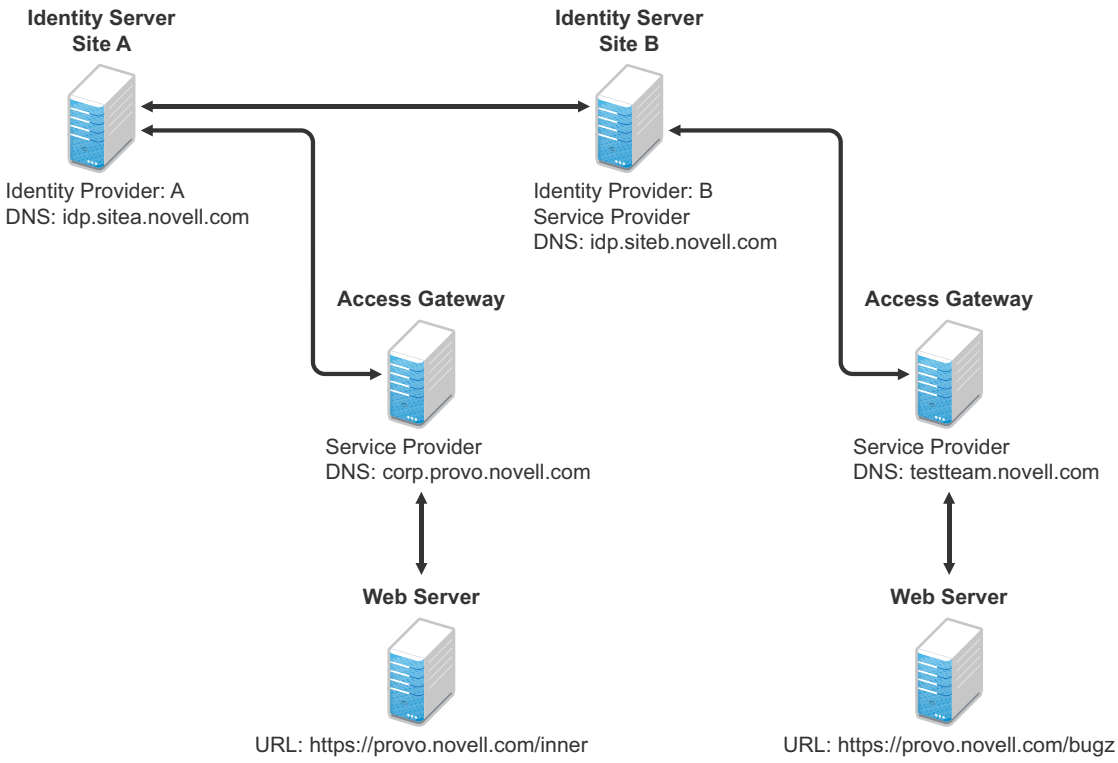
This section includes:

5.1 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 cant 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 5-1 illustrates such a network configuration where the user accounts of Site A are configured to federate with the user accounts at Site B.

Figure 5-1 *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 5-1 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.

5.2 Configuring Federation

Federation requires the configuration of a trusted relationship between an identity provider and a service provider. Figure 5-2 illustrates setting up federation between two identity servers, because a NetIQ Identity Server can act as either an identity provider or a service provider.

Figure 5-2 *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 5.2.1, “Prerequisites,” on page 86, 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 bidirectionally 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 5-1 on page 84 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 5.2.1, “Prerequisites,” on page 86, 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 5.3, “Sharing Roles,” on page 97 explains how to share the roles at Site A with Site B. For the SAML 1.1 protocol, the instructions starting in Section 5.2.1, “Prerequisites,” on page 86 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 you can 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 5.2.1, "Prerequisites," on page 86, 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 NetIQ Identity Servers have been divided as follows:

5.2.1 Prerequisites

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

  This can be the one you set up using the instructions in either Chapter 1, "Setting Up a Basic Access Manager Configuration," on page 9 or Chapter 6, "Digital Airlines Example," on page 111. For SSL configuration, see Chapter 2, "Enabling SSL Communication," on page 27.

  The Identity Server from this configuration becomes Site B in Figure 5-2.
- ❒ 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 5-2.
- ❒ 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 "Enabling Component Logging" in the *NetIQ Access Manager 3.2 Identity Server Guide*. Make sure that you enable at least application and protocol (Liberty, SAML1, or SAML2) logging at an Info level or higher.

5.2.2 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 87
- "Configuring Site B to Trust Site A as an Identity Provider" on page 88
- "Verifying the Trust Relationship" on page 90
- "Configuring User Authentication" on page 91

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. Import the trusted root certificate of Site B into the NIDP trust store of Site A:

   2a Click *Devices* > *Identity Servers* > *Edit* > *Security* > *NIDP Trust Store*.

   2b 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 5-2 specify the following:

   ```
   idp.siteb.novell.com
   ```

   Server Port: Specify 8443.

   2c Click *OK*, then specify an alias for the certificate (for example, SiteB).

   You will get two certificate options: Root CA Certificate and

   Server certificate. We recommend you to select Root CA Certificate.

   2d 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.

   2e Click *OK*.

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

   2f Click *Close*.

   2g Click *Devices* > *Identity Servers*, then update the Identity Server.

   Wait for the health status to return to green.

3. Configure a service provider for Site A:

   3a Click *Identity Servers* > *Edit* > *Liberty* [or *SAML 2.0* or *SAML 1.1*].

   3b 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 5-2, 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 5-2, 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 5-2, specify the following for SAML 1.1:

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

3c Click *Next* > *Finish* > *OK*.

3d Update the Identity Server.

Wait for the health status to return to green.

4 Continue with "Configuring Site B to Trust Site A as an Identity Provider" on page 88.

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 Import the trusted root certificate of Site A into the NIDP trust store of Site B.

2a Click *Devices* > *Identity Servers* > *Edit* > *Security* > *NIDP Trust Store*.

2b 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 5-2, specify the following:

```
idp.sitea.novell.com
```

Server Port: Specify 8443.

2c Click *OK*, then specify an alias for the certificate (for example, SiteA).

You will get two certificate options: Root CA Certificate and

Server certificate. We recommend you to select Root CA Certificate.

2d 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.

2e Click *OK*.

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

2f Click *Close*.

2g Click *Identity Servers* > *Update* > *OK*.

Wait for the health status to return to green.

3 Configure an identity provider for Site B.

3a Click *Identity Servers* > *Edit* > *Liberty* [or *SAML 2.0* or *SAML 1.1*].

3b Click *New*, select *Identity 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 SiteA_Liberty

Metadata URL: Specify the URL of the Liberty metadata on Site A. For Site A in Figure 5-2, 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 5-2, 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 5-2, specify the following for SAML 1.1:

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

3c Click *Next*.

3d To configure an authentication card, fill in the following:

ID: (Optional) Specify an alphanumeric number that identifies the card. If you need to reference this card outside of the Administration Console, you need to specify a value here. If you do not assign a value, the Identity Server creates one for its internal use.

Text: Specify the text that is displayed on the card to the user

Image: Specify the image to be displayed on the card. Select the image from the drop down list. To add an image to the list, click *Select local image*.

Login URL: (Conditional) If you are configuring an authentication card for SAML 1.1, specify an Intersite Transfer Service URL. For Figure 5-1 on page 84, 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 *NetIQ Access Manager 3.2 Identity Server Guide*.

Show Card: Determine whether the card is shown to the user. If this option is not selected, the card is only used when a service provider makes a request for the card. For this scenario, select this option.

Passive Authentication Only: Do not select this option.

3e Click *Finish* > *OK*.

3f Update the Identity Server.

Wait for the health status to return to green.

4 Continue with one of the following:

- If you are using Liberty or SAML 2.0, continue with "Verifying the Trust Relationship" on page 90.
- If you are using SAML 1.1, continue with "Configuring SAML 1.1 for Account Federation" on page 93.

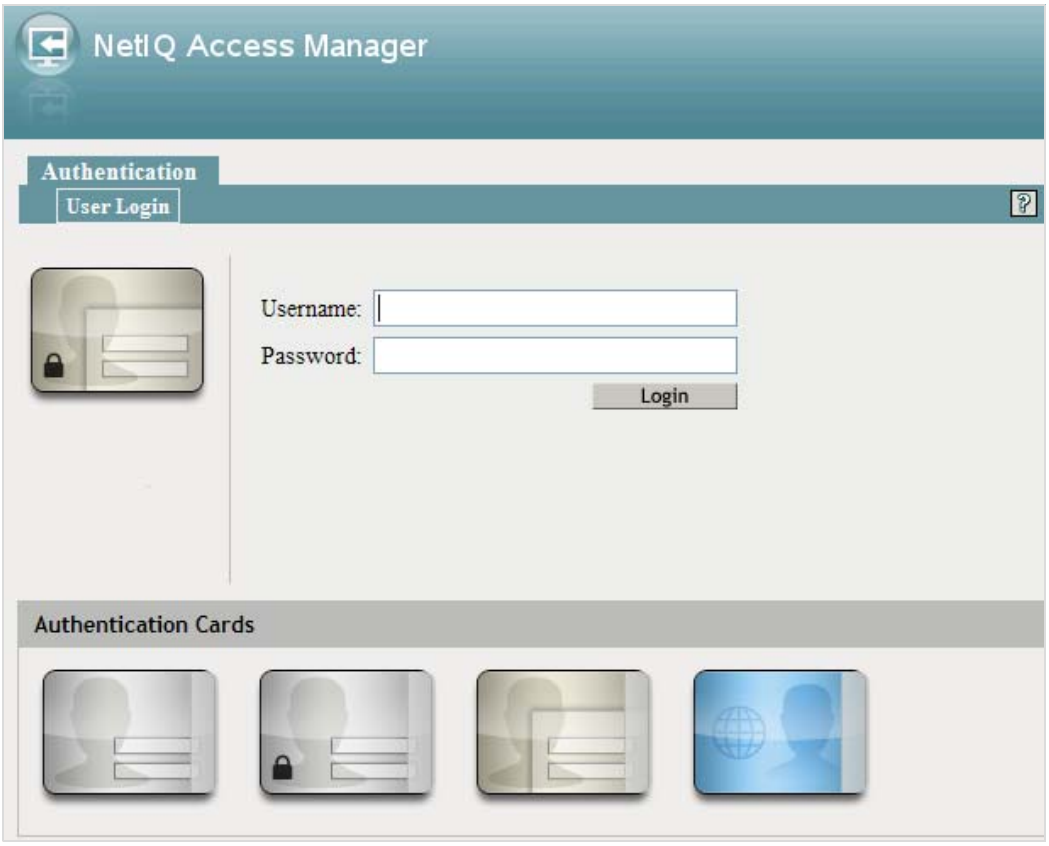
Verifying the Trust Relationship

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 5-2, specify the following:

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

The following login screen appears.



In this configuration, the customizable image was used for the Liberty authentication card.

2 Click the Liberty (or SAML 2.0) authentication card.

You are directed to Site A for login, with the default card selected for you. A screen similar to the following appears:

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 and Site B. To enable a single sign-on experience, the Identity Server at Site A, the Identity Server at Site B, and the protected resources of 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 91.

Configuring User Authentication

The following instructions describe one way to enable single sign-on to the Identity Servers and Access Gateways in Figure 5-1 on page 84. 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 Configure the authentication request:

2a Click *Devices* > *Identity Servers* > *Edit* > *Liberty* [or *SAML 2.0*] > *[Name of Identity Provider]* > *Authentication Card* > *Authentication Request*.

2b (Liberty) Verify the settings of the following fields:

Allow federation: 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.

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.

During authentication: Make sure this option is selected. Enabling this option allows federation to occur when the user selects the authentication card of the identity provider.

2c (SAML 2.0) Verify the settings of the following fields:

Persistent: Select this option to set up a persistent relationship between the two accounts.

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 after authentication.

During authentication: Make sure this option is selected. Enabling this option allows federation to occur when the user selects the authentication card of the identity provider.

2d For *Requested By*, select *Use Contracts*.

2e (SAML 2.0) For Context Comparison, accept the default value of *Exact*.

2f In the *Authentication contracts* section, select the name of the contract used by the protected resources and move it to the *Contracts* section.

If the contract you require is not in the list, it has not been configured for federation. See Step 3.

2g Click *OK*, then update the Identity Server configuration.

3 (Conditional) Configure the contract at Site B to allow federation:

3a Click *Identity Servers* > *Edit* > *Local* > *Contracts*.

3b 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.

NOTE: If site A only understands authentication class or type, select *Use Types* in the *Requested By* field and specify the authentication class in the *Allowable Class* field. Record the allowable class for the contract you are using. This allowable class should exist as a contract on site B. The name of the contract can be different at each site, but the allowable class must be the same.

3c Click the name of the contract.

3d Make sure the *Satisfiable by External Provider* option is selected.

3e Click *OK* twice, then update the Identity Server if you made any changes.

3f Return to Step 2 to select the contract.

4 If Site A is configured as a SAML 2.0 identity provider, move the contract(s) from the *Available contracts* list to the *Satisfies contract* list.

This will automatically redirect the authentication request from Site B to Site A when this contract is executed. Note that you can have multiple contracts in the *Satisfies contract* list.

5 Verify that Site A contains the same contract:.

5a Log in to the Administration Console for Site A.

5b Click *Identity Servers* > *Edit* > *Local* > *Contracts*.

5c Match the URI from Step 3b to a contract.

NOTE: Match the allowable class if you have selected *Use Types* in the *Requested By* field at site B.

If such a contract does not exist, you need to create it. For help, see "Configuring Authentication Contracts" in the *NetIQ Access Manager 3.2 Identity Server Guide*.

5d Click *OK*.

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

7 For the Authentication Contract, select the name of the contract from Step 5c.

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

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

10 Test the configuration:

10a Enter the URL to the user portal of Site B.

10b Click the federated login link to Site A.

10c Enter the credentials for Site A and log in.

10d Enter the URL for a protected resource at Site B.

You are granted access without being prompted for credentials.

11 If you want to allow federated users to log in at Site A rather than using the card at Site B to redirect them to Site A, complete the following tasks:

11a In the Administration Console for Site B, click *Devices* > *Identity Servers* > *Edit* > *Local* > *Defaults*.

11b For the Authentication Contract, select the name of the contract whose URI matches the URI of the contract used by Site A.

11c Click *Liberty* [or *SAML 2.0]* > *[Name of Identity Provider]* > *Authentication Card* > *Authentication Request*.

11d In the *Options* section, enable the *Use automatic introduction* option.

This enables single sign-on to Site B when the user has already federated the accounts at the two sites.

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

11f To test single sign-on, log in to the user portal on Site A, then enter a URL for a protected resource at Site B.

5.2.3 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 94
- "Configuring the Default Contract for Single Sign-On" on page 95
- "Verifying the Trust Relationship with SAML 1.1" on page 96

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 have unique e-mail addresses.

- "Configuring Site B for User Account Matching" on page 94
- "Configuring the Attribute for Sharing" on page 94
- "Configuring the Providers to Use the Shared Attribute" on page 95

Configuring Site B for User Account Matching

1. In the Administration Console of Site B, click *Devices* > *Identity Servers* > *Servers* > *Edit* > *SAML 1.1* > *[Identity Provider]* > *User Identification*.
2. 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*.
3. Select *Attribute matching*.

   The *Prompt for password on successful match* option is automatically selected. Leave this option enabled.
4. Click the *Define Attribute Matching Settings* icon.
5. Move the user store that you want to search for the attribute to the *User stores* list.
6. For the *User Matching Expression*, select *New User Matching Expression*.
7. Specify a name for the matching expression, such as email.
8. In *Logic Group 1*, click the *Add Attributes* 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.
9. Click *Finish*, then select your matching expression for the *User Matching Expression*.
10. Click *OK*.
11. Click *OK* twice, then update the Identity Server.
12. Continue with "Configuring the Attribute for Sharing" on page 94.

Configuring the Attribute for Sharing

1. In the Administration Console of the Site B (the service provider), click *Devices* > *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: Specify a name, such as email. Make sure you use the same remote name in the mapping for both Site B and Site A.

Leave the other options set to their default values.

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 95.

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 *Devices* > *Identity Servers* > *Edit* > *SAML 1.1* > *[Name of Identity Provider]* > *Attributes*.

2 For the *Attribute set*, select the set name you created in "Configuring the Attribute for Sharing" on page 94.

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 *Devices* > *Identity Servers* > *Edit* > *SAML 1.1* > *[Name of Service Provider]* > *Attributes*.

6 For the *Attribute set*, select the set name you created in "Configuring the Attribute for Sharing" on page 94.

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 95

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 2 in "Configuring Site B for User Account Matching" on page 94.

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

1 In the Administration Console for Site B, click *Devices* > *Identity Servers* > *Edit* > *Local* > *Defaults*.

2 For the Authentication Contract, select the name of the contract used by the user matching expression.

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

4 For Site A, repeat Step 1 through Step 3.

5 For the Access Gateway, review the contracts you have assigned to the protected resources:

5a In the Administration Console for Site B, click *Devices* > *Access Gateways* > *Edit* > *[Name of Reverse Proxy]* > *[Name of Proxy Service]* > *Protected Resources*.

5b For single sign-on, change the contract to match the contract for the user matching expression.

5c (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.

5d Click *OK* to save your changes, then update the Access Gateway.

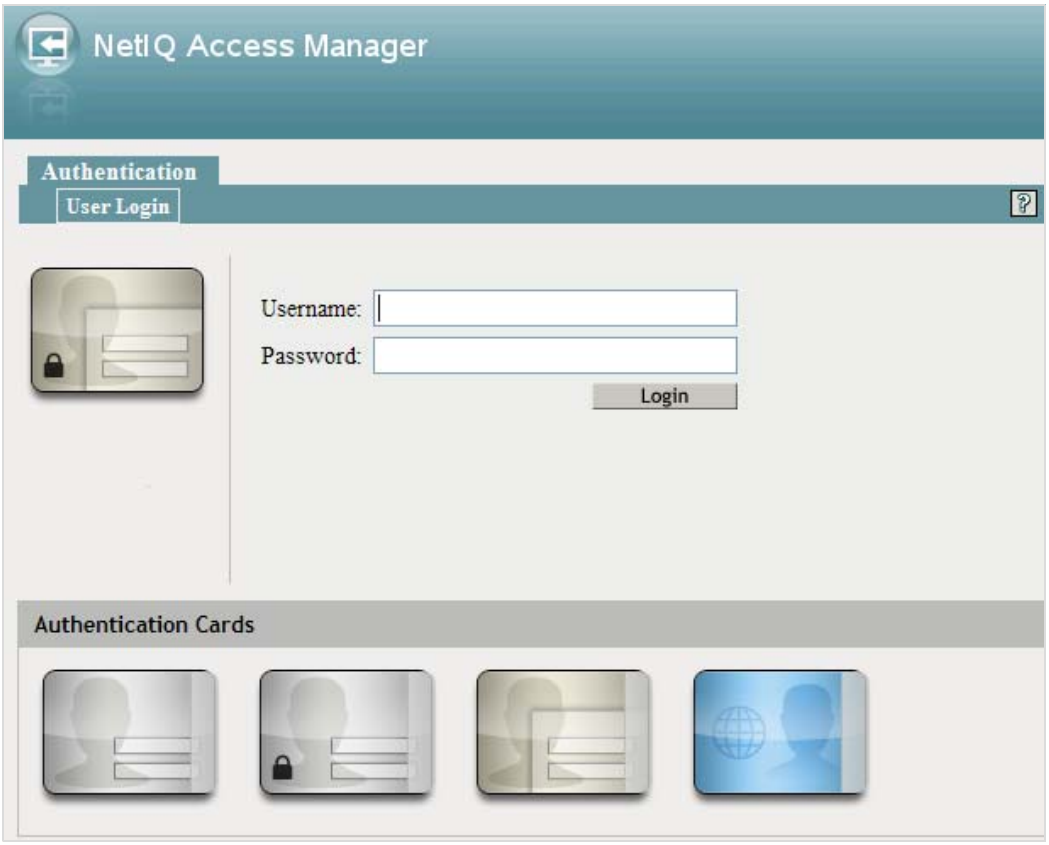
6 Continue with "Verifying the Trust Relationship with SAML 1.1" on page 96.

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 5-2, you would specify the following:

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

The following login screen appears:



Use the scroll bar to see all available cards.

2 Click the card you have configured for SAML 1.1 authentication.

You are directed to Site A for login.

3 Enter the credentials for Site A.

4 Enter the password for the user at Site B.

You are directed to the target page specified in the Login URL of the authentication card.

If you disabled the *Prompt for password on successful match* option on the User Identification page, the accounts are mapped without any user interaction.

5 (Conditional) If you receive an error, try one of the following:

- If you are not redirected to the target URL on Site B, verify the value you enter for the Login URL option. See Step 3d on page 89.
- If you receive an authentication error at Site B, verify the user matching setup. See "Configuring User Account Matching" on page 94.
- If you have enabled logging, open the logging file (`catalina.out` or `stdout.log`) and search for the error string. There should be additional information on the cause of the error in the error string entry as well as log entries before the error sting.

6 (Optional) If your protected resources on Site A and Site B use the same contract, enter the URLs of these resources.

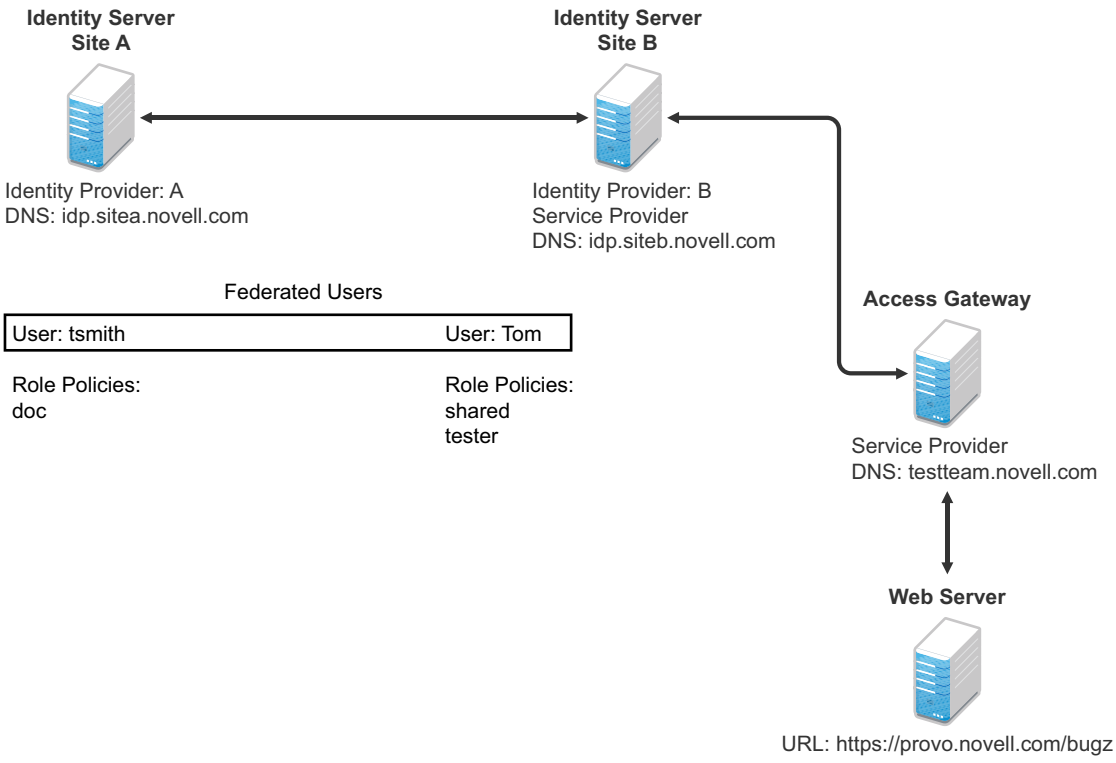
You are granted access without entering any additional credentials.

5.3 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 NetIQ Identity Servers. If you are using a third-party identity or service providers, you need to modify the instructions.

Figure 5-3 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 5-3 *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. However, Tom does not have the qualifications at Site B to be assigned the tester role.

In this scenario, when Tom requests access to the protected 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 now 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 5.2.2, "Establishing Trust between Providers," on page 87.
- 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 6.4.2, "Configuring a Role-Based Policy," on page 123, and for the Authorization policy, see Section 6.4.3, "Assigning an Authorization Policy to Protect a Resource," on page 131. 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.

5.3.1 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

1. In the Administration Console of the Site A (the identity provider), click *Devices* > *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: Specify a name, such as roles. Make sure you use the same remote name in the mapping for both the identity provider and the service provider.

   Leave the other options set to their default values.
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 99.

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 5-3, this is Site A.)
   - **1a** Click *Devices* > *Identity Servers* > *Edit* > *Liberty* > *[Name of Service Provider]* > *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 these 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 5-3, this is Site B.)
   - **2a** Click *Devices* > *Identity Servers* > *Edit* > *Liberty* > *[Name of Identity Provider]* > *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 99.

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 *Policies* > *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.

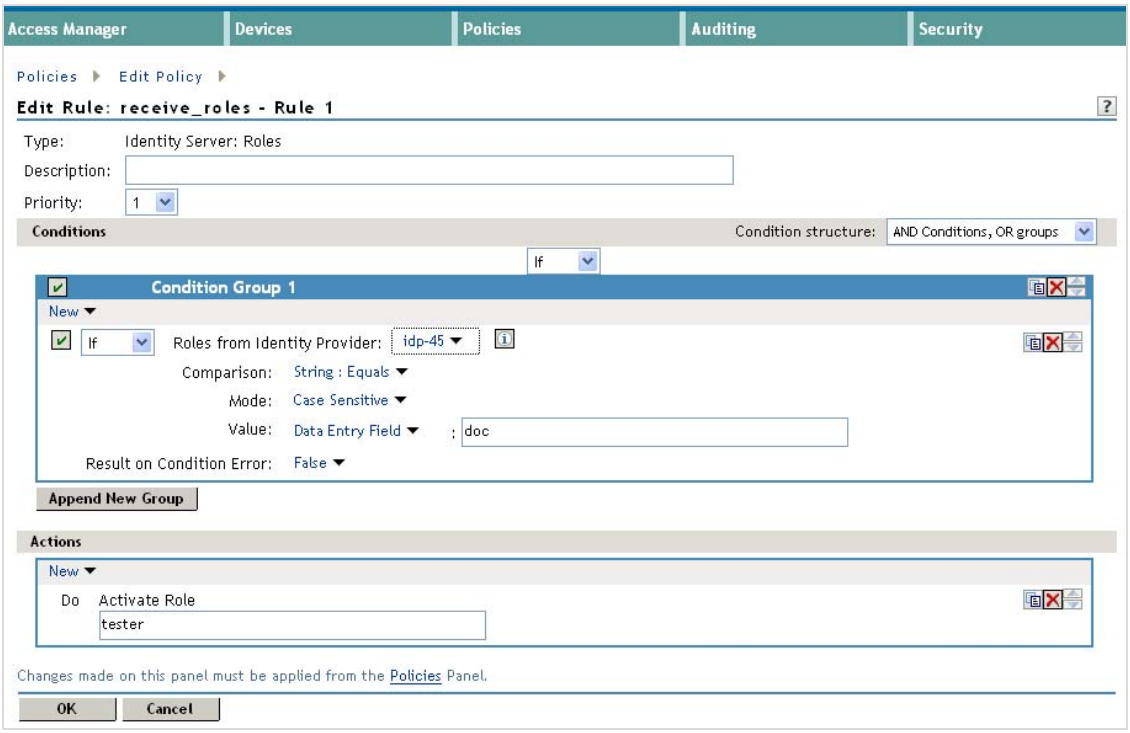
In this example, you have federated with only the identity provider at Site A, and it is selected for you.

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 5.3.2, "Verifying the Configuration," on page 101 to discover the problem.

5.3.2 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 5-3, "Two Federated Identity Servers," on page 97. 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 "Enabling Component Logging" in the *NetIQ Access Manager 3.2 Identity Server Guide*.

   You can access log files for downloading and viewing by clicking *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 (Linux) or the `stdout.log` file (Windows) 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> 2009-08-22T20:30:19Z 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 *NetIQ Access Manager 3.2 Policy Guide*.

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

   In the `catalina.out` file (Linux) or the `stdout.log` file (Windows) of the Identity Server from Site A, look for lines similar to the following:

   ```
   <amLogEntry> 2009-08-22T20:30:19Z INFO NIDS Application: AM#500105018:
   AMDEVICEID#C5F467BA50B009AC: AMAUTHID#DEEF6BEC3655DEB71CA56832DDDF866E:
   Responding to AuthnRequest with artifact
   AAPLsCVpfv3ha9Mpn+cUiCXcf3D63sc0QfscL5mZaaygHBKVOOh9aPSQ </amLogEntry>

   <amLogEntry> 2009-08-22T20:30:19Z 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 99.

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

In the `catalina.out` file (Linux) or the `stdout.log` file (Windows) of the Identity Server from Site B, look for lines similar to the following:

```
<amLogEntry> 2009-08-22T20:30:19Z INFO NIDS Application: AM#500105020:
AMDEVICEID#488475009C6D3DDF: AMAUTHID#0FBA0CF7E41E6C7F9121DABB918D34F4:
Received and processing artifact from IDP -
AAPLsCVpfv3ha9Mpn+cUiCXcf3D63sc0QfscL5mZaaygHBKVOOh9aPSQ </amLogEntry>

<amLogEntry> 2009-08-22T20:30:19Z 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 99.

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

In the `catalina.out` file (Linux) or the `stdout.log` file (Windows) 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.
NxpeOperator@string-equals~(0):hidden-param:hidden-value:~~~True(69)

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

<amLogEntry> 2009-08-22T20:30:20Z 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 99.

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> 2009-08-22T20:30:20Z 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=accessManagerCon
tainer,o=novell:romaContentCollectionXMLDoc),Policy=(Allow_Tester),Rule=(1::Ru
leID_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.

5.4 Setting Up Federation with Third-Party Providers

Setting up federation with providers other than NetIQ Identity Servers requires the same basic tasks as setting up federation with NetIQ 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 need to negotiate a schedule for these configuration changes.
- The other site might not be 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 must 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 NetIQ 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 need to negotiate with the provider to send you metadata that has been validated.
- Most third-party providers do not support authentication cards and contracts. However, most do support either authentication types or authentication URIs. You can use either of these to map from their authentication procedure to an Identity Server authentication contract.

For sample implementations with third-party providers that explain the modifications that were required to set up the federation, see the following:

- "Integrating Novell's Access Manager with Shibboleth's IDP Server" (http://www.novell.com/communities/node/6943/integrating-novells-access-manager-shibboleths-idp-server)
- "Integrating Google Apps and Novell Access Manager using SAML2" (http://www.novell.com/communities/node/8645/integrating-google-apps-and-novell-access-manager-using-saml2)
- "SAML 1.1 with Concur" (http://www.novell.com/coolsolutions/appnote/19673.html)

5.5 External Attribute Source Policy Examples

You can use an External Attribute Source policy to retrieve attributes from external sources. You can create shared secrets from this policy. This shared secret then can be used in configuring other policies or can be used by the Identity Servers in their attribute sets to retrieve attributes from external sources.

An External Attribute Source policy must be enabled and configured before using the policy for retrieving the attributes from external sources.

For more information about how to create an External Attribute Source policy, see "Creating External Attribute Source Policies" in the *NetIQ Access Manager 3.2 Policy Guide*.

This section describe the usages of the External Attribute Source policy with the help of the following scenarios:

- Section 5.5.1, “Scenario 1,” on page 104
- Section 5.5.2, “Scenario 2,” on page 106

5.5.1 Scenario 1

e_Health is a Web portal for doctors. e_Health uses Med_Association as an external identity provider to verify whether the user is a doctor and obtain the user's professional code and specialization. Med_Association retrieves these details with the help of the NetIQ Identity Server.

Med_Association completes the following steps:

1. Write an External Attribute data extension class and use the required attribute to retrieve the professional code and specialization of user.

   For more information about data extension class, see “Adding Policy Extensions” in the *NetIQ Access Manager 3.2 Policy Guide*.

   For more information on data extension example code, see The Policy Extension API in the Novell Access Manager 3.2 Developer Kit (http://developer.novell.com/documentation/nacm32/nacm_enu/data/bookinfo.html) guide.

2. Create an External Attribute Source policy for the data extension.

   For more information about how to import the data extension class and configure the External Attribute Source policy in the Identity Server, see “Configuring an External Attribute Source Policy” in the *NetIQ Access Manager 3.2 Policy Guide*.

3. Define a shared secret for the professional code and specialization.

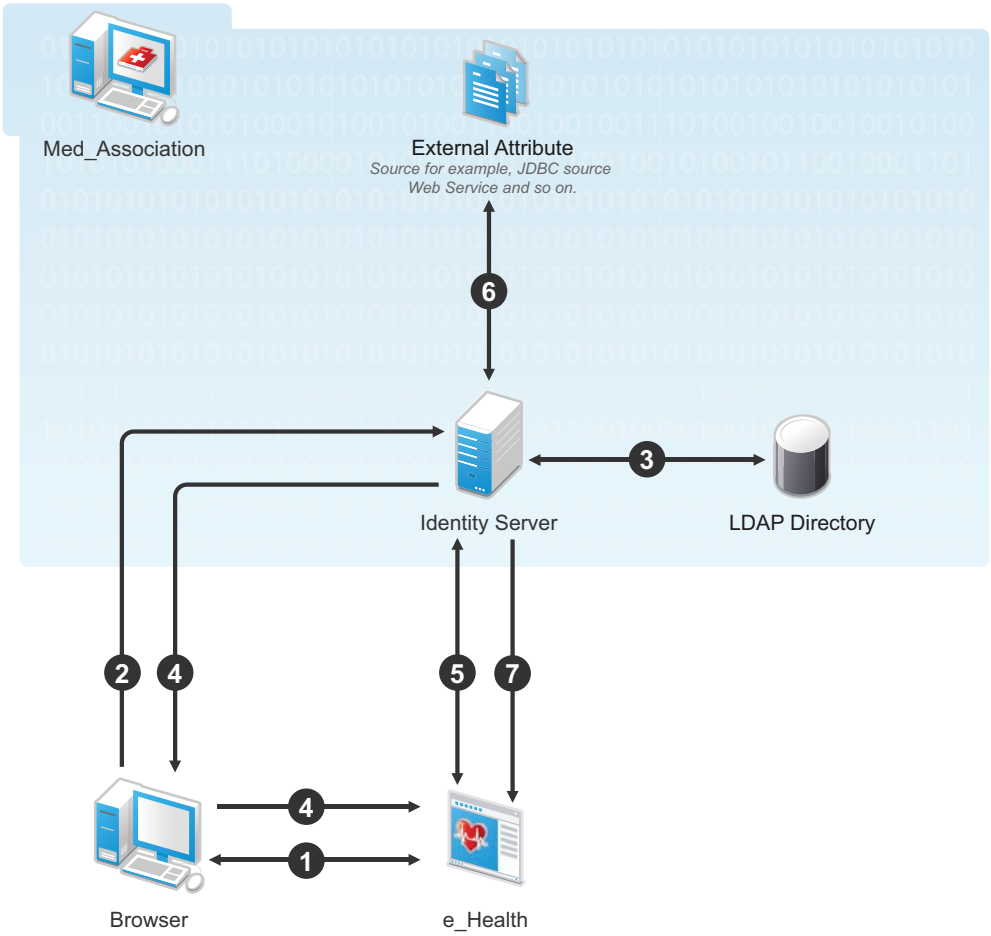
   For more information, see “Adding Custom Attributes” in the *NetIQ Access Manager 3.2 Identity Server Guide*.

4. Configure this shared secret for a service provider to be sent with authentication.

   For more information, see “Configuring the Attributes Sent with Authentication”in the *NetIQ Access Manager 3.2 Identity Server Guide*.

5. The retrieved details that are professional code and specialization are sent to e_Health.

The following diagram illustrates this scenario:



Workflow:

1. User requests for access to e-Health through browser.
2. e_Health redirects the user's browser to the NetIQ Identity Server at Med_Association for authentication.
3. User logs in with providing credentials. User is authenticated with LDAP.
4. On the successful authentication, the Identity Server sends the assertion to e_Health.
5. e_Health verifies the assertion with Med_Association by using the back channel communication.
6. After verification, the NetIQ Identity Server retrieves the attributes (professional code and specialization) from external sources (for example, database) by using the External Attribute Source policy.
7. The Identity Server returns the professional code and specialization as an attribute in the response. If the user is not a doctor, external source returns null values in the attribute in the response.

   e_Health grants access to the user if it receives valid values for the attributes in the authentication response else it denies the access.

5.5.2 Scenario 2

Company XYZ is a customer of NetIQ Access Manger. The employees of this company get authenticated to the Identity Server. Each employee's mail attribute is retrieved from the user store. XYZ wants only user name part of the email address to be displayed on the Home page after authentication. This can be achieved by using the External Attribute Source policy.

XYZ completes the following steps:

1. Write an External Attribute data extension class and use the mail attribute as the parameter to the class.

   For more information about data extension class, see "Adding Policy Extensions"in the *NetIQ Access Manager 3.2 Policy Guide*.

2. In the data extension class, read the email address and parse the name identifier in it and return as an attribute. For more information on data extension example code and example code for this scenario, see The Policy Extension API in the Novell Access Manager 3.2 Developer Kit (http://developer.novell.com/documentation/nacm32/nacm_enu/data/bookinfo.html) guide.

3. Define a shared secret for the name field of the email address.

   For more information, see "Adding Custom Attributes" in the *NetIQ Access Manager 3.2 Identity Server Guide*.

4. Create an External Attribute Source policy for the data extension.

   For more information about how to import the data extension class and configure the External Attribute Source policy in the Identity Server, see "Configuring an External Attribute Source Policy" in the *NetIQ Access Manager 3.2 Policy Guide*.

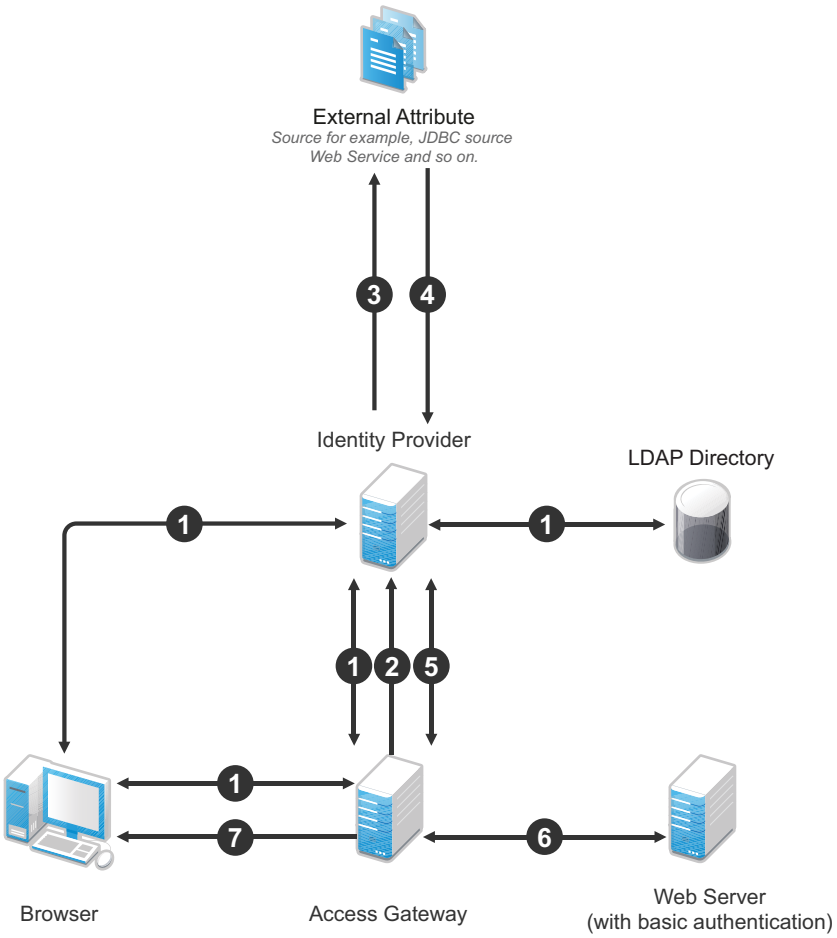
5. Create an Identity Injection policy.

   For more information, see "Creating Identity Injection Policies"and Configuring a Custom Header Policy in the NetIQ Access Manager 3.2 Policy Guide.

6. The Identity Server sends the user ID part of email address to the Access Gateway.

   In turn, the Access Gateway or service provider sends this attribute to the configured Web server. For example, John is an employee of XYZ. He provides his email address, john@mail-domain.com, as his user name. After authentication, only John will be displayed on the Home page.

The following diagram illustrates this scenario:



Workflow:

1. User (through the browser) is requesting for a resource. The Access Gateway determines whether it is a protected resource and redirects the request to the Identity Server for authentication. The Identity Server authenticates with the LDAP servers and provides the assertion details to the Access Gateway. In turn, the Access Gateway verifies the assertion details.
2. The Home page in the resource is configured to display the user ID that has to be retrieved from the Identity Server.
3. The Identity Server determines whether the attributes can be retrieved from the external source. The Identity Server will send the required details to the external source (in this example, an email address).
4. The external source returns the data. In this example, user ID part of the email address.
5. The Identity Server sends the data that it has obtained from the external source to the Access Gateway.
6. The Access Gateway sends the data to the Web server.
7. The Web server returns the resource.

5.6 Step up Authentication Example

This section discusses a Step up Authentication example for the Identity Server initiated SSO.

For more information about Identity Server initiated SSO, see "Using the Intersite Transfer Service" in the *NetIQ Access Manager 3.2 Identity Server Guide*.

Setup: Let us assume that:

- NetIQ Access Manager is acting as the identity provider.
- The following three contracts in the identity provider are configured:
  - name password basic contract with Authentication level as 10
  - name password form contract with Authentication level as 20
  - secure name password contract with Authentication level as 30

  NOTE: Enable the Satisfiable by a contract of equal or higher level option for contracts with authentication level 10 or 20 to avoid prompting for authentication when a user is already authenticated against the contract with level 30.
- The name password form contract for a service provider named SP_A is configured in the identity provider.

  For more information about creating and configuring the contracts, see "Configuring Authentication Contracts"in the *NetIQ Access Manager 3.2 Identity Server Guide*.

Configuration: Complete the following steps:

1. In the NetIQ Identity Server, configure the service provider as a trusted provider.

   For more information, see "Managing Trusted Providers"in the *NetIQ Access Manager 3.2 Identity Server Guide*.
2. In the service provider, configure the NetIQ Identity Server as a trusted provider.

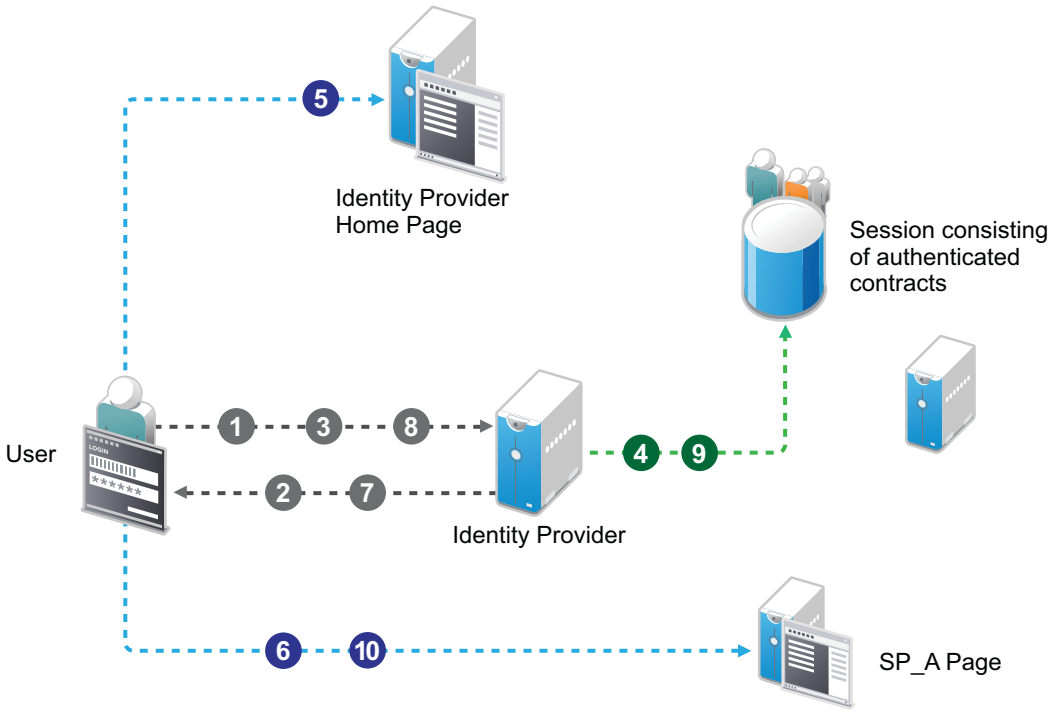
   For more information, see "Managing Trusted Providers"in the *NetIQ Access Manager 3.2 Identity Server Guide*.
3. In the NetIQ Identity Server, configure the service provider with the required authentication contracts.

For information about how to configure a service provider, see "Defining Options for Liberty or SAML 2.0 Service Provider", "To Define Options for Liberty Service Provider "and"Defining Options for SAML 1.1 Service Provider"in the *NetIQ Access Manager 3.2 Identity Server Guide*.

Results: The following are the four possible scenarios:

- If the user was authenticated with the name password basic contract before making an Intersite Transfer Service request to SP_A, the identity provider will step up to the name password form authentication.
- If the user was authenticated with the name password form contract before making an Intersite Transfer Service request to SP_A, the identity provider will not ask for the authentication.
- If the user was authenticated with the secure name password contract before making an Intersite Transfer Service request to SP_A, the identity provider will not ask for the authentication.
- If the user is not authenticated while making an Intersite Transfer Service request to SP_A, the identity provider will step up to the name password form authentication.

The following diagram illustrates the workflow:



Workflow:

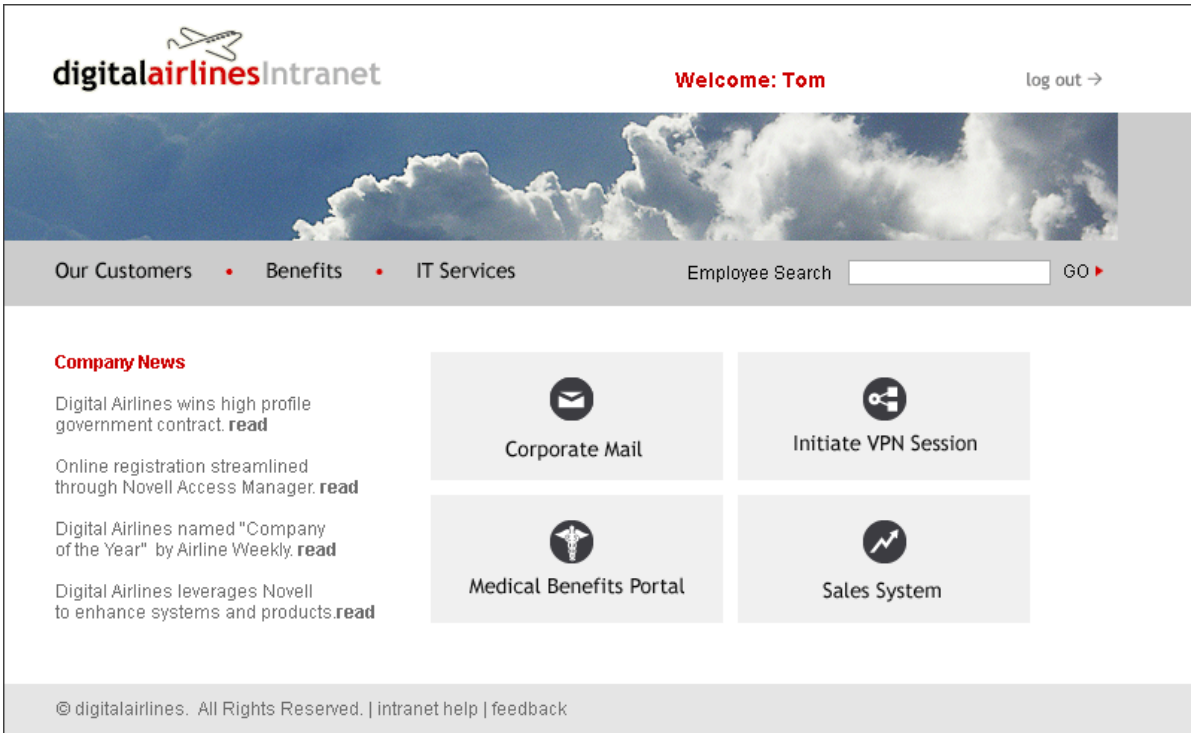
1. User tries to authenticate in the identity provider.
2. User is prompted to authentication using the Name Password Basic contract.
3. User enters the credentials.
4. The Name Password Basic contract is authenticated in the identity provider and added to the user session.

   The Name Password Basic contract is the default contract in the identity provider.
5. User logs into the identity provider.
6. User makes an Intersite Transfer Service request to SP_A.
7. The identity provider prompts for the authentication using the Name Password Form contract.
8. User enters the credentials.
9. The Name Password Form contract is authenticated in the identity provider and added to the user session.
10. User is redirected to SP_A.

6 Digital Airlines Example

This section explains how to use Access Manager to protect the Web site illustrated in Figure 6-1.

Figure 6-1 *Digital Airlines Web Services*



This section explains how to configure the Access Manager components to allow access to 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 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.

6.1 Installation Overview and Prerequisites

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

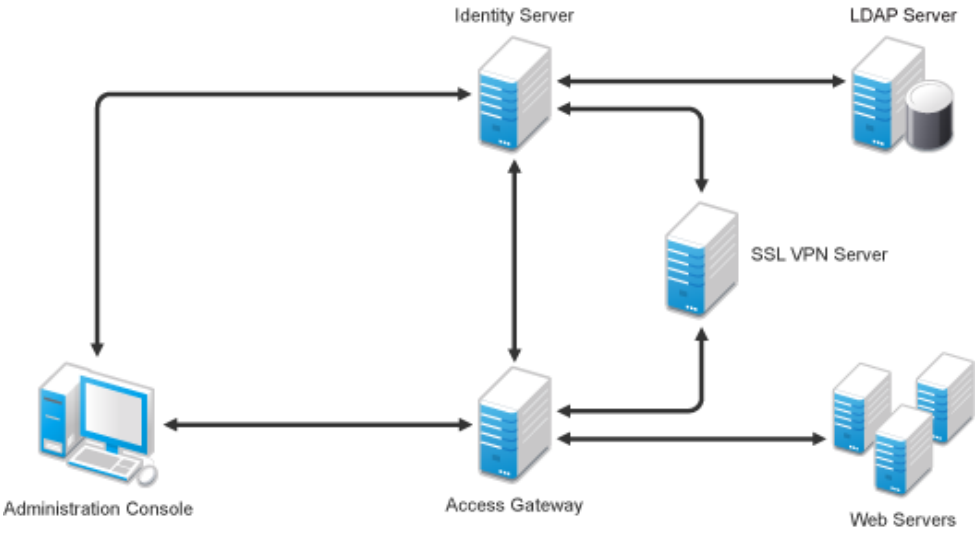
- Section 6.1.1, “Installation Architecture,” on page 112
- Section 6.1.2, “Deployment Overview,” on page 113

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.

6.1.1 Installation Architecture

The diagram below illustrates how the Digital Airlines example is integrated with Access Manager.

Figure 6-2 *Digital Airlines Architecture*



This document explains how to use a browser machine and two other machines for this configuration. The SSL VPN server can be installed either in a traditional mode or with an Embedded Service Provider (ESP). For this sample configuration, you need to install the Traditional SSL VPN server with Access Manager. If you select to use the ESP-enabled SSL VPN server, you need to install it with the Identity Server. For this sample configuration, select to install only one version of the SSL VPN server, not both.

Table 6-1 *NetIQ 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	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. In a production environment, you would not want to install the Administration Console, the ESP-enabled SSL VPN server, the Identity Server, and the Web server on the same machine. 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 *NetIQ Access Manager 3.2 SP1 Installation Guide*.

6.1.2 Deployment Overview

Prerequisite Tasks

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

- ❒ Enable pop-ups on a Firefox browser (3.x or above) or Internet Explorer browser (7.x or above) for managing and configuring the Access Manager components.
- ❒ Install the NetIQ Access Manager Administration Console, Identity Server, Access Gateway, and SSL VPN as described in the *NetIQ Access Manager 3.2 SP1 Installation Guide*.
- ❒ Configure the NetIQ Access Manager Identity Server. For configuration details, see Section 1.3, "Creating a Basic Identity Server Configuration," on page 11.

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 or the SSL VPN server at this time. Other tasks explain how to configure the Access Gateway and the SSL VPN server 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 6.2, "Setting Up the Web Server," on page 114.
2. Configure the Access Gateway to protect the Web server, but allow public access to the site. See Section 6.3, "Configuring Public Access to Digital Airlines," on page 116.

3. Configure the Access Gateway to allow access to the protected pages. See Section 6.4, “Implementing Access Restrictions,” on page 120.
4. Configure the SSL VPN server to allow access to the page on the Web server that is designed to be protected by the SSL VPN server. See Section 6.4.5, “Initiating an SSL VPN Session,” on page 138.

6.2 Setting Up the Web Server

6.2.1 Installing the Apache Web Server and PHP Components

The following instructions are for SLES 11 SP1 (or a higher version).

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

1a On your SLES 11 SP1 (or a higher version) server, click the *YaST* 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 multiprocessing module.

apache2-worker: Specifies the Apache 2 worker multiprocessing module.

1e Click *Accept*.

1f Verify that the php5 package is also selected for install, then click *Continue* to install that package as well as the other dependent packages.

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*.

2c Reboot the server or manually start the Apache server.

6.2.2 Installing Digital Airlines Components

The Digital Airlines example package contains the following 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 a subdirectory that can be configured to require basic authentication.
- **images:** Contains all image files associated with the example.

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.netiq.com/documentation/novellaccessmanager32/index.html) section in the NetIQ Documentation site.
2. Extract `htdocs.tar.gz` to a root directory of the Web server. For an Apache 2 Web server on SLES 11 SP1 (or a higher version), 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 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 118), 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 6.2.3, “Configuring Name Resolution,” on page 115.

6.2.3 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.

Each platform has its own location for the host file.

Platform	Location
Windows	`\WINDOWS\SYSTEM32\DRIVERS\ETC\HOSTS`
Linux	`/etc/hosts`

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.

- **Access Gateway Appliance:** Do not manually edit the `hosts` file on the Access Gateway Appliance. The file is overwritten every time the configuration is updated with the entries specifies on the Hosts page. To add an entry to the Hosts page, click *Devices* > *Access Gateways* > *Edit* > *Hosts,* then click *New*. The entries on this page are written to the *hosts* file when the configuration is updated.
- **Access Gateway Service:** You can edit the `hosts` file on the Access Gateway Service. Add an entry that allows the Access Gateway Service to resolve the name of the Identity Server.

Continue with Section 6.3, "Configuring Public Access to Digital Airlines," on page 116.

6.3 Configuring Public Access to Digital Airlines

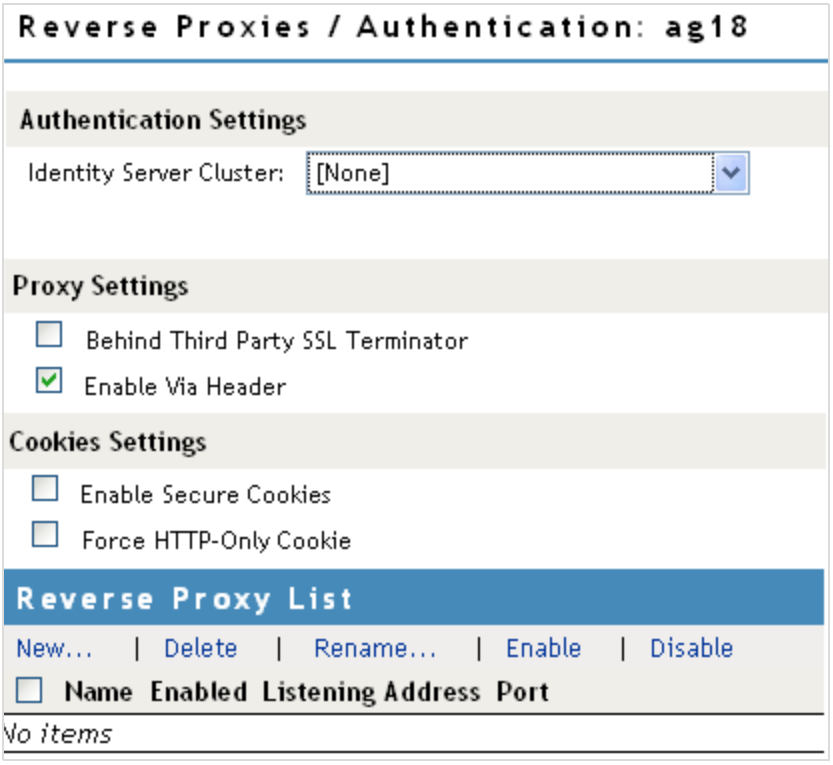
This section describes the procedures for configuring the Access Gateway so that a client can access the Digital Airlines site. Before continuing, make sure you have completed the prerequisite tasks described in "Prerequisite Tasks" on page 113 and Section 6.2, "Setting Up the Web Server," on page 114.

1. On the client machine, open a browser and log in to the Administration Console.
2. In the Administration Console, click *Devices* > *Access Gateways*.

   The IP address or name 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.

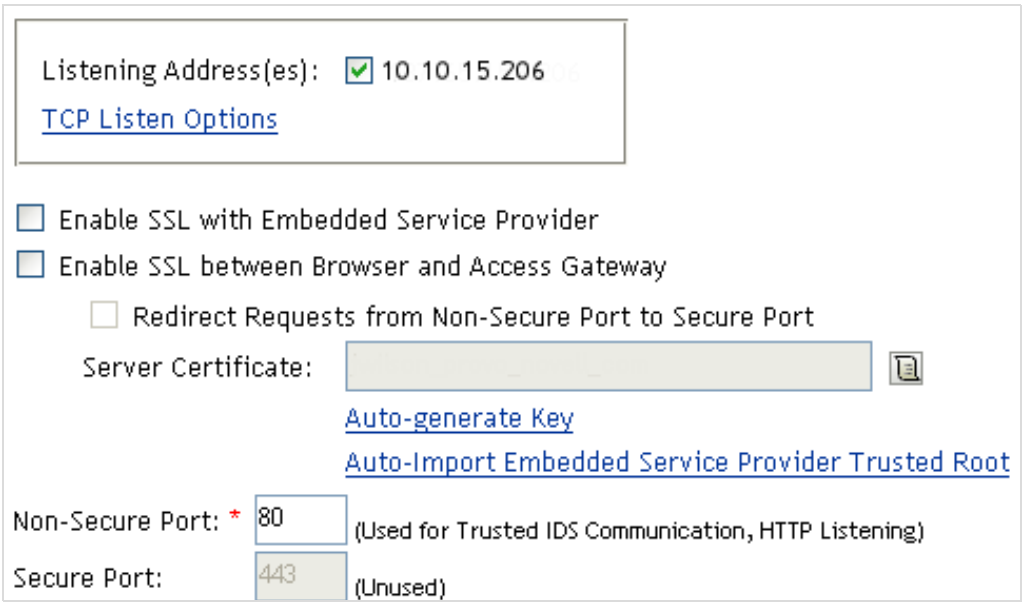
3 Click *Edit* > *Reverse Proxy / Authentication*.



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 configuration scenario does not contain SSL configuration instructions.

8 In the *Proxy Service List*, click *New* and specify the following information:

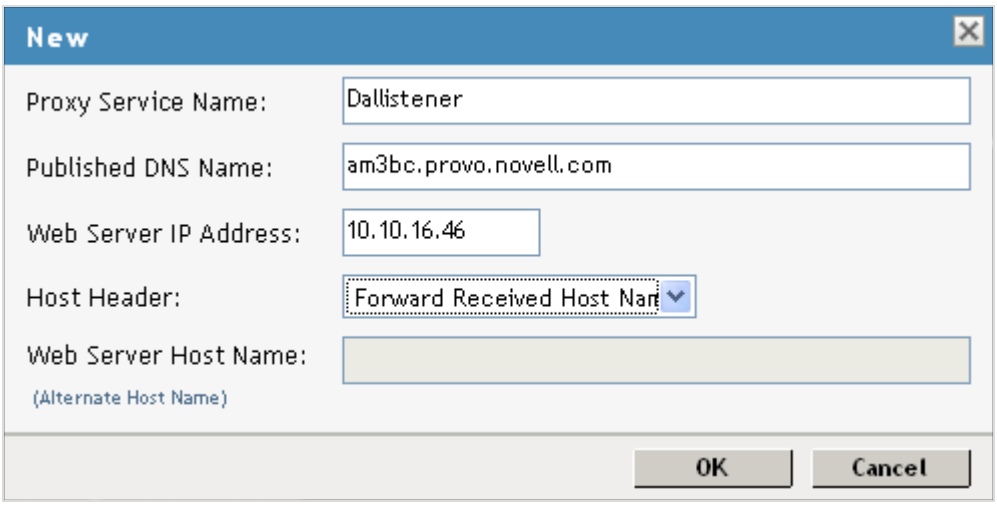
Proxy Service Name: Specify any name that intuitively identifies this service on your Access Gateway server. For this example, specify *Dallistener*.

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.

Your form should look similar to the following:

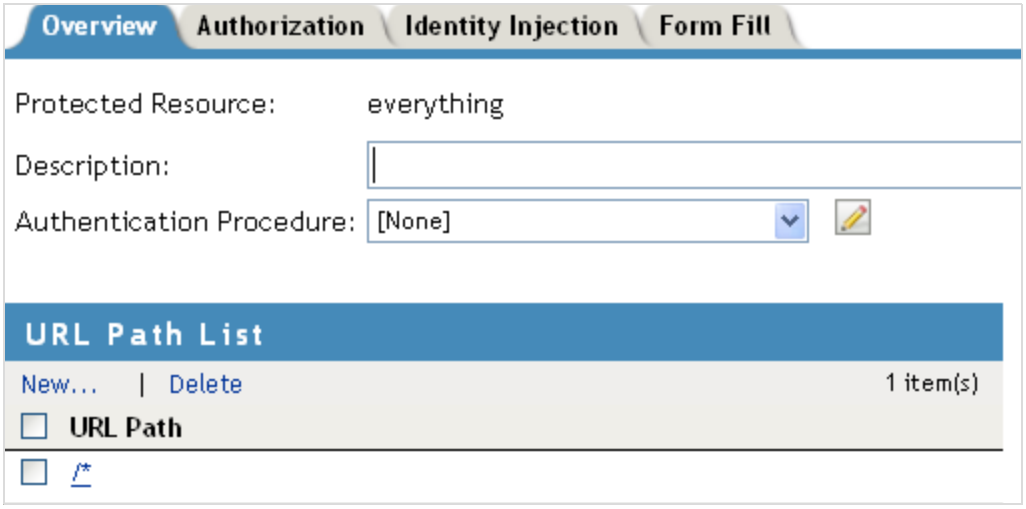


9 Click *OK*.

10 In the *Proxy Service List*, click *Dallistener*.

11 Click *Protected Resources*, then in the *Protected Resource List*, click *New*.

12 Type `everything` in *Name*, then click *OK*.



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

16 Click the *Devices* > *Access Gateways*.

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 *Devices* > *Identity Servers*, then click *Update* > *OK*.

19 To test the results, complete the following.

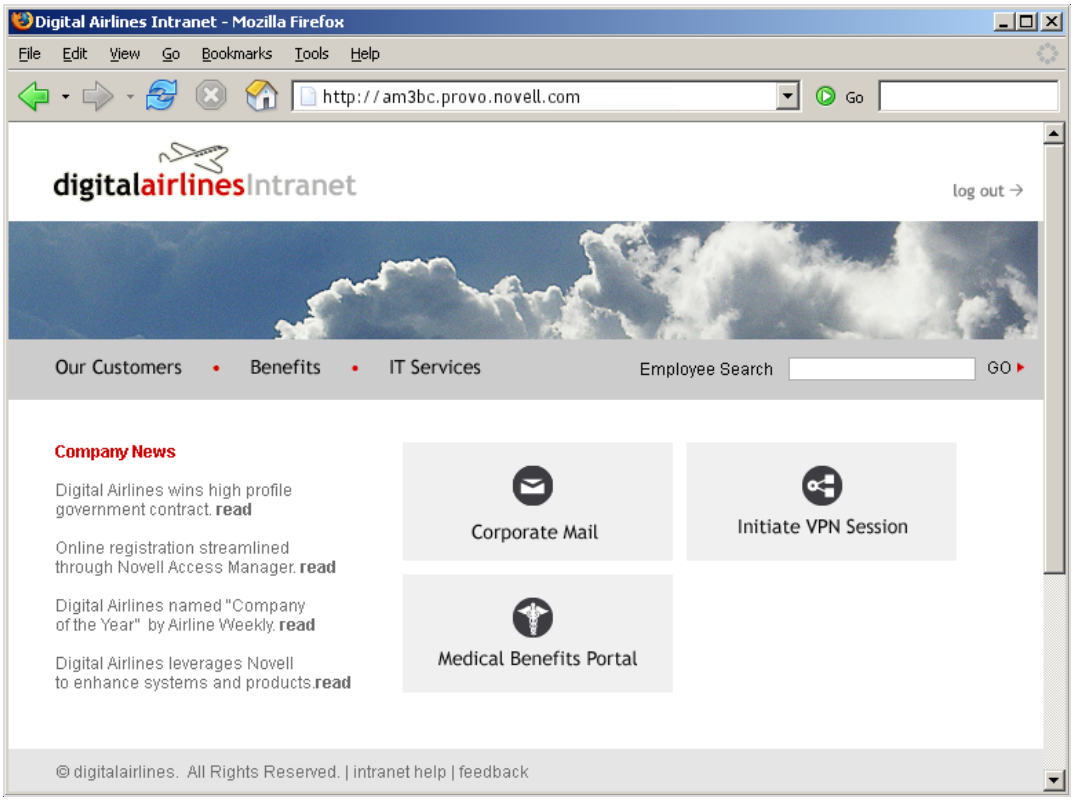
19a Open a browser on the client machine.

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. Their time should be synchronized and 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 6.4, "Implementing Access Restrictions," on page 120.

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.

6.4 Implementing Access Restrictions

After you access the Digital Airlines site as a public resource (see Section 6.3, "Configuring Public Access to Digital Airlines," on page 116), you can configure the site for authentication and authorization requirements. This section describes the following tasks:

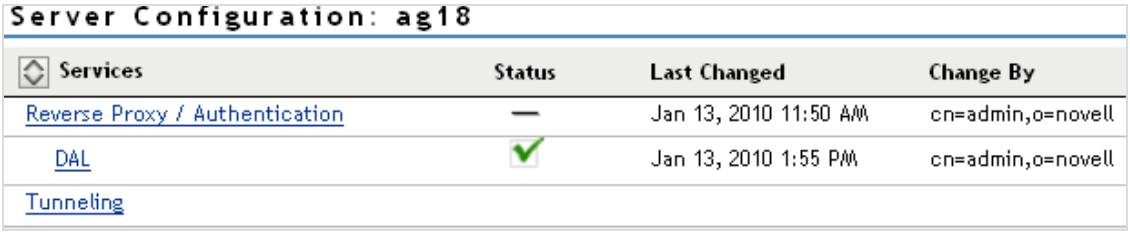
- Section 6.4.1, "Enabling an Authentication Procedure," on page 121
- Section 6.4.2, "Configuring a Role-Based Policy," on page 123
- Section 6.4.3, "Assigning an Authorization Policy to Protect a Resource," on page 131

- Section 6.4.4, “Configuring an Identity Injection Policy for Basic Authentication,” on page 134
- Section 6.4.5, “Initiating an SSL VPN Session,” on page 138

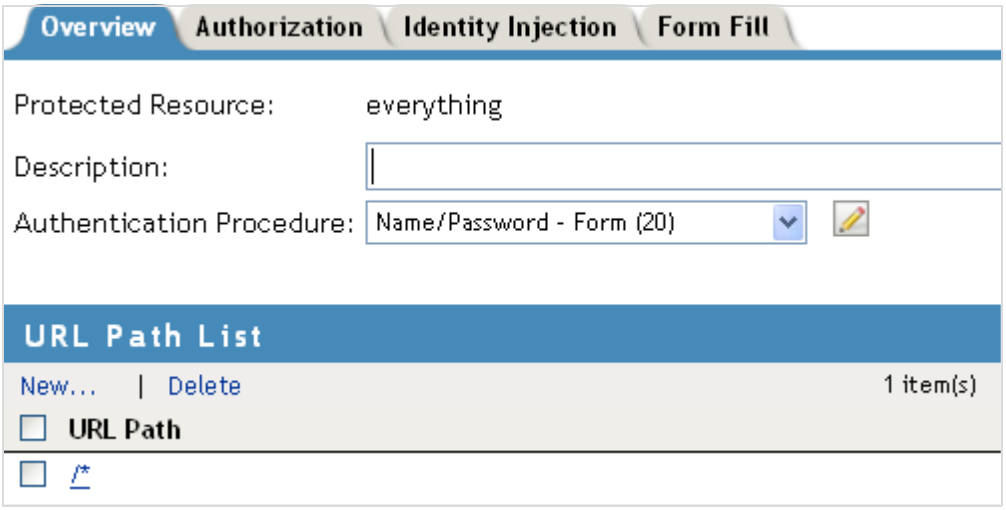
6.4.1 Enabling an Authentication Procedure

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 *Devices* > *Access Gateways* > *Edit*.



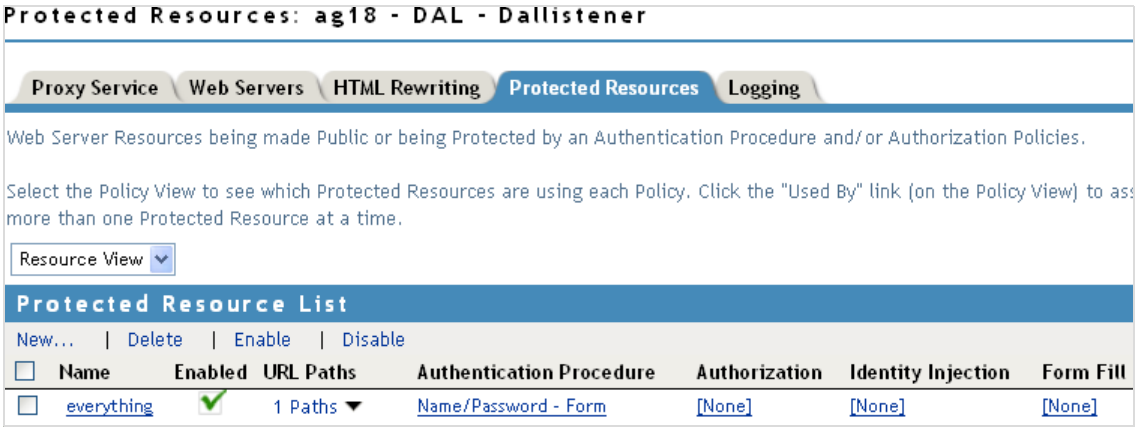
2 Click *DAL* > *Dallistener* > *Protected Resources* > *everything*.



3 In the *Authentication Procedure* 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 *Devices* > *Access Gateways*, 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.

7 Enter the credentials of the admin user of your Administration Console.

The Digital Airlines site appears. If you receive an error, see "Common Authentication Problems" on page 122.

8 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 20 minutes), or you close all sessions of the browser.

9 Continue with Section 6.4.2, "Configuring a Role-Based Policy," on page 123.

Common Authentication Problems

In this basic configuration there are two common configuration errors that can cause login to fail:

Error 300101015: If your Access Gateway and Identity Server do not have the same time, the assertion is invalid. Check the time of each machine.

Errors 100101043 and 100101044: The Identity Server and the Access Gateway need to be able to resolve each other's DNS names. If you are in a lab and not using a DNS server, make sure the host files of each machine have been configured to resolve the DNS name to the IP address of the device.

The other cause for these errors, when SSL has not been enabled, is the failure to update either the Identity Server or the Access Gateway after making a change to the base URL of the Identity Server or modifying the Identity Server the Access Gateway is trusting for authentication. For information on how to force the Access Gateway to update the metadata for the Identity Server, see "Embedded Service Provider Metadata" in the *NetIQ Access Manager 3.2 Identity Server Guide*.

6.4.2 Configuring a Role-Based Policy

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.

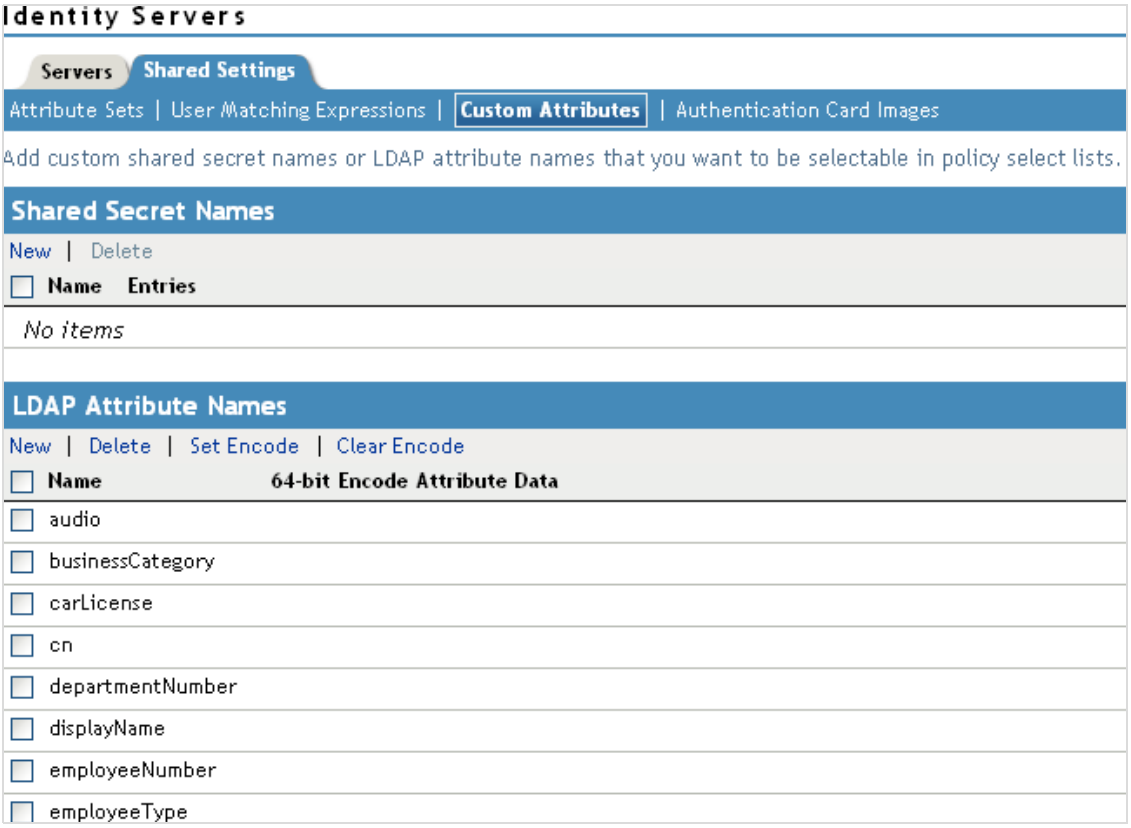
To configure an Identity Injection policy that uses a role, complete the following tasks:

- "Adding an LDAP Attribute to Your Configuration" on page 124
- "Creating a Sales Role" on page 125
- "Creating a New User with a Sales Role" on page 127
- "Creating the Identity Injection Policy for a Custom Header" on page 128

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 *Devices* > *Identity Servers*, then click *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.

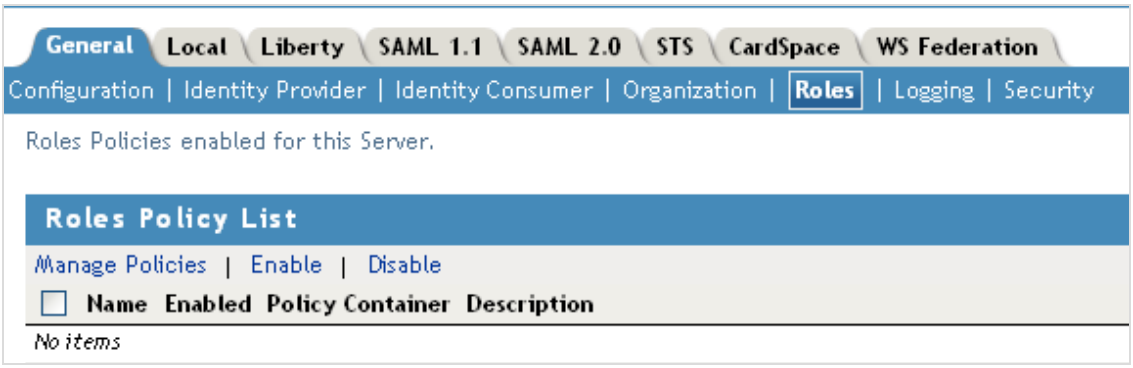
3 Click *Close*.

4 Continue with "Creating a Sales Role" on page 125.

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 *NetIQ Access Manager 3.2 Policy Guide*.)

1 In the Administration Console, click *Devices* > *Identity Servers*, then click *Edit* > *Roles*.



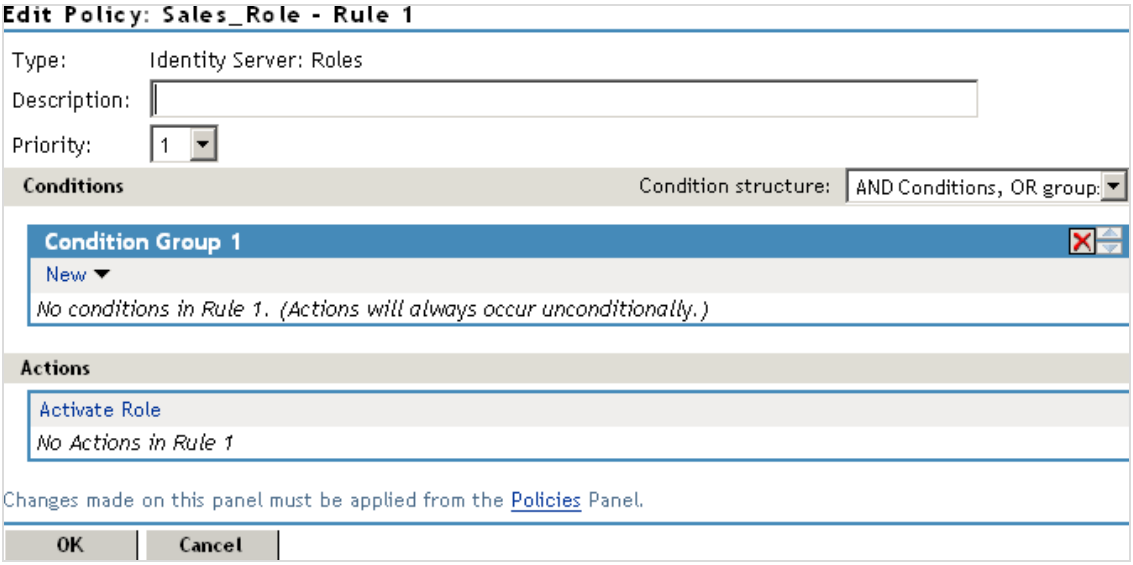
2 In the *Roles Policy List* section, click *Manage Policies*.

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*.

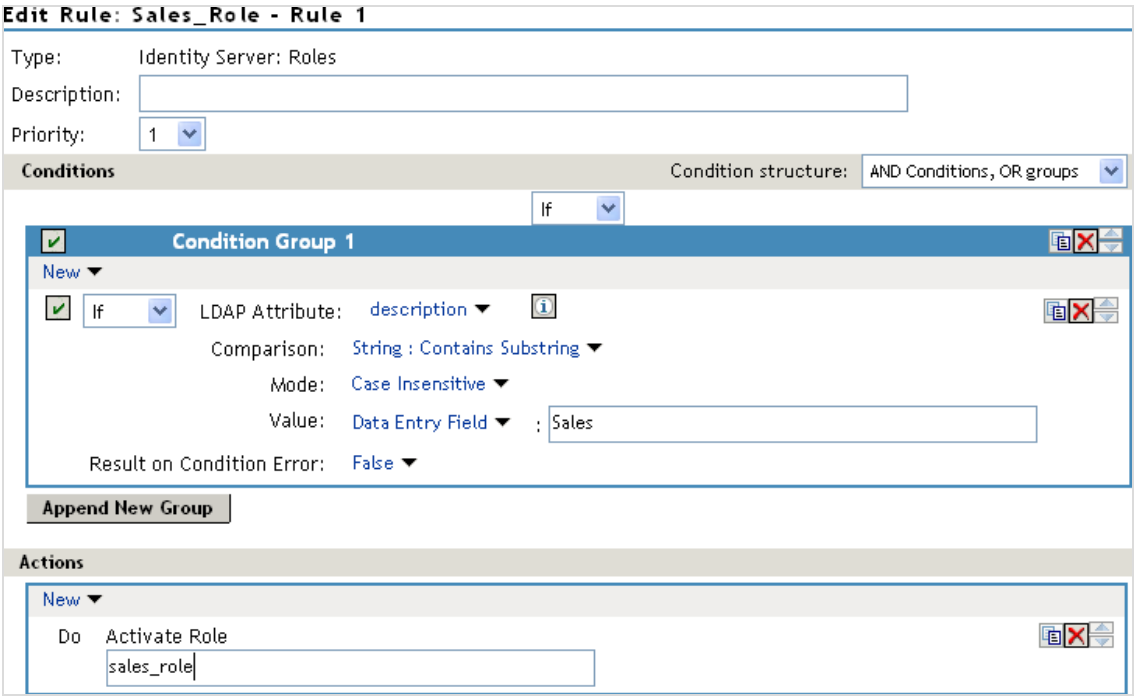
If the *description* attribute is not listed in the *LDAP Attribute* drop-down menu, create it by following this procedure:

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* section, click *New* > *Activate Role*, then specify *sales_role* in the *Do Activate Role* field. Your rule should look similar to the following:

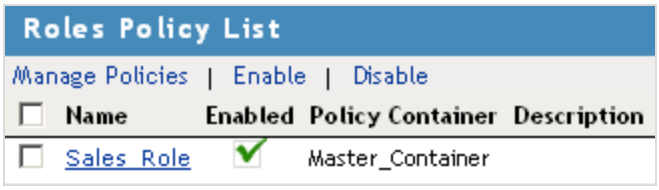


The value for *Activate Role* might be case sensitive. If you are going to inject this role into a policy for a Web server, and the page on the Web server is configured so that it evaluates case, make sure the value entered here matches what is expected on the Web server. The *Sales System* button on 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 Update the Identity Server.

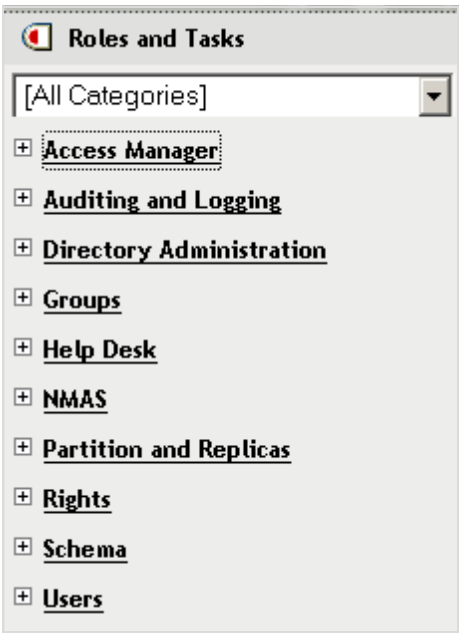
Wait for the *Status* to return to *Current*.

12 Continue with "Creating a New User with a Sales Role" on page 127.

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 the *Roles and Task*  icon in the top menu bar.



2 Click *Users*.

3 Click *Create User,* then fill in the following fields:

Username: Specify *Tom.*

First name: Specify *Tom.*

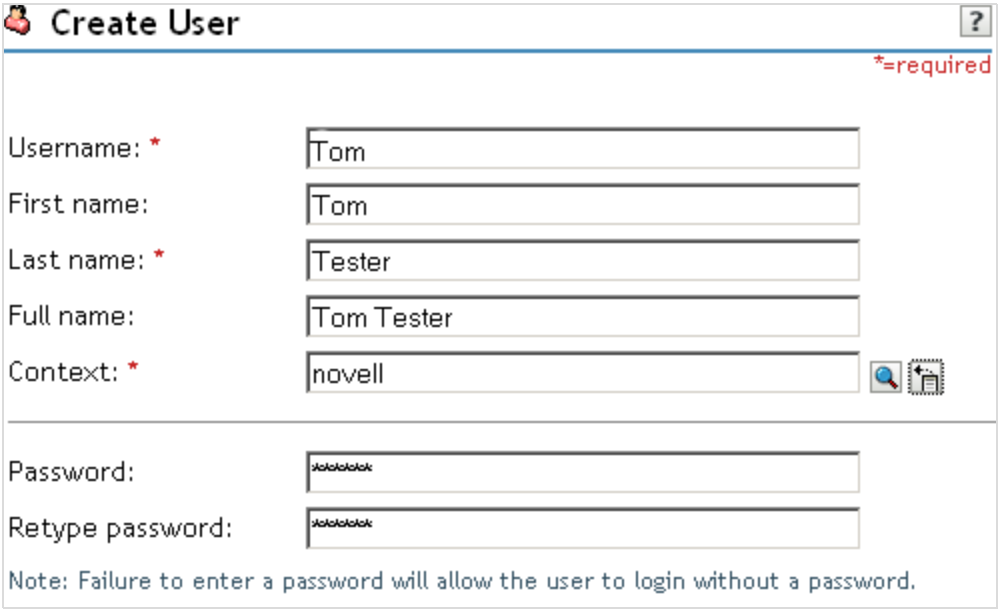
Last name: Specify *Tester.*

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:



4 Scroll to the *Description* field, then click the + icon.

5 In the *Add* text box, type `Sales` (initial uppercase), then click *OK* to return to the Create User page.

6 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.

7 Continue with "Creating the Identity Injection Policy for a Custom Header" on page 128.

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 the *Access Manager*  icon in the top menu bar.

2 Click *Devices* > *Access Gateways*, then click *Edit* > *DAL* > *Dallistener* > *Protected Resources* > *everything*.

3 Click *Identity Injection* > *Manage Policies*.

4 In the *Policy List* section, click *New*, then fill in the following:

Name: Specify *Custom_Injection*.

Type: Select *Access Gateway: Identity Injection*.

5 In the *Actions* section, click *New* > *Inject into Custom Header*.

6 To inject the user's name, fill in the following values:

Custom Header Name: Specify *X-Name*.

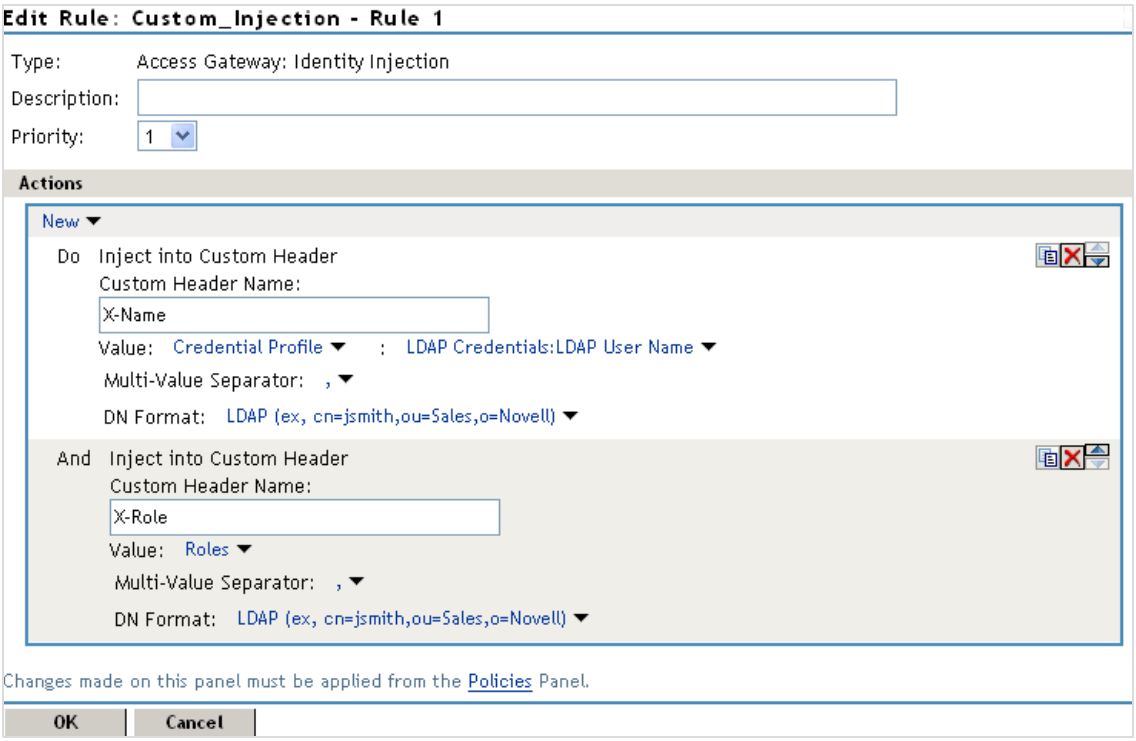
Value: Select *Credential Profile*. The *LDAP Credentials: LDAP User Name* is selected automatically for you.

7 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*.

Your policy should look similar to the following:



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

9 Click *Close*.

10 In the *Identity Injection Policy List* section, select *Custom_Injection*, then click *Enable*.

11 Click *OK*.

12 Click *Devices* > *Access Gateways*, then click *Update* > *OK*.

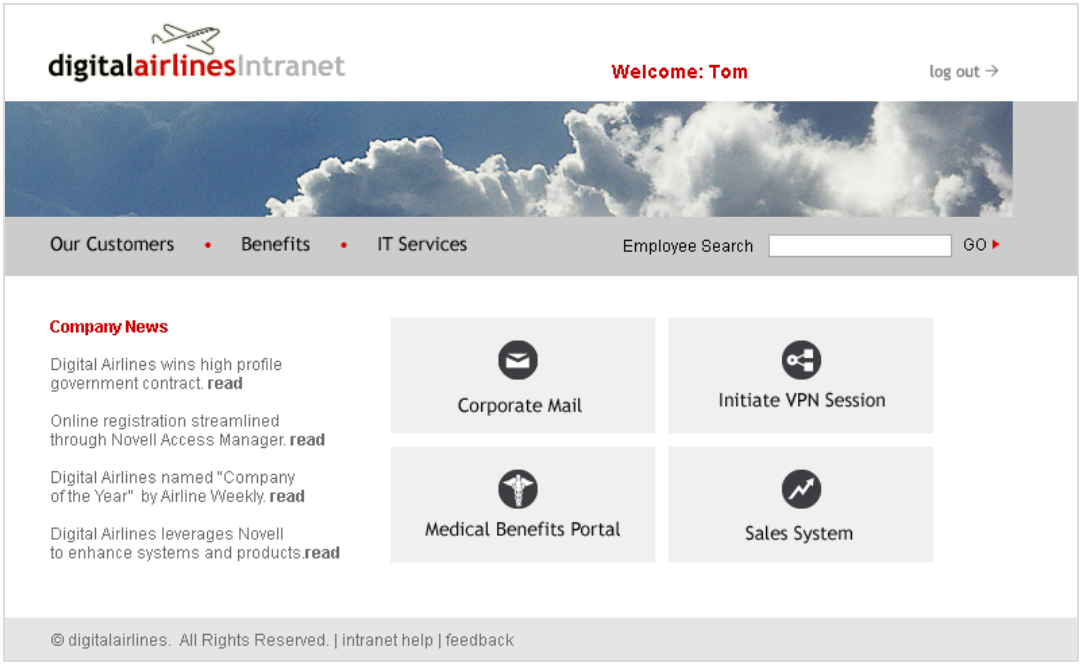
13 To test Tom's access rights, complete the following steps:

13a Open a new browser, then enter the URL of the Digital Airlines Web site you created.

In this example, it is *am3bc.provo.novell.com*.

13b 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 corner of the page.



13c Click the *Sales System* button, and the Sales page appears.

If the Sales System button does not appear, Tom was not assigned the sales_role:

- Verify that the role policy is enabled for the Identity Server by clicking *Policies* > *Policies*, and confirm that the Identity Server is listed in the *Used By* column for the policy.
- On the Policies page, confirm that the Access Gateway is listed in the *Used By* column for the Identity Injection policy.
- Discover whether there was an error in the Role policy evaluation. Click *Auditing* > *General Logging*, then download the `catalina.out` (Linux) or the `stdout.log` (Windows) file for the Identity Server. Search for the name of the role policy and determine whether the role was successfully assigned.
- Determine whether there was an error in Identity Injection policy evaluation. Click *Auditing* > *General Logging*, then download the `catalina.out` (Linux) or the `stdout.log` (Windows) file for the Access Gateway. Search for the name of the Identity Injection policy and determine whether its values were successfully injected.

For more information about troubleshooting policies, see "Troubleshooting Access Manager Policies" in the *NetIQ Access Manager 3.2 Policy Guide*.

13d Close all sessions of the browser.

14 To test that the sales_role is required for the *Sales System* button to appear, complete the following steps:

14a Open a new browser, then enter the URL of the Digital Airlines Web site you created.

In this example, it is *am3bc.provo.novell.com*.

14b 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.

14c To the URL, add `/sales`, and the Sales page appears.

This illustrates that although the link is hidden, the Sales page is not protected.

14d Close all sessions of the browser.

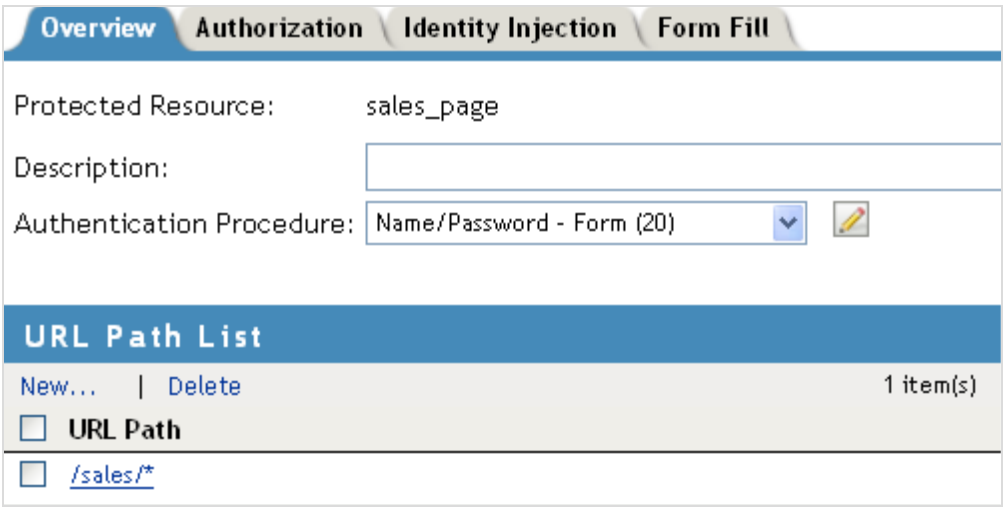
15 Continue with Section 6.4.3, "Assigning an Authorization Policy to Protect a Resource," on page 131.

6.4.3 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 *Devices* > *Access Gateways*, then click *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 *Authentication Procedure*, 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*, then specify the following values:

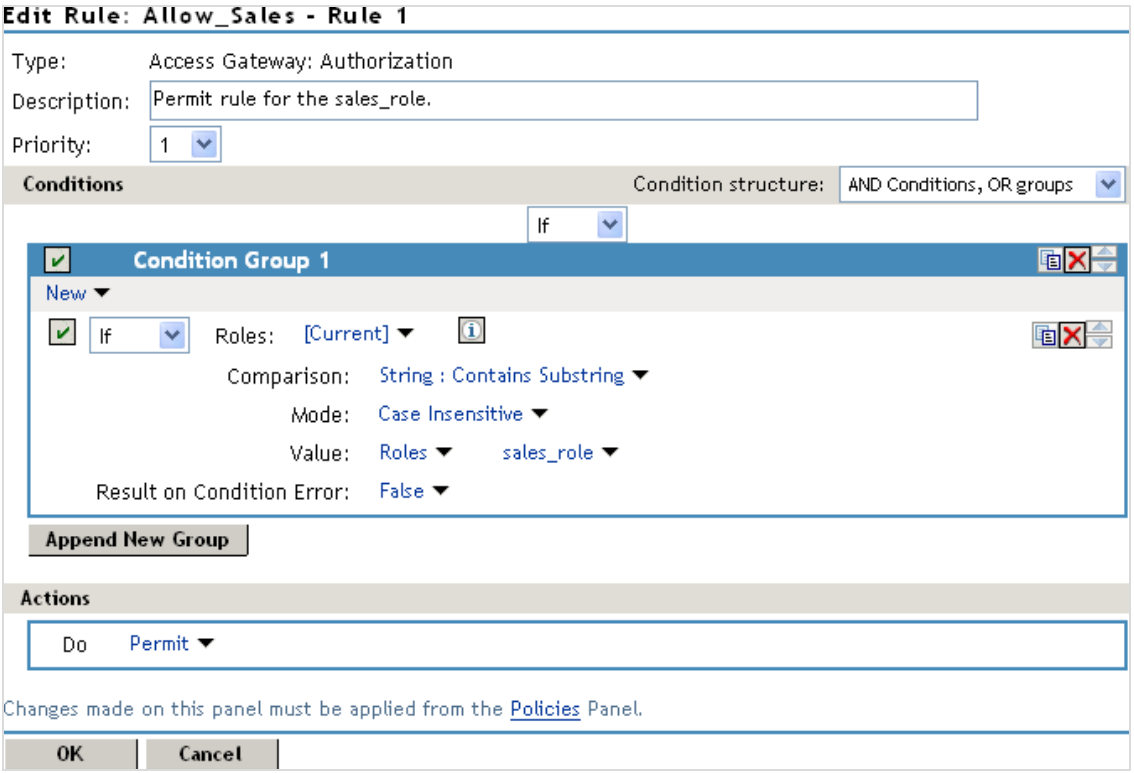
   Comparison: Select *String: Contains Substring*.

   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*.

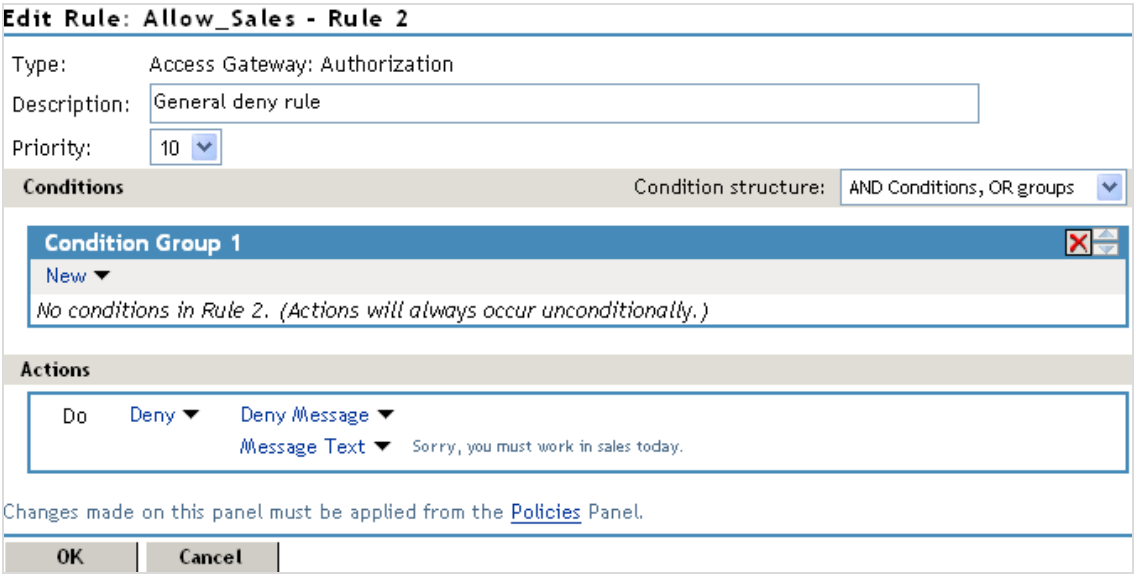
This second rule is a general deny rule for everyone who has not been assigned the sales_role.

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 Click *Message Text*, then 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:

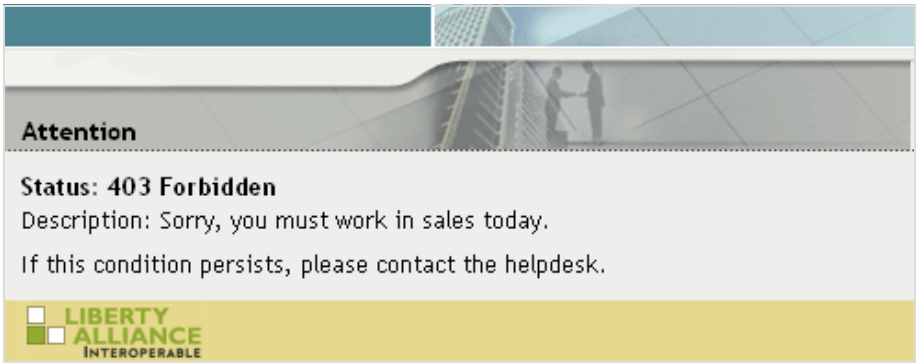
20a Open a new browser, then enter the URL of the Digital Airlines Web site you created.

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 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 6.4.4, "Configuring an Identity Injection Policy for Basic Authentication," on page 134.

6.4.4 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

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 of 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

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 Click *Search*, then configure the following fields.

Context: Accept the default [root] value and leave the *Search sub-containers* option enabled.

Name: Accept the default wildcard value.

Type: Select *LDAP Group* from the list.

4 In the *Results* section, click the `LDAP Group - <your server name>` object, 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 *Access Manager* 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. On SLES 11 SP1 (or a higher version), 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 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 136.

Creating an Identity Injection Policy for Basic Authentication

This section explains how to enable single sign-on 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 *Devices* > *Access Gateways*, then click *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:

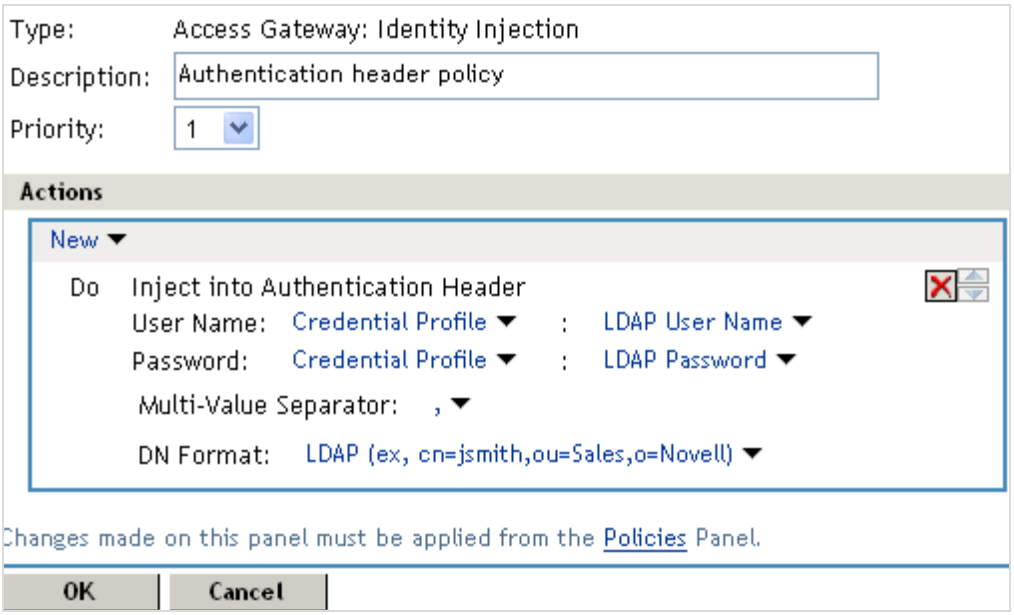
   Name: Specify *Basic_Auth* for the name.

   Type: Select *Access Gateway: Identity Injection* for the type.
5. Click *OK*.
6. In the *Actions* section, 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*.

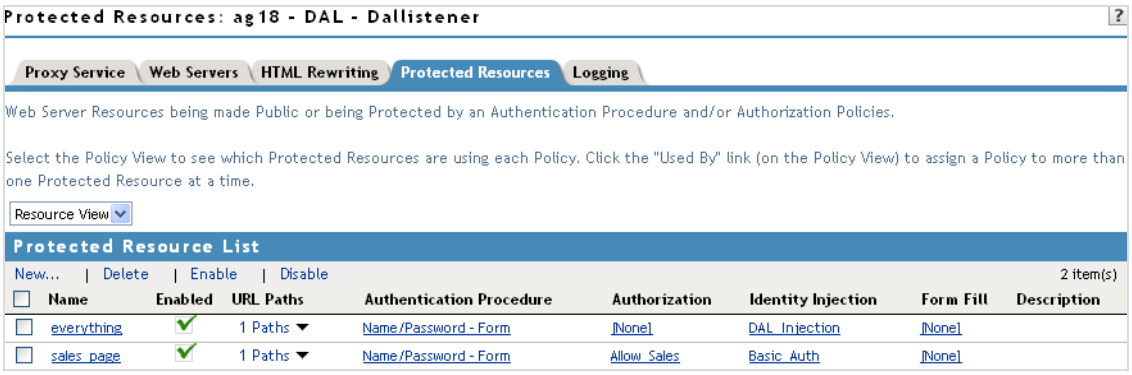
   Your policy should look similar to the following:



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 *Basic_Auth* 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*.

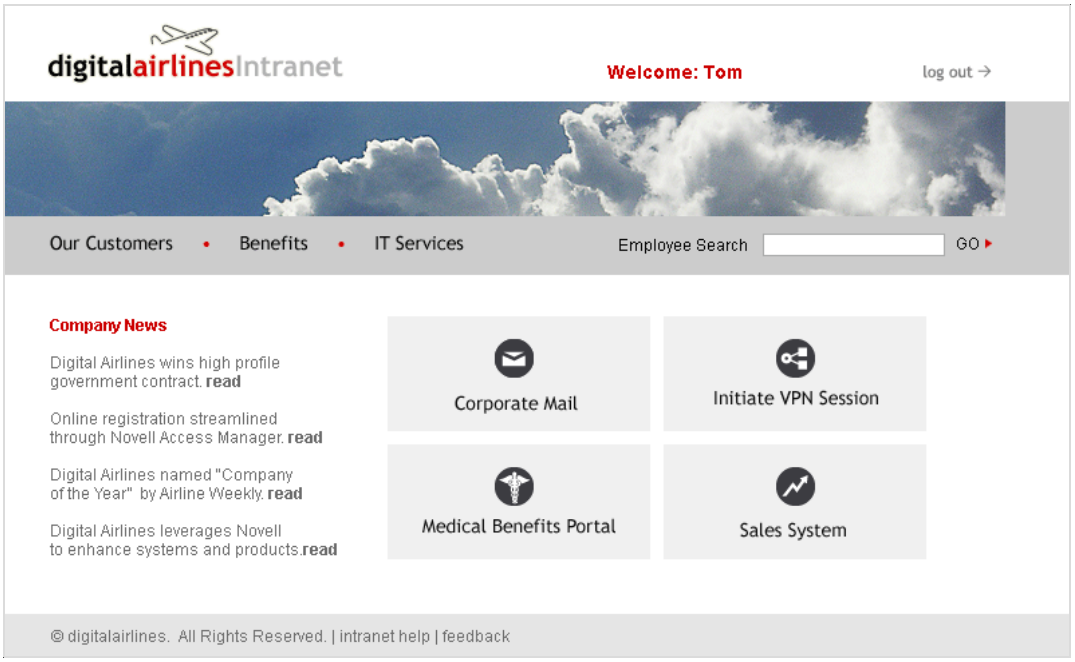
12 To test the configuration:

12a Open a new browser, then enter the URL of the Digital Airlines Web site you created.

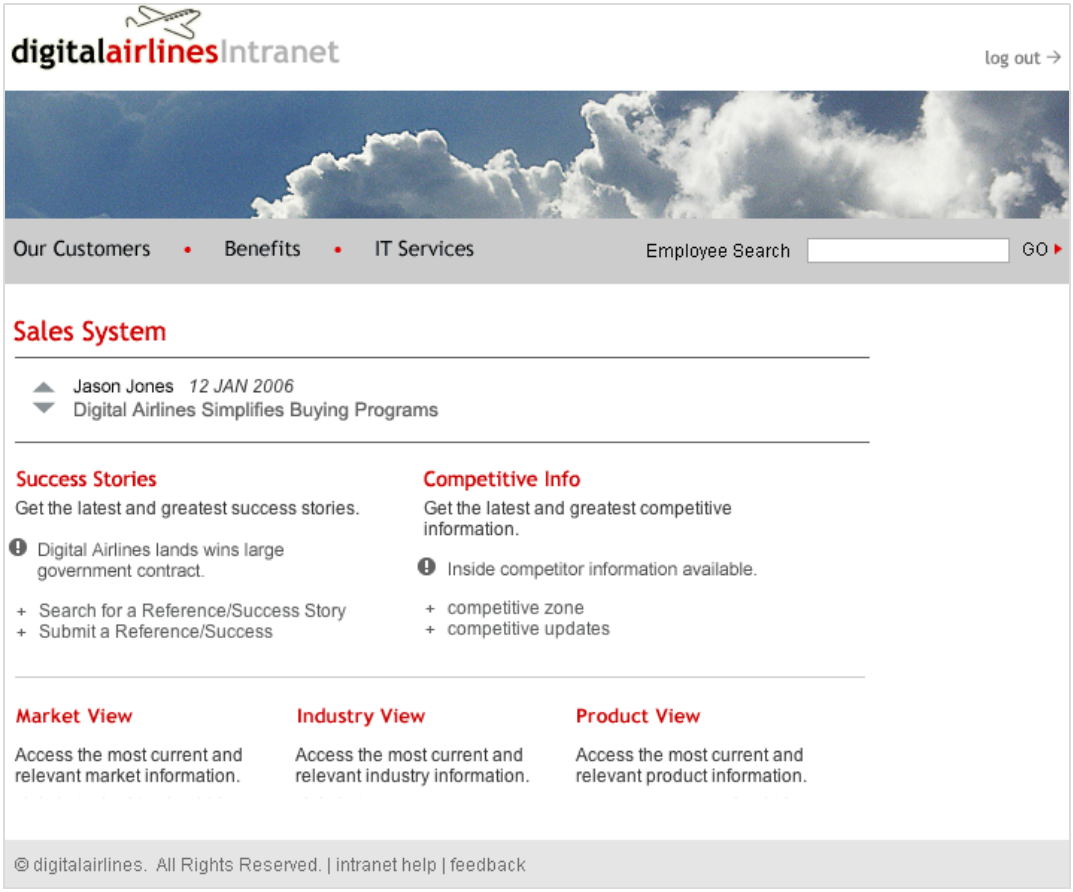
In this example, it is *am3bc.provo.novell.com*.

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 *NetIQ Access Manager 3.2 Policy Guide*.

12d Close all sessions of the browser.

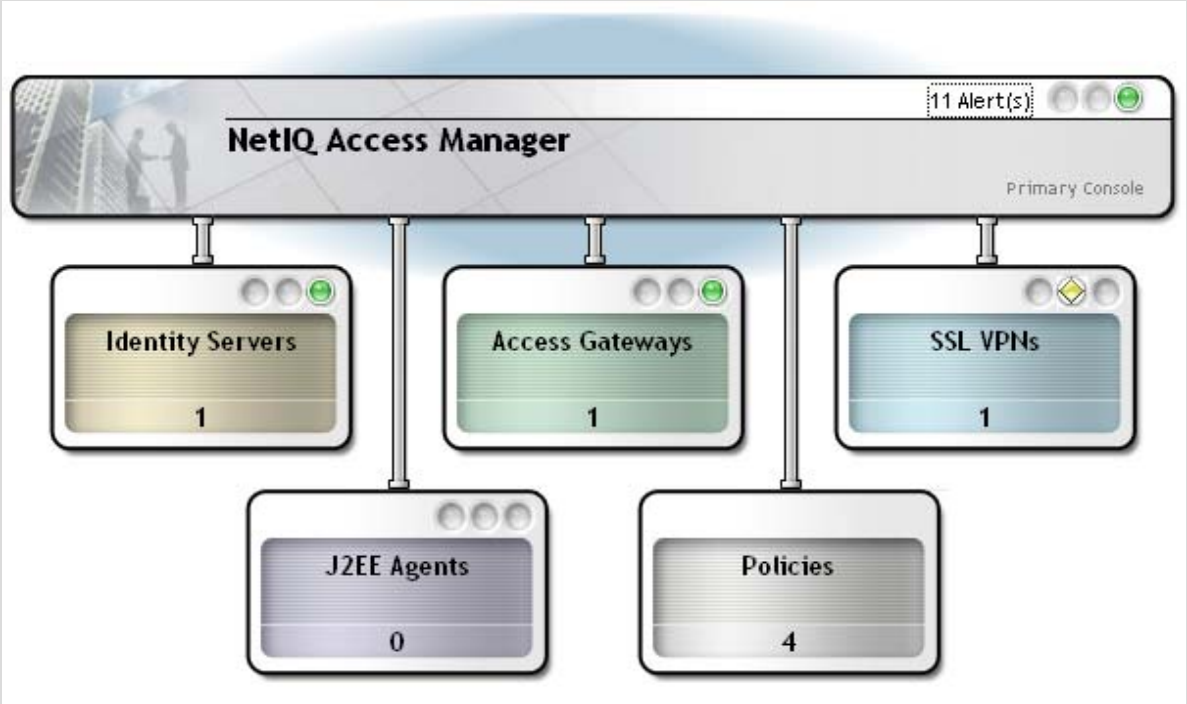
13 Continue with Section 6.4.5, "Initiating an SSL VPN Session," on page 138.

6.4.5 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.

Before performing this task, you must have the SSL VPN server installed. Your Access Manager console should appear similar to the green state shown in Figure 6-3:

Figure 6-3 *Dashboard Indicating the Status of Access Manager Components*



The yellow status of the SSL VPN indicates that it has not been configured. For more information about installing the SSL VPN server, see the *NetIQ Access Manager 3.2 SSL VPN Server Guide*.

For the Digital Airlines example, perform the following tasks:

- "Configuring the ESP-Enabled SSL VPN" on page 139
- "Configuring the Traditional SSL VPN Server" on page 140
- "Testing the SSL VPN Basic Configuration" on page 142
- "Configuring a Traffic Policy" on page 142

Configuring the ESP-Enabled SSL VPN

You can configure SSL VPN installed along with the Identity server for authentication as follows:

1. In the Administration Console, click *Devices* > *SSL VPNs*.
2. Click *Edit* to modify the configuration of the server.
3. In the *Basic Gateway Configuration* section, click *Authentication Configuration*.
4. Fill in the following fields:

   Identity Server Cluster: Select the configuration you have assigned to the Identity Server.

   This sets up the trust relationship between the SSL VPN server and the Identity Server that is used for authentication.

   Authentication Contract: Select the *Name/password - Form* option.

   Embedded Service Provider Base URL: This is the application path for the Embedded Service Provider. This needs to be DNS name of the machine with the port and the application path used by the SSL VPN server. For example, *http://nam.provo.novell.com:8080/sslvpn*, where `nam.provo.novell.com` is the DNS name of the machine.

5 Restart the Tomcat server when prompted.

6 To save your modifications, click *OK* twice, then click *Update* on the server page.

7 Click *Update* on the Identity Server page.

8 Configure a traffic policy. For more information see "Configuring a Traffic Policy" on page 142.

Configuring the Traditional SSL VPN Server

To configure the Traditional SSL VPN server to access the SSL VPN page on the Digital Airlines site, complete the following tasks:

- "Configuring the SSL VPN Server as a Protected Resource" on page 140
- "Creating a Protected Resource and an Identity Injection Policy for the SSL VPN Server" on page 141

Configuring the SSL VPN Server as a Protected Resource

To configure the SSL VPN as a protected resource, you must first create a reverse proxy for it.

1 In the Administration Console, click *Devices* > *Access Gateways*, then click *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 *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.)

Path: Specify */sslvpn*.

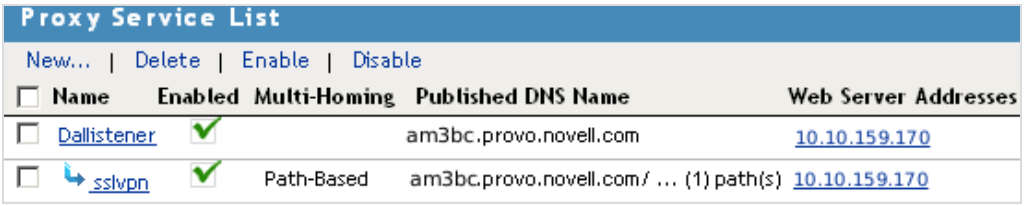
Web Server IP Address: Specify the IP address of SSL VPN server. If the traditional SSL VPN server is installed with the Access Gateway Appliance, enter the localhost IP address (127.0.0.1).

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 a Protected Resource and an Identity Injection Policy for the SSL VPN Server" on page 141.

Creating a Protected Resource and an Identity Injection Policy for the SSL VPN Server

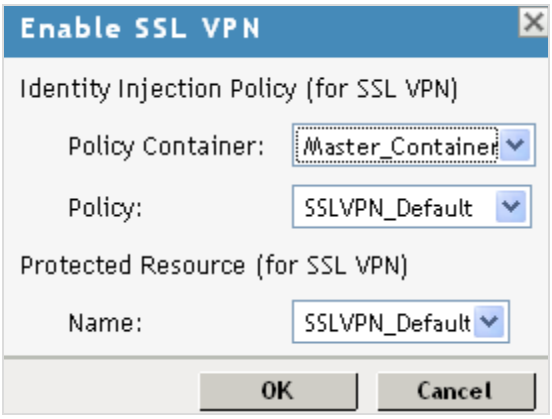
1. In the *Proxy Service List*, select the *sslvpn*.
2. In the *Path List*, select the *sslvpn* path, then click *Enable SSL VPN*.
3. Fill in the following fields:

   Policy Container: Select *Master_Container*.

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

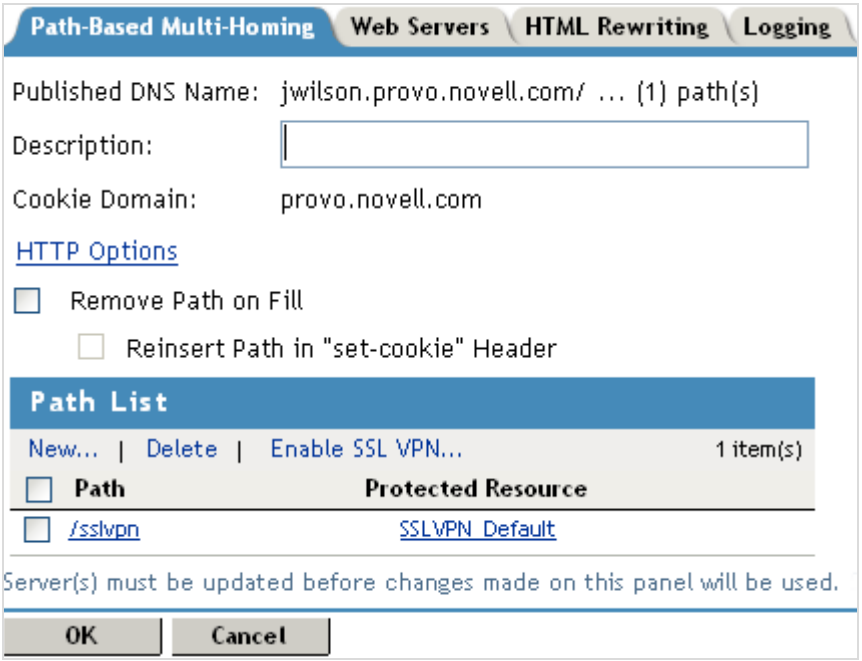
   Name: Select *Create SSL VPN Default Protected Resource*.

   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 *Devices* > *Access Gateways*, then click *Update* > *OK*.

7 Click *Devices* > *SSL VPNs*, 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 service, open a new browser and enter the URL for the Digital Airlines site. For this example, it is the following:

```
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 127.

3 Click *Initiate VPN Session* on the Digital Airlines site.

4 (Optional) If you have logged in by using the Internet Explorer, you might be asked to install an ActiveX control.

5 When the SSL VPN client downloads, installs, and runs, the following page appears:

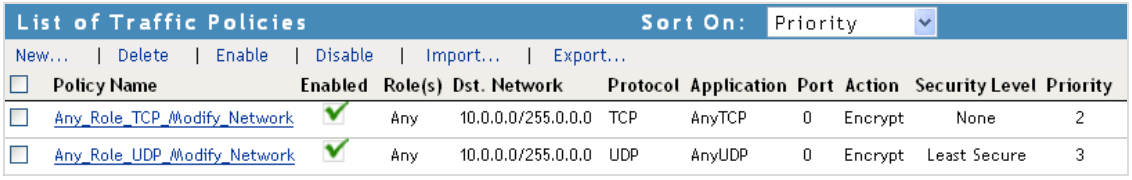
Notice that the user's first name ("Tom") is injected into the header of the SSL VPN browser.

6 Click the *Logout* icon, 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 server. Simulate this by creating a rule that allows access to your network:

1 In the Administration Console, click *Devices* > *SSL VPNs*, then click *Edit* > *Traffic Policies*.



2 Click *New*, type *sales*, then click *OK*.

3 Click the new, enabled sales policy, then provide the following values:

Role: *sales_role*. Select the role from the *Available Roles* list and move it to the *Assigned Roles* list.

Destination Network: This field is usually prepopulated (10.0.0.0), or you can specify the IP address of the SSL network. The network mask (255.0.0.0) is also 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.

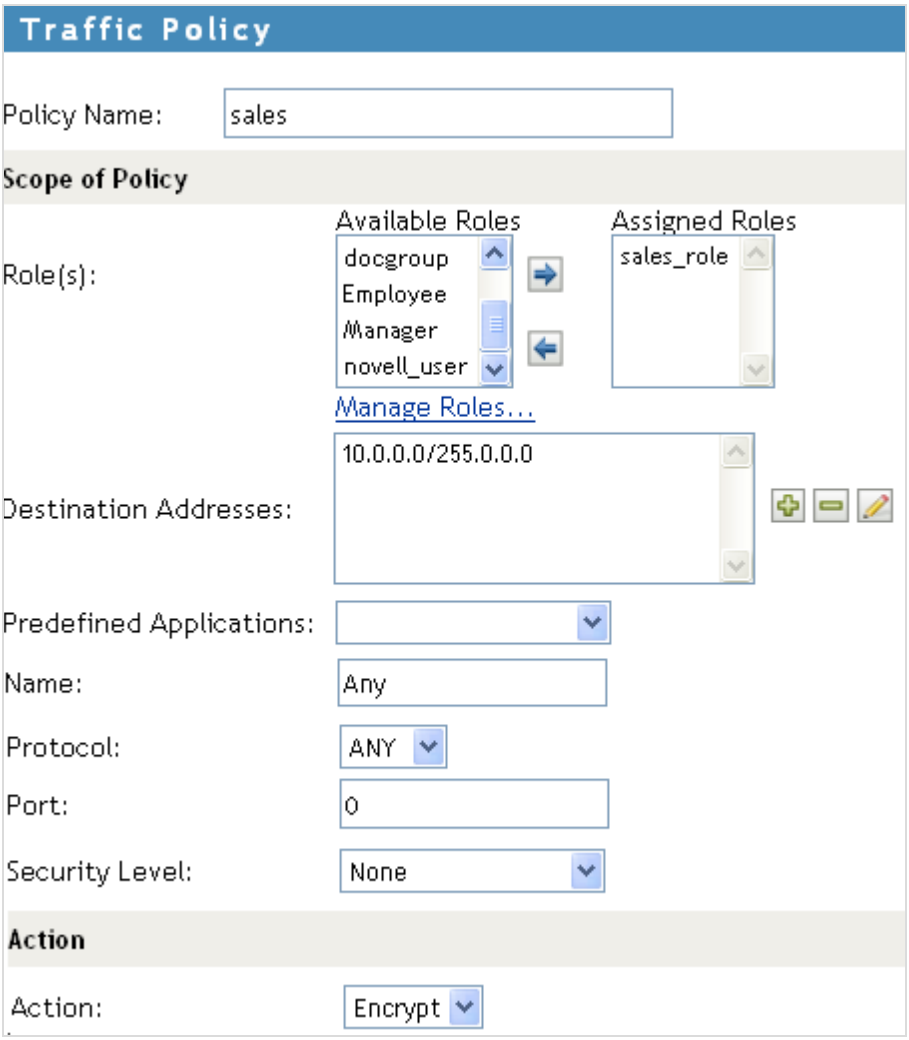
Protocol: *Any*. Specifies whether the protocol is *ICMP*, *UDP*, *TCP*, or *Any*.

Port: *Port*. Specifies the port number on which the service you select listens. The value of 0 allows all ports.

Security Level: *None*. Specifies the minimum level of security for the client machine in order to apply this traffic policy.

Action: *Encrypt*. Specifies whether the service can be encrypted or denied.

Your rule should look similar to the following rule:



4 Click *OK* to save the configuration and return to the List of Traffic Policies page.

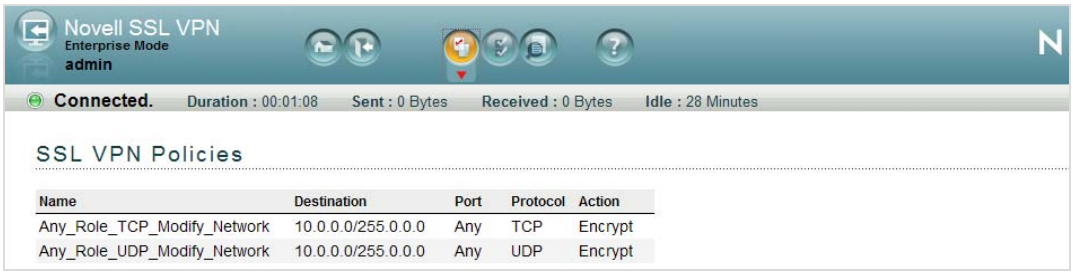
5 Click *OK* twice, then on the SSL VPNs page, click *Update*.

6 Test the traffic rule:

6a Open a new browser session and enter *http://am3bc.provo.novell.com/sslvpn/login*.

6b Log in as the *admin* user of the Administration Console.

6c 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 127.

6d Log out of the SSL VPN session.

6e Open a new SSL VPN browser session and enter *http://am3bc.provo.novell.com/sslvpn/login*.

6f Log in as Tom. (See "Creating a New User with a Sales Role" on page 127.)

6g Click *Policies*.

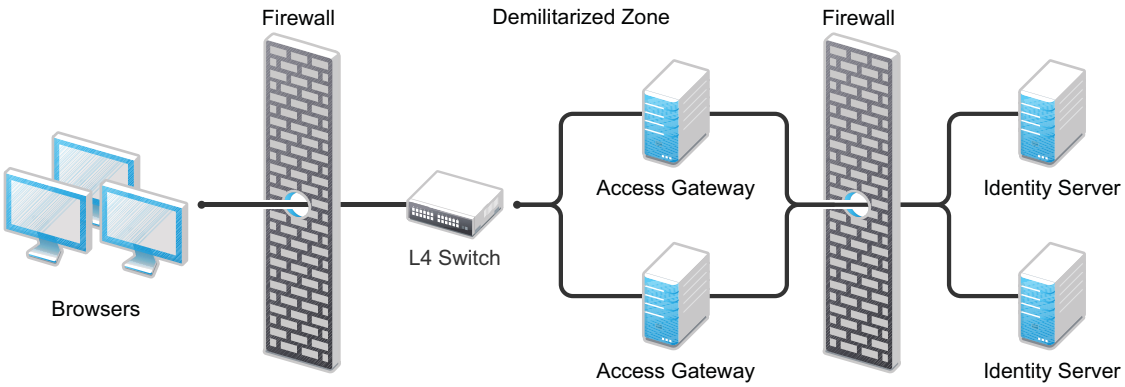
Notice that the user Tom is now assigned a *sales_role* on the SSL VPN server because the sales policy has been applied.

For more information about traffic policies, see "Configuring Traffic Policies" in the *NetIQ Access Manager 3.2 SSL VPN Server Guide*.

7 Protecting an Identity Server with an Access Gateway

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 7-1 illustrates such a configuration.

Figure 7-1 *Identity Servers behind an Access Gateway*



With this configuration, you need an L4 switch to cluster the Access Gateways. However, you do not need an L4 switch to cluster the Identity Servers. 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.

Limitations: The following features are not supported with this configuration:

- The Identity Server cannot respond to Identity Provider introductions.
- Federation to an external service provider that requires the artifact profile with SOAP/Mutual SSL binding 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.
- The proxy service that is protecting the Identity Server cannot be configured to use NMAS.

Configuration Options: To configure Access Manager in this manner, you must perform the following changes to the basic configuration.

- Section 7.1, “Configuring a Linux Identity Server as a Protected Resource,” on page 146
- Section 7.2, “Configuring a Windows Identity Server as a Protected Resource,” on page 152

7.1 Configuring a Linux Identity Server as a Protected Resource

These configuration steps assume that you are using SSL.

1. (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, `*.provo.novell.com`, where the Identity Server DNS is `idp.provo.novell.com` and the Access Gateway DNS is `jwilson1.provo.novell.com`.

   If you don't have a wildcard certificate, you cannot use domain-based multi-homing for this configuration scenario.

   If you are using path-based multi-homing, you can use the same certificate for the Identity Server and the Access Gateway.

2. Configure the Base URL of the Identity Server. For complete configuration information, see Section 1.3, "Creating a Basic Identity Server Configuration," on page 11.

   2a Click *Devices* > *Identity Servers* > *Edit*.

   2b Set the port to 443.

   2c Specify the correct domain name for the proxy service type.

   Path-Based Proxy Service: 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.

   For example, if your proxy service has a public DNS name of `jwilson1.provo.novell.com`, that is the name you must specify for the Base URL.

   Domain-Based Proxy Service: 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. Specify a name that allows the two to share a common subdomain.

   For example, if the proxy service name is `jwilson1.provo.novell.com`, replace `jwilson1`with `idp` so that the name is `idp.provo.novell.com`.

3. Configure the Identity Server to use the correct certificate:

   3a Click the *SSL Certificate* icon.

   3b Click *Replace*, then click the *Select Certificate* icon.

   3c For a domain-based proxy service, select the wildcard certificate. For a path-based proxy service, select the certificate that matches the DNS name of the Access Gateway.

   3d Click *OK* twice, then accept the prompt to restart Tomcat.

4. When the health of the Identity Server turns green, continue with Step 5 for a domain-based proxy service or Step 6 for a path-based proxy service.

5. (Domain-Based Proxy Service) Set up a proxy service on the Access Gateway for the Identity Server:

   5a Click *Devices* > *Access Gateways* > *Edit* > *[Name of Reverse Proxy]*.

   For more information about creating a proxy service, see "Managing Reverse Proxies and Authentication" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

   5b In the *Proxy Service* list, click *New*.

   5c Set the *Multi-Homing Type* field to *Domain-Based*.

   5d Set the following fields to the specified values:

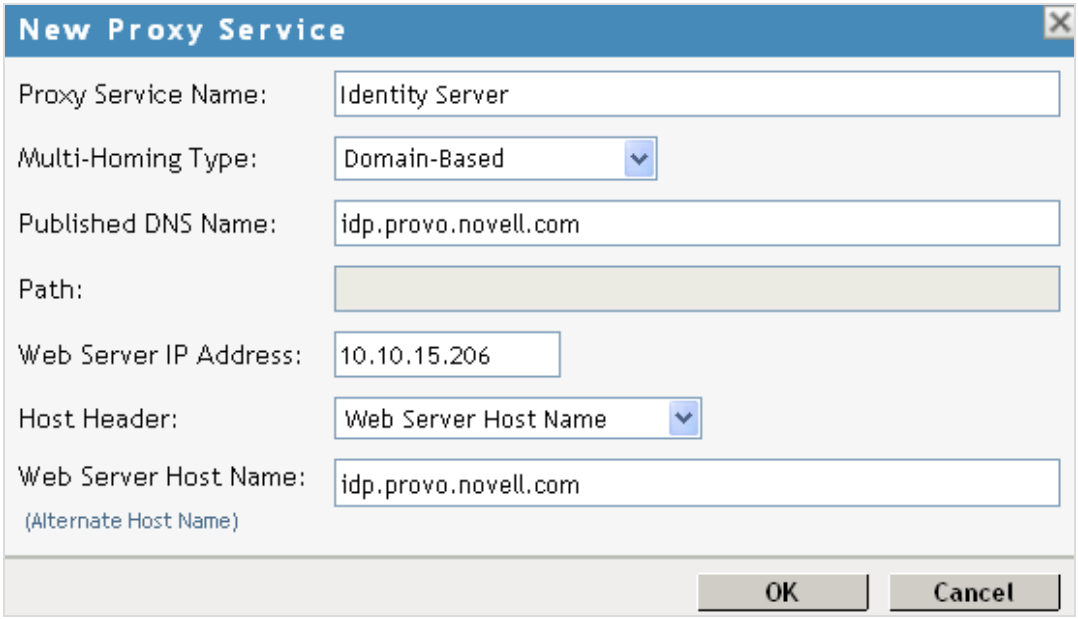
Published DNS Name: Specify the same name you have specified for the domain name of the Base URL of the Identity Server. Your DNS server must be set up to resolve this name to the Access Gateway.

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.

Your proxy service configuration should look similar to the following:



6 (Path-Based Proxy Service) Set up a proxy service on the Access Gateway for the Identity Server:

6a Click *Devices* > *Access Gateways* > *Edit* > *[Name of Reverse Proxy]*.

For more information about creating a proxy service, see "Managing Reverse Proxies and Authentication" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*

6b In the *Proxy Service* list, click *New*.

6c Set the *Multi-Homing Type* field to *Path-Based* and set the *Path* field to `/nidp`.

6d Set the following fields to the specified values:

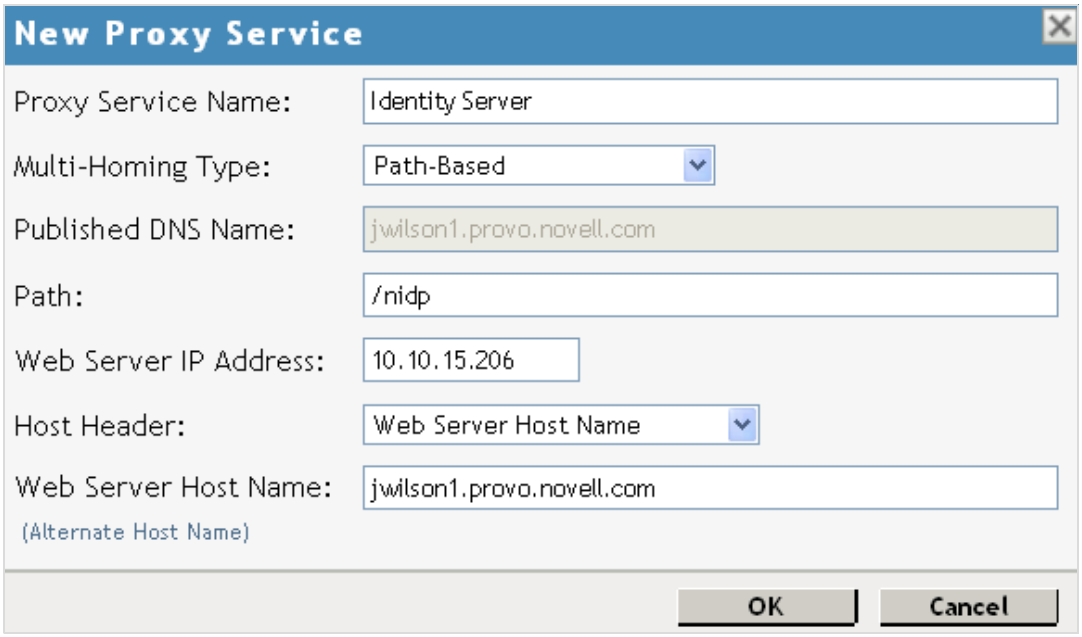
Published DNS Name: Specify the same name you have specified for the domain name of the Base URL of the Identity Server. Your DNS server must be set up to resolve this name to the Access Gateway.

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.

Your proxy service configuration should look similar to the following:



6e Click *OK*.

6f Click the name of your proxy service.

6g On the Path-Based Multi-Homing page, make sure the *Remove Path on Fill* option is not selected.

The Identity Server needs the `/nidp` path.

6h Click *OK*.

7 Configure a protected resource for the proxy service:

7a In the *Proxy Service List*, click the link under the *Protected Resources* column.

For more information about configuring protected resources, see "Configuring Protected Resources" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

7b Click *New*, specify a name, then click *OK*.

7c Configure the following fields:

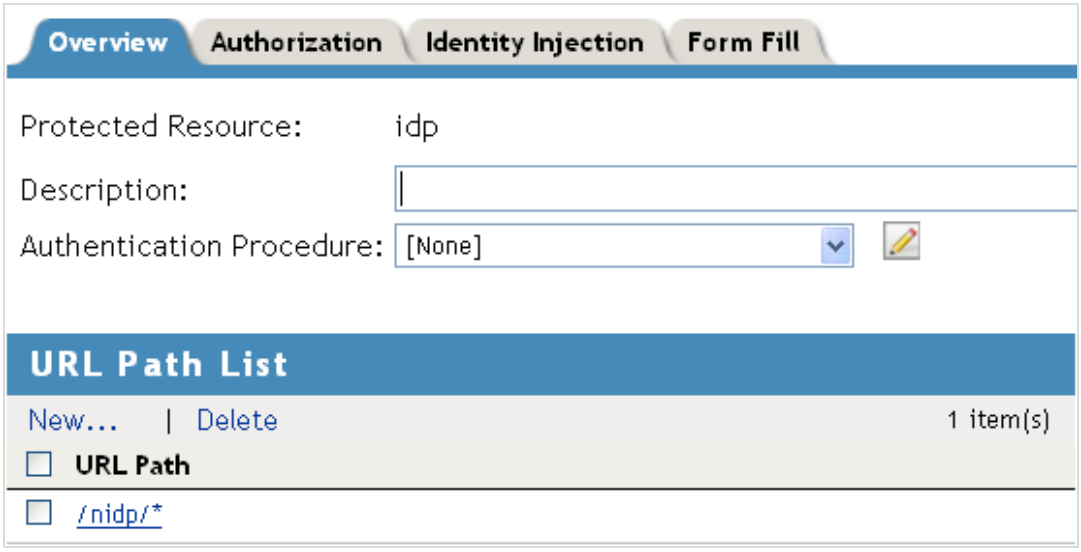
Authentication Procedure: Set this field to *None*.

The Identity Server needs to be set up as a public resource.

URL Path: Set the path of the protected resource to the following value:

```
/nidp/*
```

Your protected resource should look similar to the following:



7d Click *OK*.

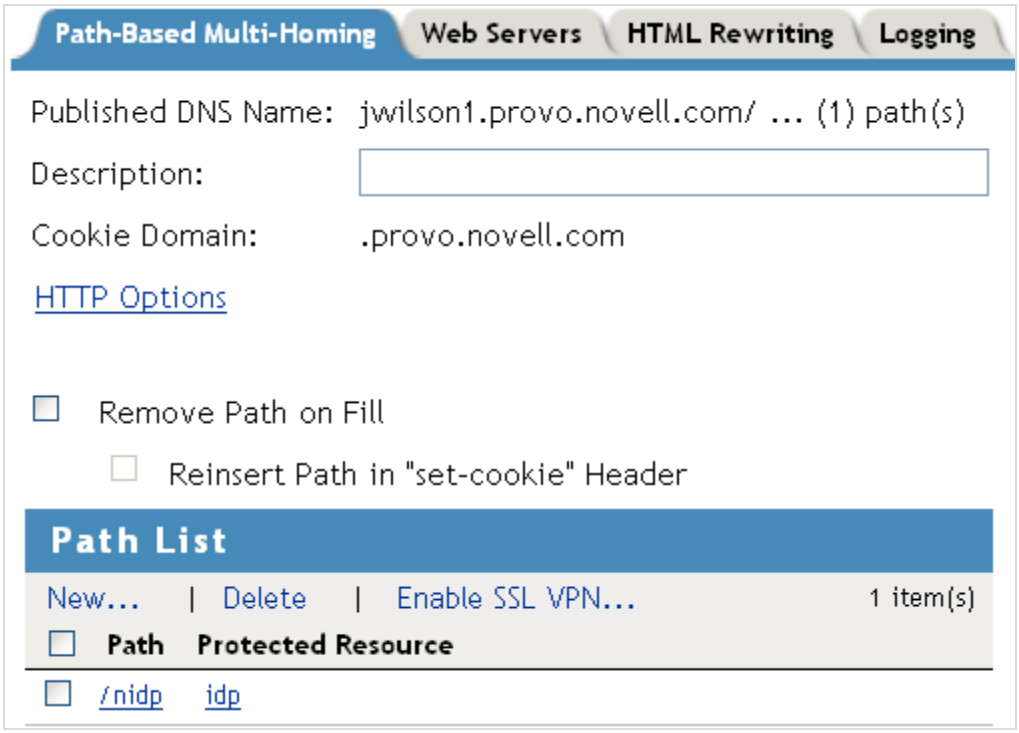
8 (Path-Based Proxy Service) Verify the configuration:

8a Click the name of your path-based proxy service.

8b Verify that the *Remove Path on Fill* option is not selected.

8c Verify that the *Path List* has an entry with /nidp as the path for the protected resource.

Your configuration should look similar to the following:



8d Click *OK*.

9 Set up the Access Gateway to use SSL between the browsers and the Access Gateway.

For configuration information, see "Configuring SSL Communication with the Browsers and the Identity Server " in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

- For a domain-based proxy service, select to use the wildcard certificate.
- For a path-based proxy service, SSL is configured on the parent proxy service. Configure the parent proxy service to use a certificate that matches its DNS name.

10 Set up SSL between the proxy service that is protecting the Identity Server and the Identity Server. In this type of configuration, the Identity Server is acting as a protected Web server of the Access Gateway.

10a Click *Devices* > *Access Gateways* > *Edit* > *[Name of Reverse Proxy]* > *[Name of Proxy Service]* > *Web Servers*.

For additional configuration information, see "Configuring SSL between the Proxy Service and the Web Servers" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

10b Configure the following:

Connect Using SSL: Enable this option.

Web Server Trusted Root: Select *Any in Reverse Proxy Trust Store*.

SSL Mutual Certificate: Do not configure this option.

Connect Port: Specify 8443.

11 (Conditional) If the cluster configuration for the Identity Server contains more than one Identity Server, configure the following options:

11a Click *Devices* > *Access Gateways* > *Edit* > *[Name of Reverse Proxy]* > *[Name of Proxy Service]* > *Web Servers*.

11b 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.

11c Click *TCP Connect Options*, then configure the following options:

Policy for Multiple Destination IP Addresses: For the Identity Servers, select *Round Robin*.

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.

12 Configure HTML rewriting:

12a Click *Devices* > *Access Gateways* > *Edit* > *[Name of Reverse Proxy]* > *[Name of Proxy Service]* > *HTML Rewriting*

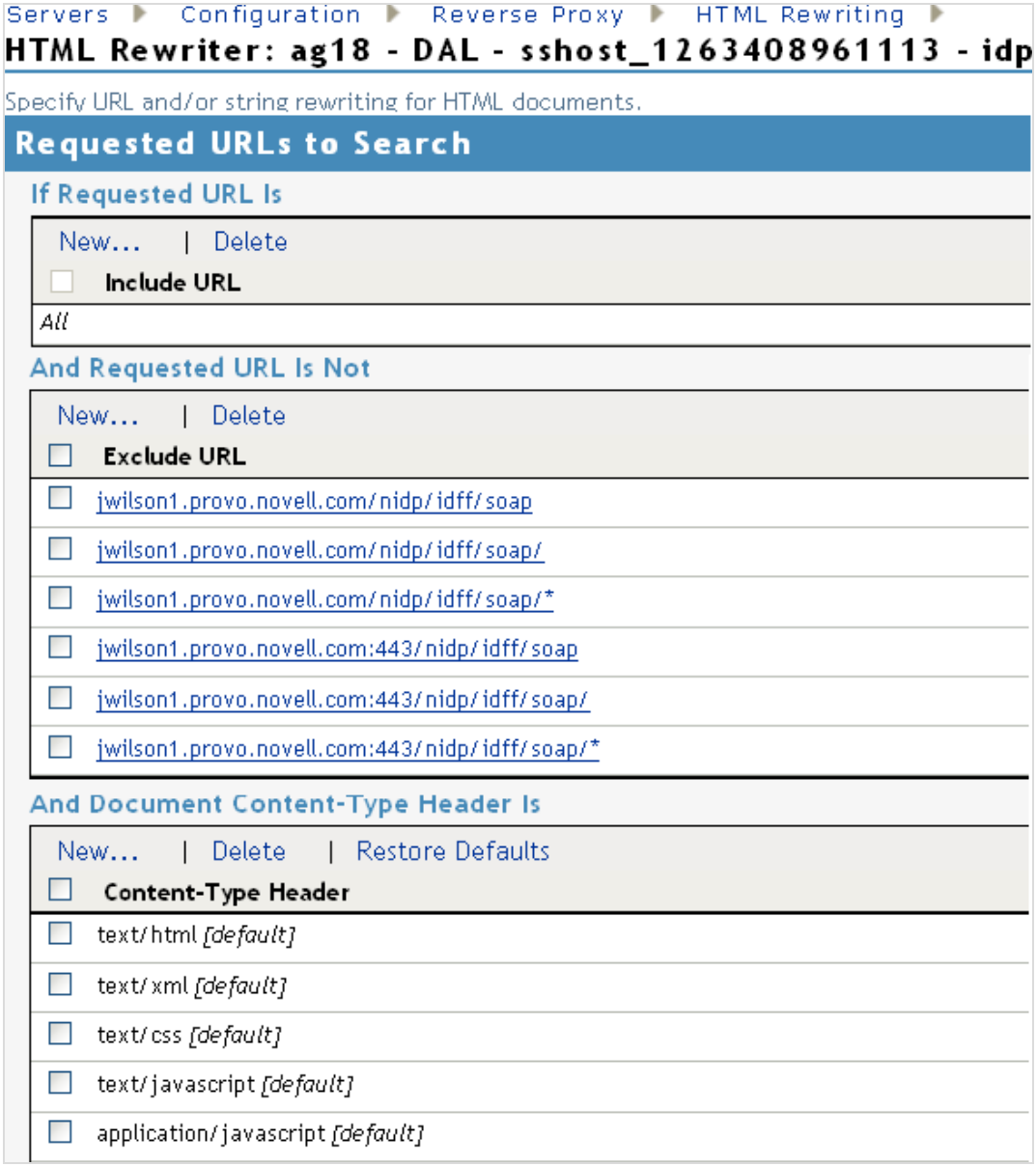
12b Make sure the *Enable HTML Rewriting* option is selected.

12c In the *HTML Rewriter Profile List*, click *New*, then specify a name for the profile and select *Word* for the *Search Boundary*.

12d Specify the following URLs in the *And Requested URL Is Not* section. The following URLs use `jwilson1.provo.novell.com/nidp` as the DNS name of the reverse proxy for the Identity Server.

```
jwilson1.provo.novell.com/nidp/idff/soap
jwilson1.provo.novell.com/nidp/idff/soap/
jwilson1.provo.novell.com/nidp/idff/soap/*
jwilson1.provo.novell.com:443/nidp/idff/soap
jwilson1.provo.novell.com:443/nidp/idff/soap/
jwilson1.provo.novell.com:443/nidp/idff/soap/*
```

Your rewriter profile should look similar to the following for the path-based proxy service example:



The example name for the domain-based proxy service is `idp.provo.novell.com`, which is the DNS name you would use when configuring the rewriter for a domain-based proxy service.

12e Click *OK*.

12f Use the up-arrow icon to move your profile to the top of the list.

13 Configure the Pin List so that the Identity Server pages are not cached:

13a On the Server Configuration page, click *Pin List*.

13b In the list, click *New*, then specify the following values:

URL Mask: Specify `/nidp/*` for the URL.

Pin Type: Select *Bypass*.

For more information, see "Configuring a Pin List" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

13c Click *OK* twice.

14 Update the Access Gateway.

7.2 Configuring a Windows Identity Server as a Protected Resource

These configuration steps assume that you are using SSL.

1 (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, `*.provo.novell.com`, where the Identity Server DNS is `idp.provo.novell.com` and the Access Gateway DNS is `jwilson1.provo.novell.com`.

If you don't have a wildcard certificate, you cannot use domain-based multi-homing for this configuration scenario.

If you are using path-based multi-homing, you can use the same certificate for the Identity Server and the Access Gateway.

2 Configure the Base URL of the Identity Server. For complete configuration information, see Section 1.3, "Creating a Basic Identity Server Configuration," on page 11.

2a Click *Devices* > *Identity Servers* > *Edit*.

2b Set the port to 443.

When you change the base URL of the Identity Provider, all Access Manager

devices that have an Embedded Service Provider need to be updated to import the new metadata. To re-import the metadata, configure the device so it does not have a trusted relationship with the Identity Server, update the device, reconfigure the device for a trusted relationship, and update the device. For more information, see "Embedded Service Provider Metadata" in the *NetIQ Access Manager 3.2 Identity Server Guide*.

2c Specify the correct domain name for the proxy service type.

Path-Based Proxy Service: If you are using path-based multi-homing, the domain name of the Base URL must match the public DNS of the authentication proxy service set up in the Access Gateway.

For example, if your proxy service has a public DNS name of `jwilson1.provo.novell.com`, that is the domain name you must specify for the Base URL.

Domain-Based Proxy Service: 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. Specify a name that allows the two to share a common subdomain.

For example, if the proxy service name is `jwilson1.provo.novell.com`, replace `jwilson1` with `idp` so that the domain name is `idp.provo.novell.com`.

3 Configure the Identity Server to use the correct certificate:

3a Click the *SSL Certificate* icon.

3b Click *Replace*, then click the *Select Certificate* icon.

3c For a domain-based proxy service, select the wildcard certificate. For a path-based proxy service, select the certificate that matches the DNS name of the Access Gateway.

3d Click *OK* twice, then accept the prompt to restart Tomcat.

4 Continue with Step 5 for a domain-based proxy service or Step 6 for a path-based proxy service.

5 (Domain-Based Proxy Service) Set up a proxy service on the Access Gateway for the Identity Server:

5a Click *Devices* > *Access Gateways* > *Edit* > *[Name of Reverse Proxy]*.

For more information about creating a proxy service, see "Managing Reverse Proxies and Authentication" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

5b In the *Proxy Service* list, click *New*.

5c Set the *Multi-Homing Type* field to *Domain-Based*.

5d Set the following fields to the specified values:

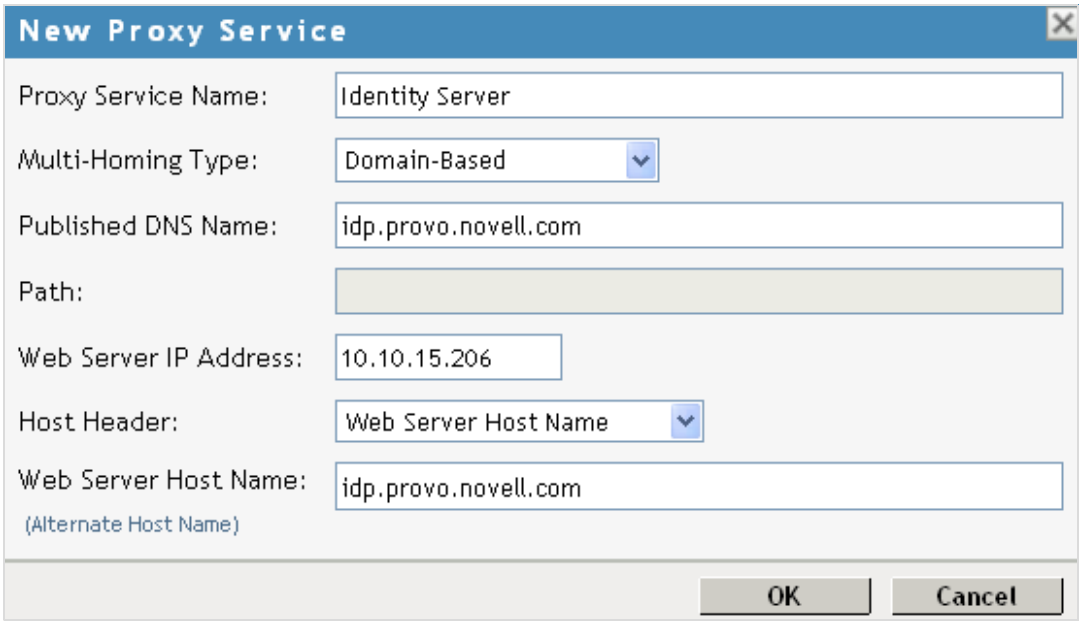
Published DNS Name: Specify the same name you have specified for the domain name of the Base URL of the Identity Server. Your DNS server must be set up to resolve this name to the Access Gateway.

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.

Your proxy service configuration should look similar to the following:



6 (Path-Based Proxy Service) Set up a proxy service on the Access Gateway for the Identity Server:

6a Click *Devices* > *Access Gateways* > *Edit* > *[Name of Reverse Proxy]*.

For more information about creating a proxy service, see "Managing Reverse Proxies and Authentication" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*

6b In the *Proxy Service* list, click *New*.

6c Set the *Multi-Homing Type* field to *Path-Based* and set the *Path* field to `/nidp`.

6d Set the following fields to the specified values:

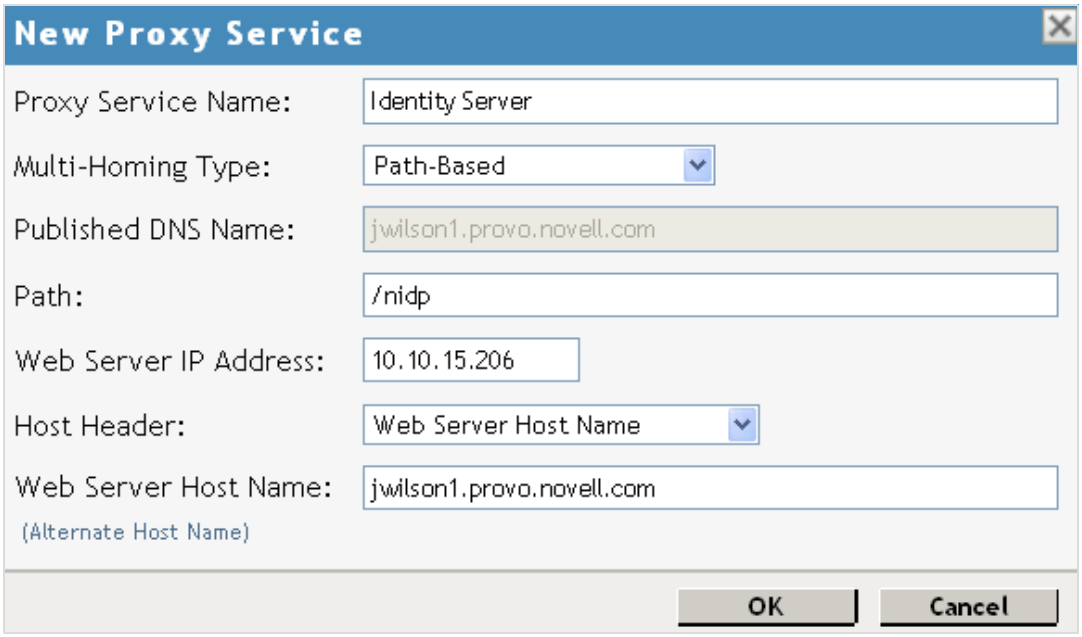
Published DNS Name: Specify the same name you have specified for the domain name of the Base URL of the Identity Server. Your DNS server must be set up to resolve this name to the Access Gateway.

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.

Your proxy service configuration should look similar to the following:



6e Click *OK*.

7 Configure a protected resource for the proxy service:

7a In the *Proxy Service List*, click the link under the *Protected Resources* column.

For more information about configuring protected resources, see "Configuring Protected Resources" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

7b Click *New*, specify a name, then click *OK*.

7c Configure the following fields:

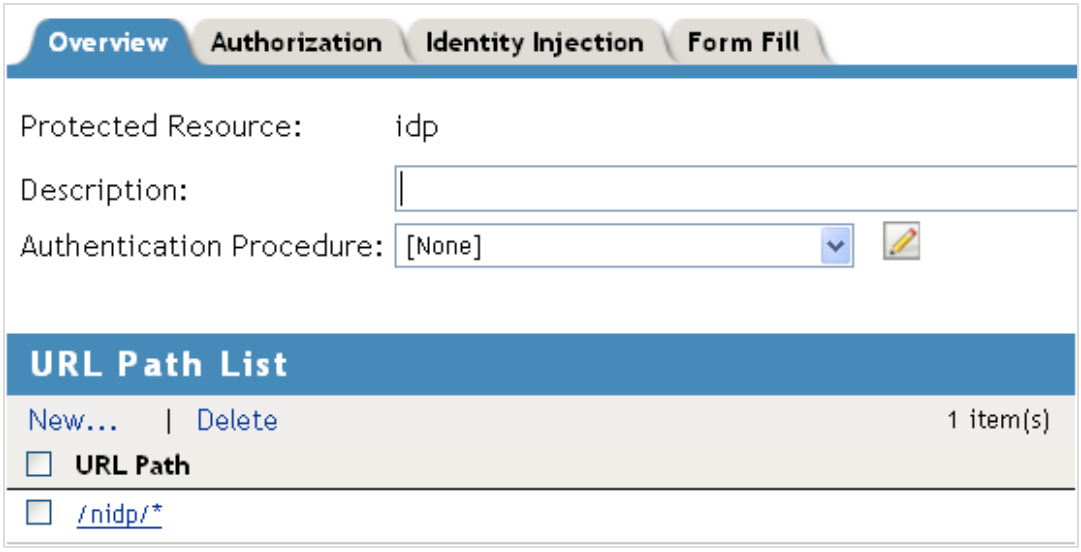
Authentication Procedure: Set this field to *None*.

The Identity Server needs to be set up as a public resource.

URL Path: Set the path of the protected resource to the following value:

```
/nidp/*
```

Your protected resource should look similar to the following:



7d Click *OK*.

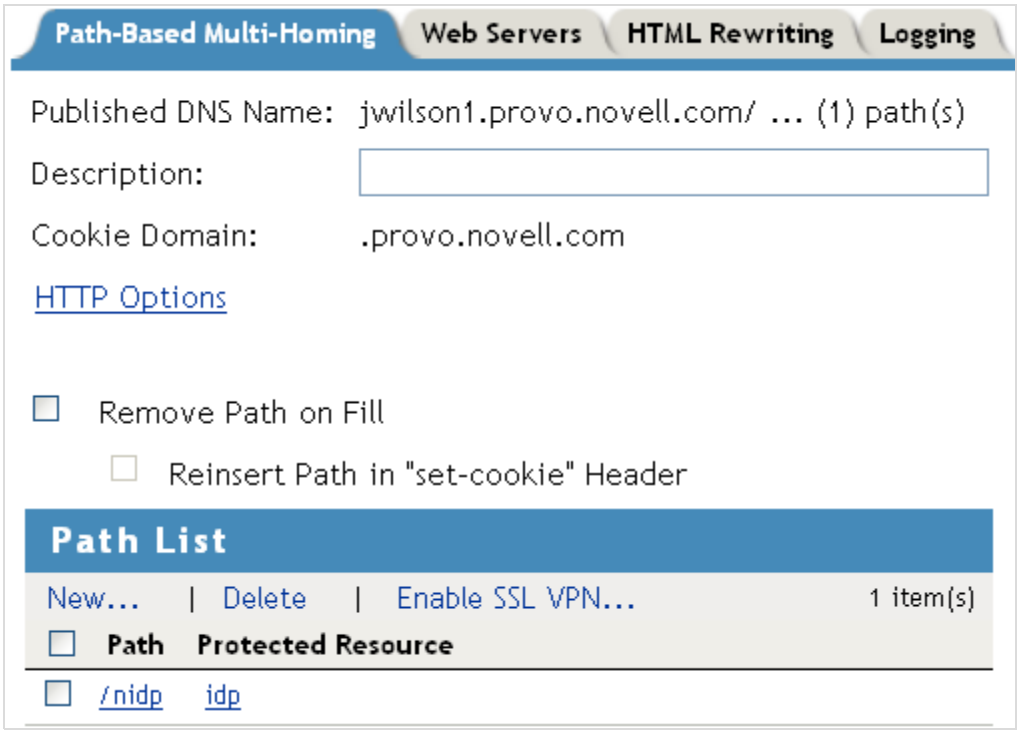
8 (Path-Based Proxy Service) Verify the configuration:

8a Click the name of your path-based proxy service.

8b Verify that the *Remove Path on Fill* option is not selected.

8c Verify that the *Path List* has an entry with /nidp as the path for the protected resource.

Your configuration should look similar to the following:



8d Click *OK*.

9 Specify a host entry for the Identity Server:

9a Click *Devices* > *Access Gateways* > *Edit* > *Hosts*.

9b Click *New*, specify the IP address of the Identity Server, then click *OK*.

9c In the *Host Name(s)* text box, specify the DNS name of the Identity Server machine.

9d Click *OK*.

10 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 *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

11 Set up SSL between the proxy service that is protecting the Identity Server and the Identity Server.

In this type of configuration, the Identity Server is acting as a protected Web server of the Access Gateway.

11a Click *Devices* > *Access Gateways* > *Edit* > *[Name of Reverse Proxy]* > *[Name of Proxy Service]* > *Web Servers*.

For additional configuration information, see "Configuring SSL between the Proxy Service and the Web Servers" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

11b Configure the following:

Connect Using SSL: Enable this option.

Web Server Trusted Root: Select *Any in Reverse Proxy Trust Store*.

SSL Mutual Certificate: Do not configure this option.

Connect Port: Specify 443.

12 Modify the `server.xml` file on the Identity Server to use port 443.

12a Change to the Tomcat configuration directory.

Windows Server 2008: `\Program Files (x86)\Novell\Tomcat\conf`

12b Open the `server.xml` file.

12c Change port 8080 to port 80 and port 8443 to 443, then save the file.

12d Restart the Tomcat service.

13 (Conditional) If the cluster configuration for the Identity Server contains more than one Identity Server, configure the following options:

13a Click *Devices* > *Access Gateways* > *Edit* > *[Name of Reverse Proxy]* > *[Name of Proxy Service]* > *Web Servers*.

13b 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.

13c Click *TCP Connect Options*, then configure the following options.

Policy for Multiple Destination IP Addresses: For the Identity Servers, select *Round Robin*.

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.

14 Configure HTML rewriting:

14a Click *Devices* > *Access Gateways* > *Edit* > *[Name of Reverse Proxy]* > *[Name of Proxy Service]* > *HTML Rewriting*

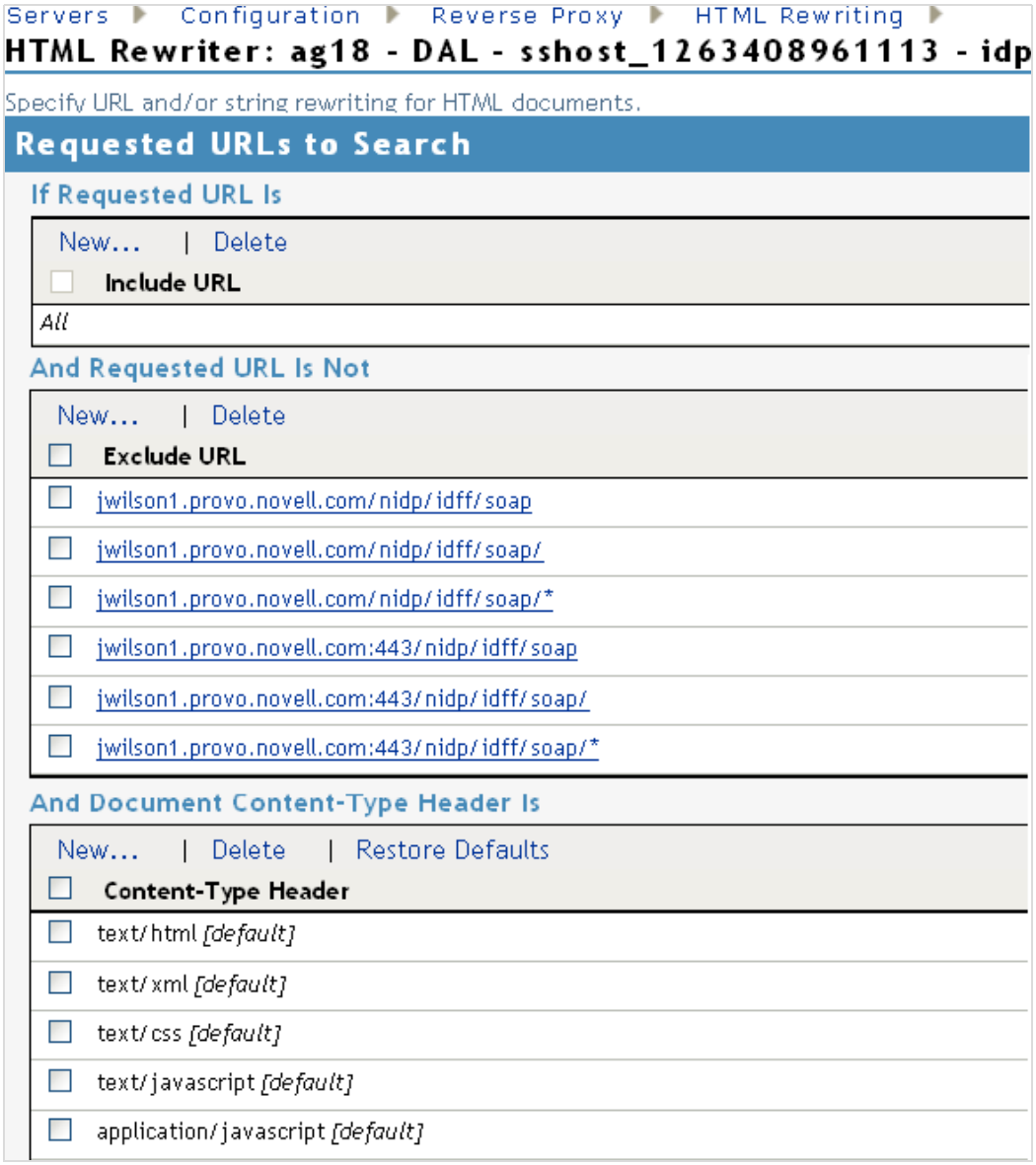
14b Make sure the *Enable HTML Rewriting* option is selected.

14c In the *HTML Rewriter Profile List*, click *New*, then specify a name for the profile and select *Word* for the *Search Boundary*.

14d Specify the following URLs in the *And Requested URL Is Not* section. The following URLs use `jwilson1.provo.novell.com/nidp` as the DNS name of the proxy service for the Identity Server. This is the example name for the path-based proxy service.

```
jwilson1.provo.novell.com/nidp/idff/soap
jwilson1.provo.novell.com/nidp/idff/soap/
jwilson1.provo.novell.com/nidp/idff/soap/*
jwilson1.provo.novell.com:443/nidp/idff/soap
jwilson1.provo.novell.com:443/nidp/idff/soap/
jwilson1.provo.novell.com:443/nidp/idff/soap/*
```

Your rewriter profile should look similar to the following:



The example name for the domain-based proxy service is `idp.provo.novell.com`, which is the DNS name you would use when configuring the rewriter for a domain-based proxy service.

14e Click *OK*.

14f Use the up-arrow icon to move your profile to the top of the list.

15 Configure the Pin List so that the Identity Server pages are not cached:

15a On the Server Configuration page, click *Pin List*.

15b In the list, click *New*, then specify the following values:

URL Mask: Specify `/nidp/*` for the URL.

Pin Type: Select *Bypass*.

For more information about configuring a Pin list, see "Configuring a Pin List" in the *NetIQ Access Manager 3.2 SP1 Access Gateway Guide*.

15c Click *OK* twice.

16 Update the Access Gateway.

NOTE: If the SuSEFirewall is configured, after starting the firewall, all ports and services are blocked by default. You need to create filters to allow the Access Gateway and any other service to communicate with the Identity Servers.
