Novell Access Manager

3.0

www.novell.com

SETUP GUIDE

March 7, 2007

Novell®

Legal Notices

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

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

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

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

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

Novell is a registered trademark of Novell, Inc., in the United States and other countries.
SUSE is a registered trademark of Novell, Inc., in the United States and other countries.

Third-Party Materials

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

Contents

About This Guide

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

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

- Chapter 1, “Setting Up a Basic Access Manager Configuration,” on page 9
- Chapter 3, “Configuring SSL VPN to Protect an Application,” on page 37
- Chapter 2, “Enabling SSL Communication,” on page 27
- Chapter 4, “Clustering Identity Servers,” on page 41
- Chapter 5, “Configuring Access Gateways for Fault Tolerance,” on page 45
- Chapter 6, “Setting Up Firewalls,” on page 49
- Chapter 7, “Protecting an Identity Server with an Access Gateway,” on page 63

Not all Access Manager functionality and administrative tasks are discussed here. After you are familiar with Access Manager and the steps in this section, you can use the *Novell Access Manager 3.0 Administration Guide* as the source for additional or advance configuration, such as Identity Federation. To gain more experience before deploying Access Manager in a production environment, you also might first deploy the Digital Airlines example. See *Novell Access Manager 3.0 Digital Airlines Example Documentation*.

Audience

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

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

Feedback

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

Additional Documentation

- *Novell Access Manager 3.0 Installation Guide*
- *Novell Access Manager 3.0 Administration Guide*
- *Novell Access Manager 3.0 Digital Airlines Example Documentation*
- *Novell Access Manager 3.0 J2EE Agent Guide*

Documentation Conventions

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

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

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

Setting Up a Basic Access Manager Configuration

1

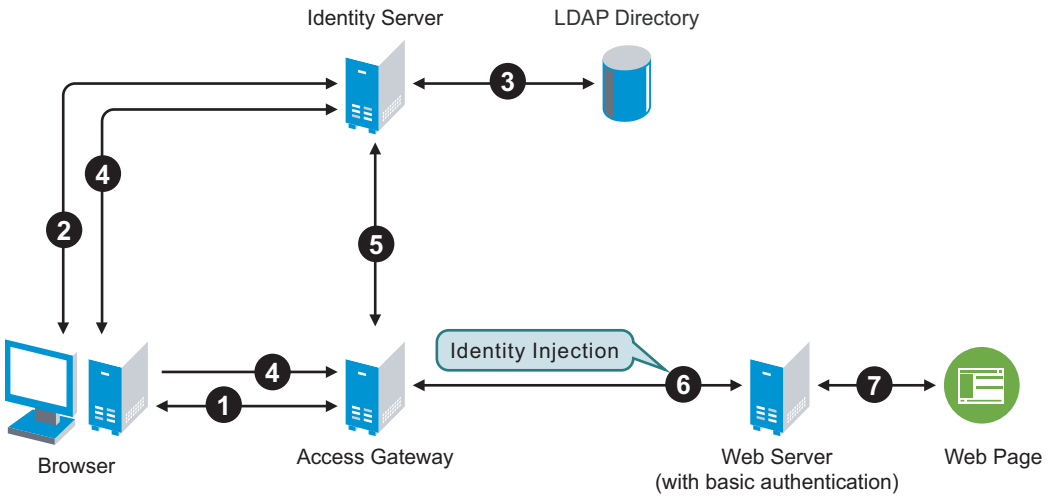
The initial setup for Novell® Access Manager consists of installing the components and setting up the Identity Server and the Access Gateway to protect your corporate resources running on an HTTP Web server. Access Manager can also be configured to protect other resources such as applications on J2EE servers and non-HTTP applications. These should be set up after you have created a basic setup. For J2EE server applications, see the "Novell Access Manager 3.0 J2EE Agent Guide". For non-HTTP applications, see Chapter 3, "Configuring SSL VPN to Protect an Application," on page 37.

This tutorial describes the following topics and tasks:

1.1 Understanding an Access Manager Configuration

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

Figure 1-1 *Basic Process Flow*

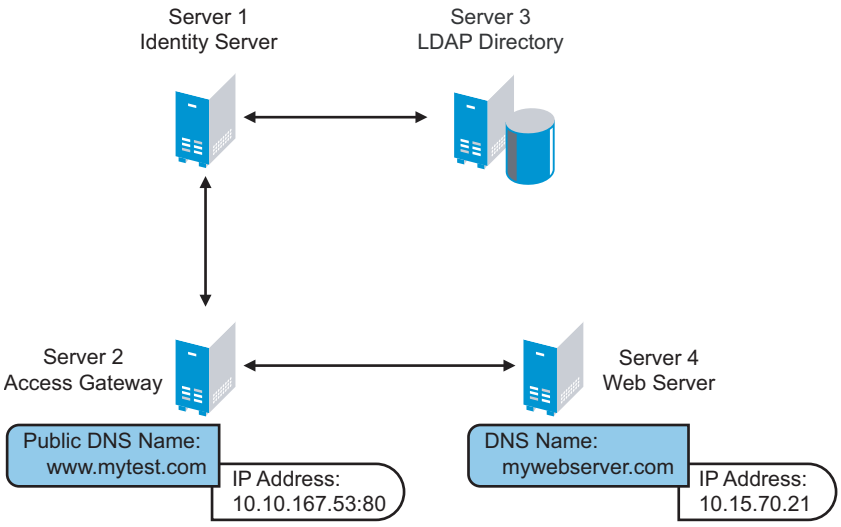


1. The user requests access to a protected resource.
2. The Access Gateway redirects the user to the Identity Server, which prompts for a username and password.

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

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

Figure 1-2 *Basic Access Manager Configuration*



Although other configurations are possible, this section explains the configuration tasks for this basic Access Manager configuration. This section explains how to set up communication use HTTP. For HTTPS over SSL, see Chapter 2, "Enabling SSL Communication," on page 27.

1.2 Prerequisites for Setup

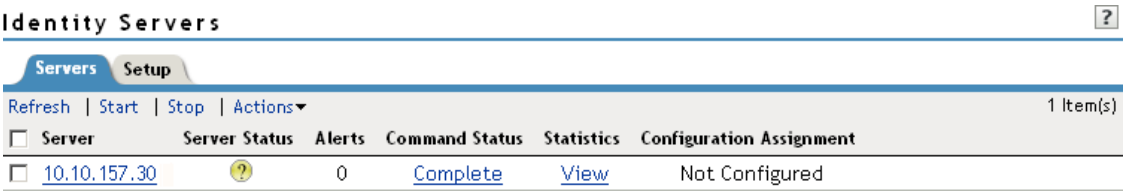
The following prerequisites are for setting up a basic Access Manager configuration:

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

- ❑ 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 that you will configure the Access Gateway to require authentication before allowing access. You have not configured the Web server to protect this page.
  - A link to a page in the `basic` directory that you have configured your Web server to require basic authentication before allowing access. See your Web Server documentation for instructions on setting up basic authentication.
- ❑ A client workstation with a browser.
- ❑ Browser pop-ups are enabled.

1.3 Creating a Basic Identity Server Configuration

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



At this point the Identity Server is in an unconfigured state and is halted. It remains in this state and cannot function until you create an Identity Server configuration. After you create an Identity Server configuration, you must assign the Identity Server to the configuration.

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

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

- The base URL for the server site.
- The LDAP directories (user stores) used to authenticate users, and the trusted root for secure communication between the Identity Server and the user store.
- Certificates used between the Identity Server and the LDAP user store.

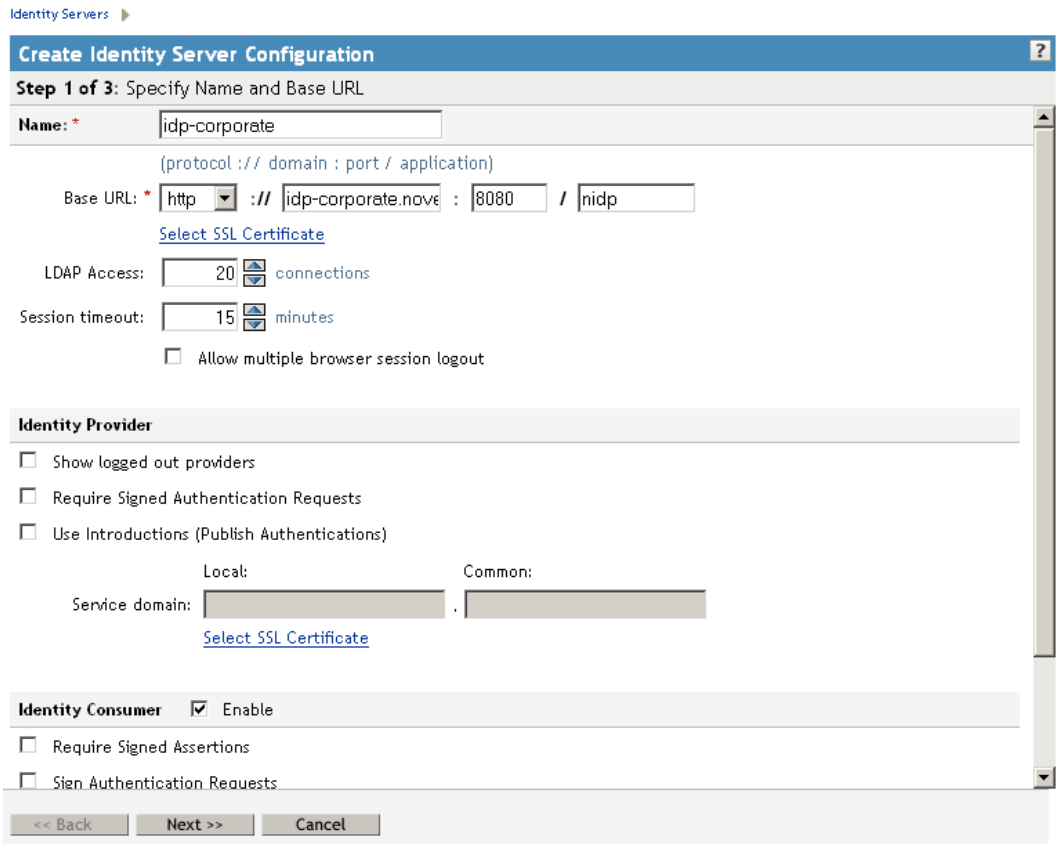
After you create a configuration, you can later change the initial settings, such as local authentication and authorization decisions to meet your needs. The new configuration will be available for you to assign to one or more Identity Servers.

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 an Identity Server Configuration (Advanced Options)" in the *Novell Access Manager 3.0 Administration Guide*.

To create an Identity Server configuration:

1. Enable browser pop-ups.
2. In the Administration Console, click *Access Manager* > *Identity Servers* > *Setup* > *New*.

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



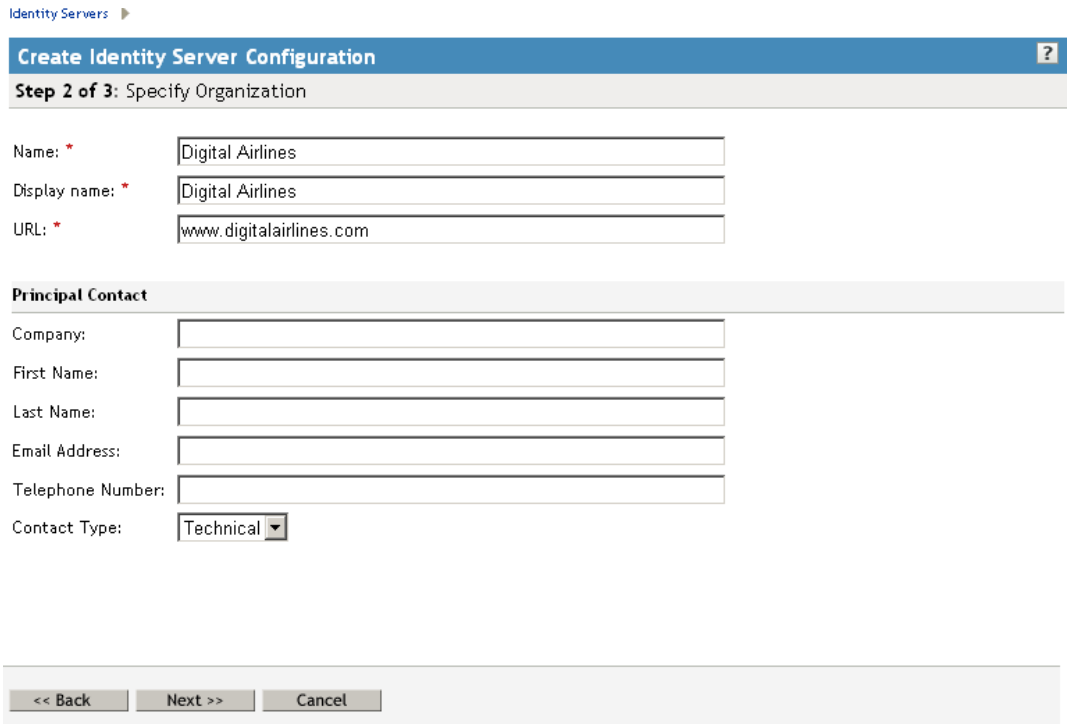
3. Fill in the following fields to specify the properties for your Identity Server configuration:

   Name: The name by which you want to refer to the Identity Server configuration.

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

   - **Protocol:** The communication protocol. Select HTTP for a basic setup.
   - **Domain:** The domain name used to access the Identity Server. Using an IP address is not recommended.
   - **Port:** The port values for the protocol: 8080 for HTTP.
   - **Application:** The Identity Server application path. Leave the default value as *nidp*.
4. 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.

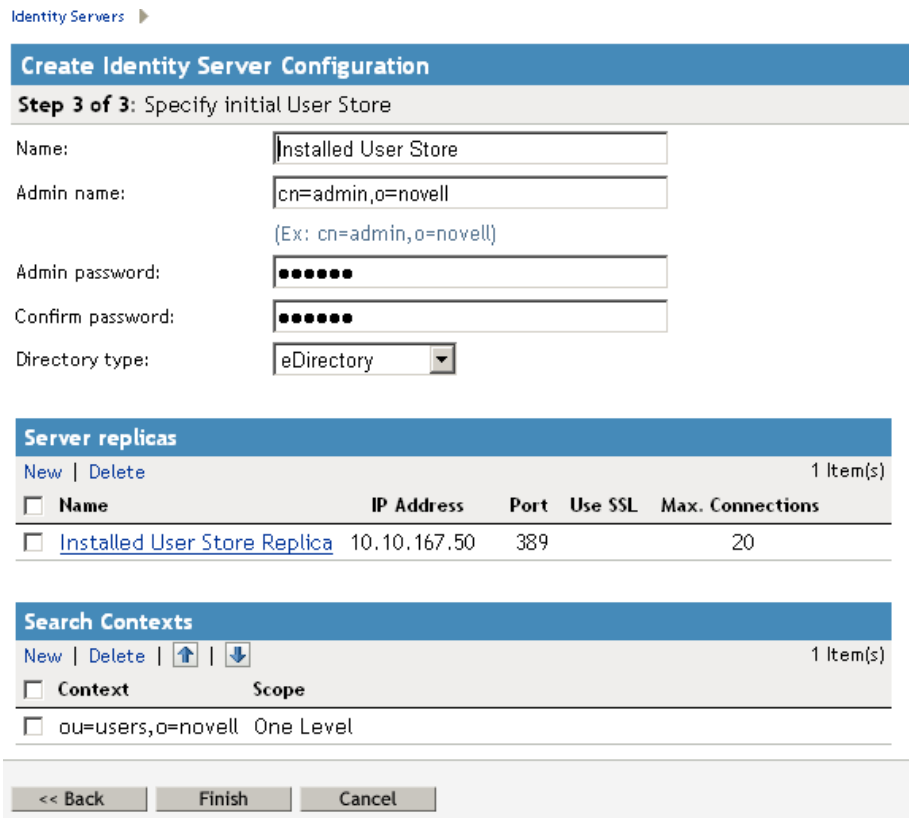
The following fields require information.

- **Name:** The name of the organization.
- **Display Name:** The display name for the organization.
- **URL:** The organization's URL for contact purposes.

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

5 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 (replicas) to which end users authenticate. You can configure a user store with more than one replica to provide load balancing and failover capability. You must reference an existing user store.

Name: A display name for the LDAP directory.

Admin Name: The distinguished name of the admin user of the LDAP directory. Administrator-level rights are required for setting up a user store. This ensures read/write access to all objects used by Access Manager, which allows you to create user accounts, create objects in the configuration store, and use the Credential profile to interact with SecretStore.

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

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

6 Under *Server Replicas*, click *New* to specify the user store replica information. It is recommended that this is a read/write replica.

Name: The display name for the LDAP directory server. If your LDAP directory is replicated on multiple servers, use this name to identify a specific replica.

IP Address: The IP address of the LDAP directory server.

Port: The port of the LDAP directory server.

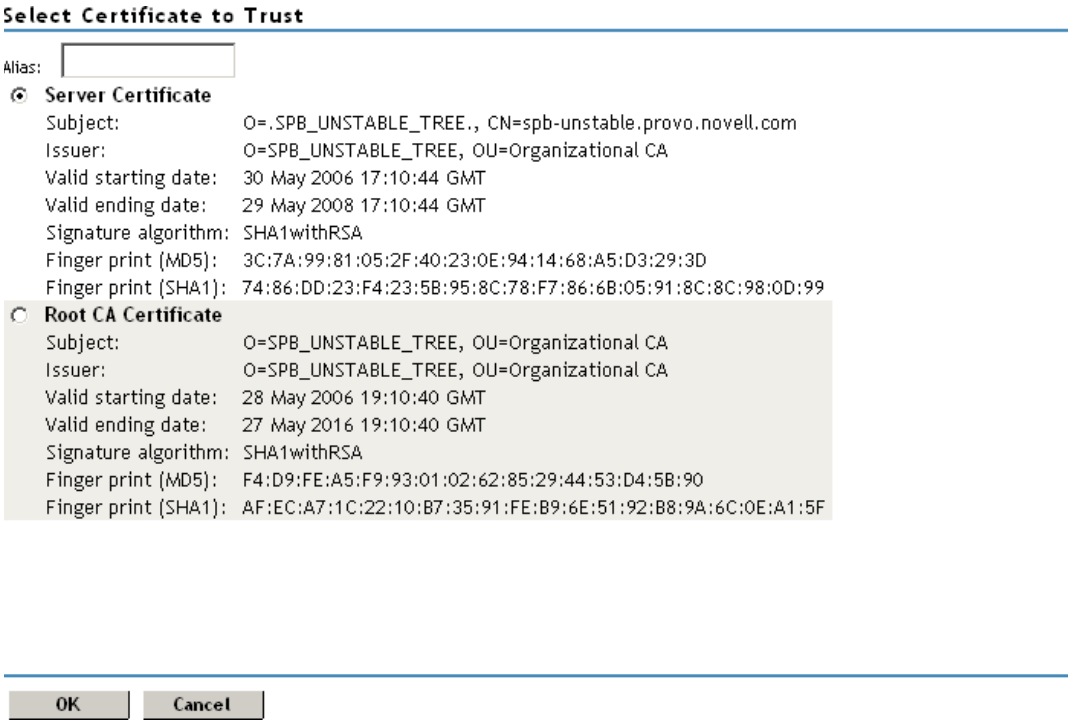
Connection limit: The maximum number of pooled simultaneous connections allowed to the LDAP server. Valid values are between 5 and 100.

7 Click *Use secure LDAP connections*. You must enable SSL between the identity user store and the Identity Server.

This option also must be enabled if you use this user store as a SecretStore User Store Reference in the Credential Profile details. (See "Configuring Credential Profile Security and Display Settings" in the *Novell Access Manager 3.0 Administration Guide*.) If you have specified that this user store is a SecretStore User Store Reference, this option is enabled but not editable.

8 Click *Auto import trusted root*.

9 Click *OK* to confirm the import.



10 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.

11 Specify an alias, then click *OK*.

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

12 Click *OK* in the *Specify server replica information* dialog box.

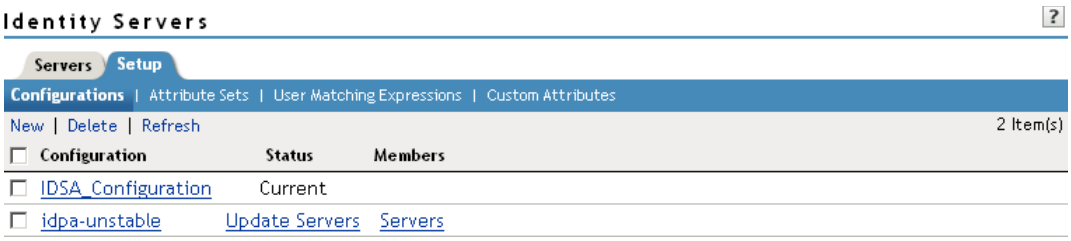
13 Add a Search Context.

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

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

14 Click *Finish* to save the server configuration.

The system displays the new configuration on the Configurations page.



15 Assign the server to a configuration:

15a Click the *Servers* tab.

15b Select the server.

15c Click *Actions* > *Assign to configuration*.

15d Select the configuration.

15e Click *Assign*.

16 Restart Tomcat as prompted.

The status icon for 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.

17 Continue with installing the Access Gateway. See"Installing the Linux Access Gateway" or "Installing the NetWare Access Gateway" in the *Novell Access Manager 3.0 Installation Guide*.

If you have already installed the Access Gateway, continue with Section 1.4, "Configuring the Access Gateway," on page 16.

1.4 Configuring the Access Gateway

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. It can be configured to protect one or more proxy services.

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

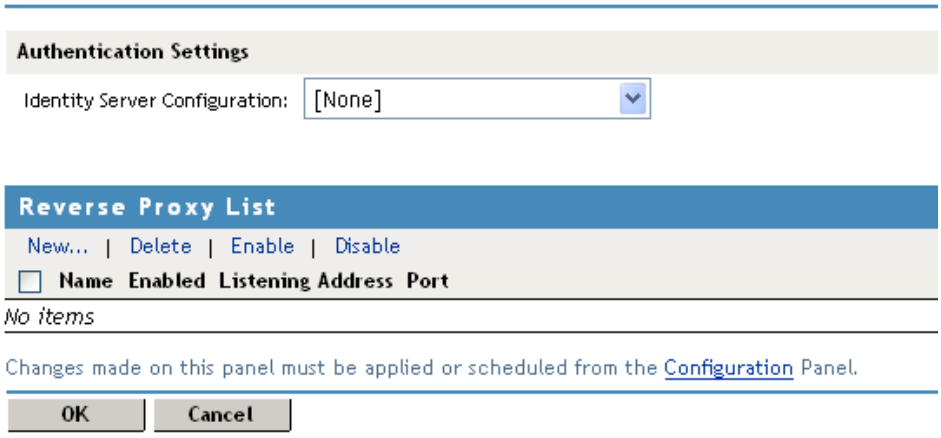
- Section 1.4.1, "Configuring a Reverse Proxy," on page 16
- Section 1.4.2, "Configuring a Public Protected Resource," on page 19

1.4.1 Configuring a Reverse Proxy

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 of these reverse proxies can have a proxy service named `corporate`.

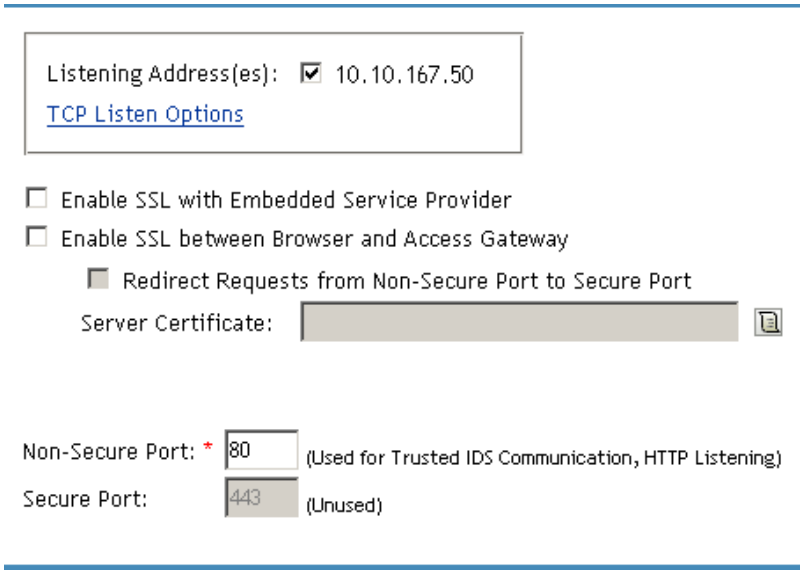
Protected resource names need to be unique to the proxy service, but they don't need to be unique to the Access Gateway because they are always accessed through their proxy service. For example, if you have a proxy service named `account` and a proxy service named `sales`, they both can have a protected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

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



2 In the *Identity Server Configuration* option, select the Identity Server you want the Access Gateway to trust for authentication by selecting the configuration you have assigned to the Identity Server.

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



4 Enable a listening address. Fill in the following fields:

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.

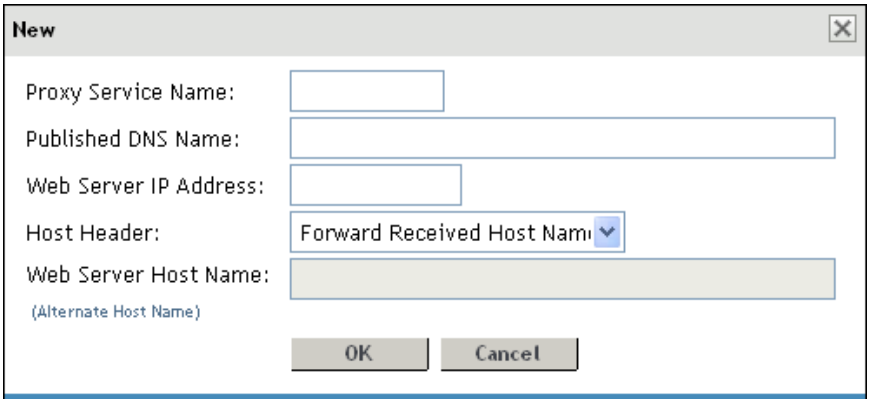
This basic configuration does not set up SSL. For SSL information, see Chapter 2, "Enabling SSL Communication," on page 27.

5 Configure *Non-Secure Port* as the HTTP listening port.

The default port for HTTP is 80. When SSL is not enabled, the *Non-Secure Port* is used for additional tasks, which are listed to the right of the text box.

The *Secure Port* is unused and does not need to be configured.

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



7 Fill in the fields.

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

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

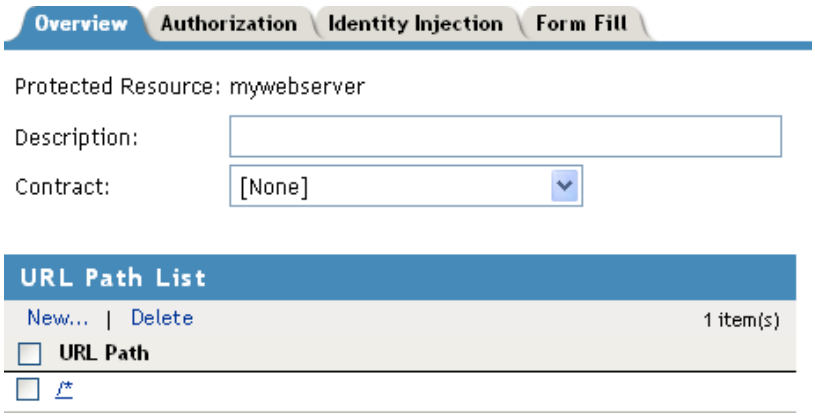
8 Click *OK*.

9 Continue with Section 1.4.2, "Configuring a Public Protected Resource," on page 19.

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 20.

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 *Contact* field must be set to *None*. This is what makes this resource a public resource.
6. Configure the *URL Path List*.

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

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

     `/public/*`
7. Click *OK*.
8. In the *Protected Resource List*, verify that the protected resource you created is enabled.
9. At the bottom of the page, select the *Configuration Panel*, then in the pop-up, click *OK*.

   This is a short cut to return you to the page where you can apply the changes.
10. On the *Configuration* page, select *Apply Changes*, then wait.

Do not click *OK* in the first pop-up which asks you to wait while the changes are being scheduled. When the second pop-up appears confirming that the changes have been applied, click *OK*.

Until this step, nothing has been saved. The *Apply Changes* button pushes the configuration to the server. When the configuration has been successfully applied, the *Server Status* is green and the *Command Status* is *Succeeded*.

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

Wait until the Server Status of the Identity Server turns green.

12 Click *Close*.

13 (Optional). To test this configuration from a client browser, enter the published DNS name as the URL in the browser. For the example illustrated in Figure 1-2 on page 10, you would enter the following URL:

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

This should resolve to the published DNS name you specified in Step 7 on page 18, and the user should be connected to the Web server through the Access Gateway.

14 Continue with Section 1.5, "Configuring the Access Gateway for Authentication," on page 20.

1.5 Configuring the Access Gateway for Authentication

The procedures in Section 1.4, "Configuring the Access Gateway," on page 16 set up the Access Gateway to protect your Web server by hiding its IP address and DNS name from Internet users. The procedures does not require the user to login 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 20
- Section 1.5.2, "Enabling Trusted Authentication," on page 22

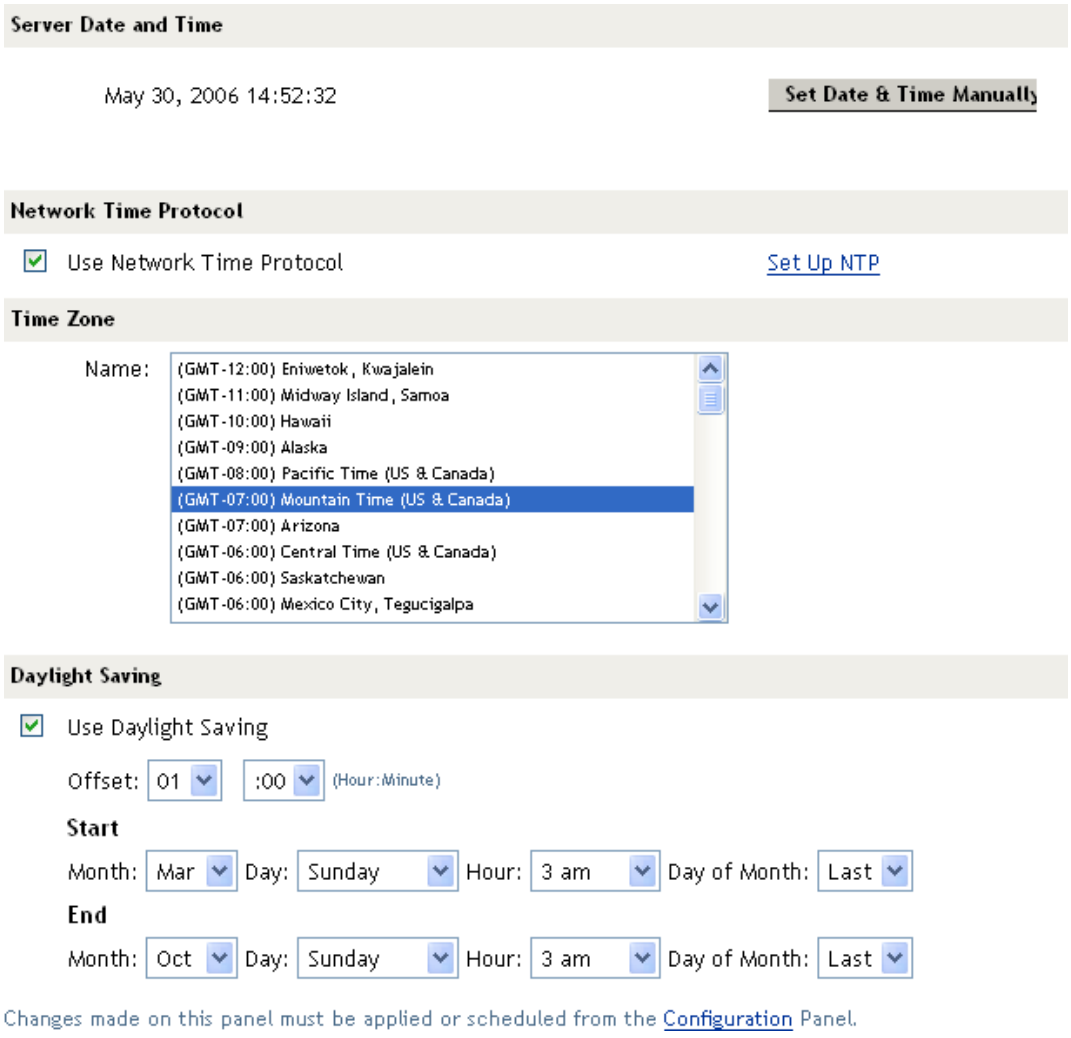
1.5.1 Verifying Time Synchronization

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

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

For an Access Gateway, complete the following steps:

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



2 Select the method you want to use for time:

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

Set Up NTP: Allows you to specify the IP address of an NTP server. Click this option > *New*, specify the IP address of an NTP server, then click *OK*.

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

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

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

4 (NetWare only) In the Daylight Saving section, configure the following fields:

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

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

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

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

5 Click *OK*.

6 On the *Configuration* page, click *Apply Changes*, wait, then in the second pop-up, click *OK*.

7 Continue with "Enabling Trusted Authentication" on page 22.

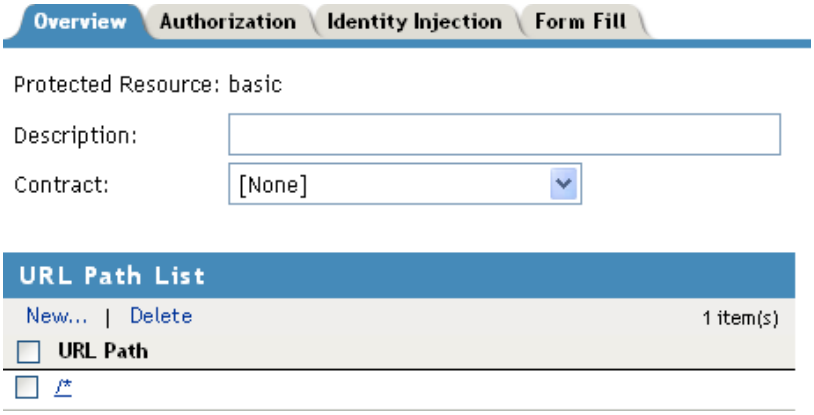
1.5.2 Enabling Trusted Authentication

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

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

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

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



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

- **Name/Password - Basic:** Basic authentication over HTTP using a standard login pop-up screen 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.

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 16 and select a value for the *Trusted Identity Configuration* 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 At the bottom of the page, select *Configuration Panel*, then click *OK*.

6 On the *Configuration* page, select *Apply Changes*, wait, then in the second pop-up, click *OK*.

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

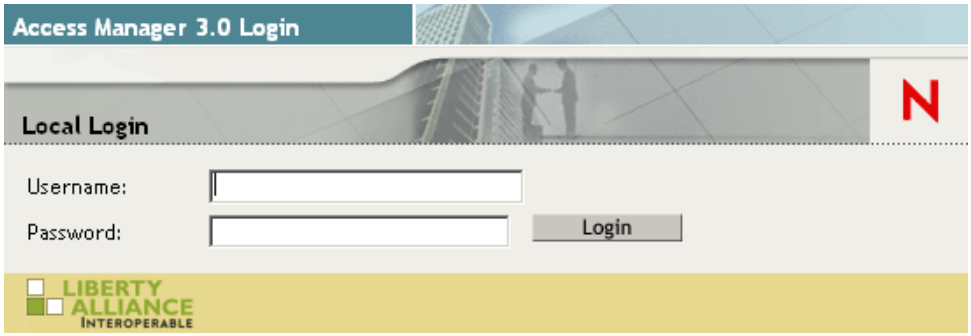
8 (Optional) To test this configuration from a client browser, log in to the Access Manager Portal:

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

9 Continue with Section 1.6, "Setting Up an Identity Injection Policy," on page 23.

1.6 Setting Up an Identity Injection Policy

The Access Gateway lets you retrieve information from your LDAP directory, use it to inject information into HTML headers, query strings, or basic authentication headers, and send this information to the back-end Web servers. Access Manager calls this technology *Identity Injection* (iChain® calls it Object Level Access Control).

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

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

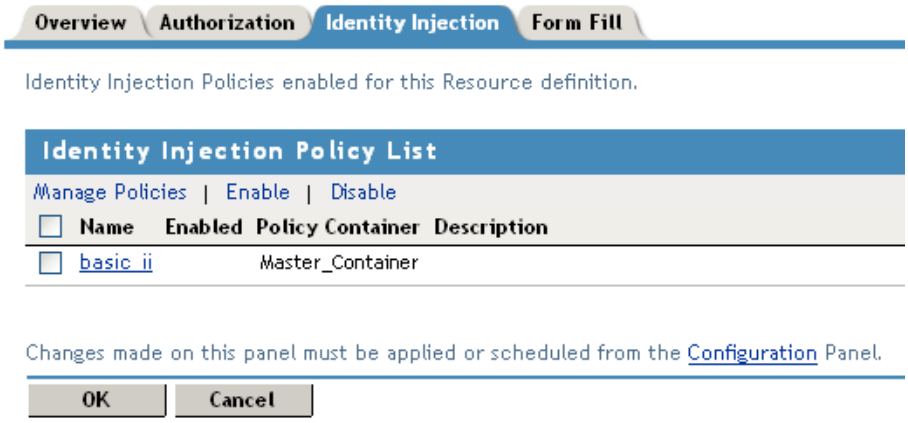
2 Configure the resource for the basic directory as described in Section 1.2, "Prerequisites for Setup," on page 10.

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*.



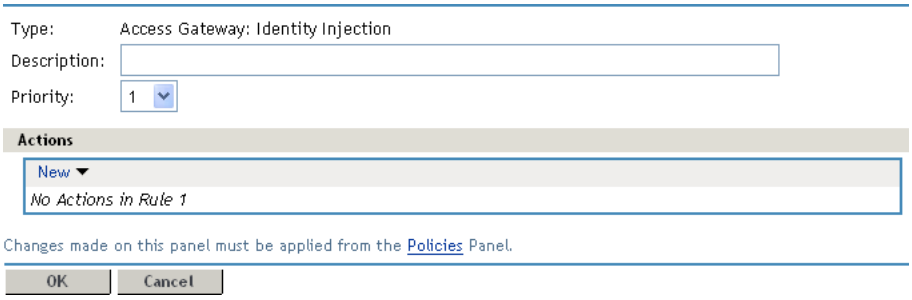
4 In the *Identity Injection Policy List* section, click *Manage Policies*.

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

Name: A name for the new 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*.
- For Password, select *Credential Profile* and *LDAP Credentials: LDAP Password*.

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

11 Click *Close*.

12 Select the new identity injection policy, then click *Enable*.

13 At the bottom of the page, select *Configuration Panel*, then click *OK*.

14 On the *Configuration* page, select *Apply Changes*, wait, then in the second pop-up, click *OK*.

15 To update the Identity Server, click *Identity Servers > Setup*, then click *Update Servers*.

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

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

Enabling SSL Communication

2

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.

The eDirectory that resides on the Administration Console is the main certificate store for all of the Access Manager components. This document describes using this local certificate authority (CA). By default, all Access Manager components (Identity Server, Access Gateway, SSL VPN, and J2EE Agents) trust the local CA. However, if the Identity Server is configured to use an SSL certificate signed externally, the trusted store of the embedded service provider for each component must be configured to trust this new CA.

This section discusses the following procedures:

2.1 Configuring Secure Communication on the Identity Server

The Identity Server comes with test-encryption, test-signing, test-connector, test provider, and test-consumer certificates. You must replace the test-connector certificate. This procedure shows you how to:

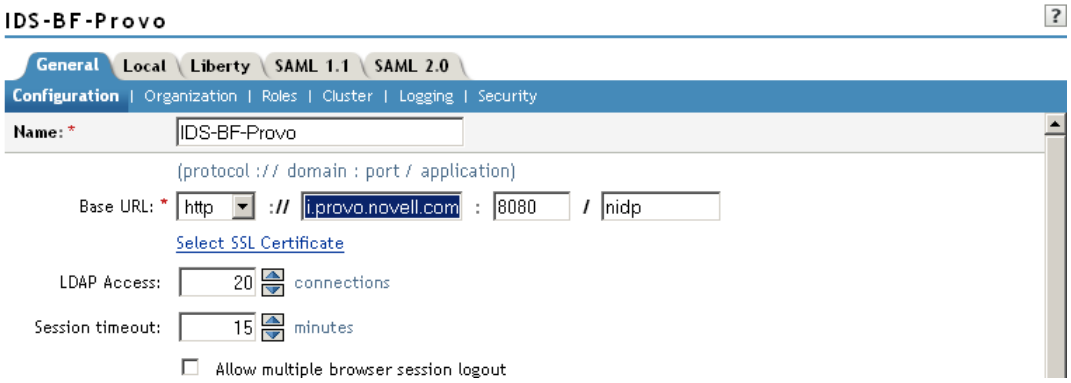
- Enable SSL on the Identity Server (changing from HTTP to HTTPS)
- Create a certificate
- Replace the test-connector certificate with the newly created one

  Whenever you replace a certificate for an Identity Server configuration, you must re-import the metadata associated with trusted providers. See "Reimporting a Trusted Provider's Metadata" in the *Novell Access Manager 3.0 Administration Guide*.
- Re-establish trust between the Access Gateway embedded service provider and the Identity Server.

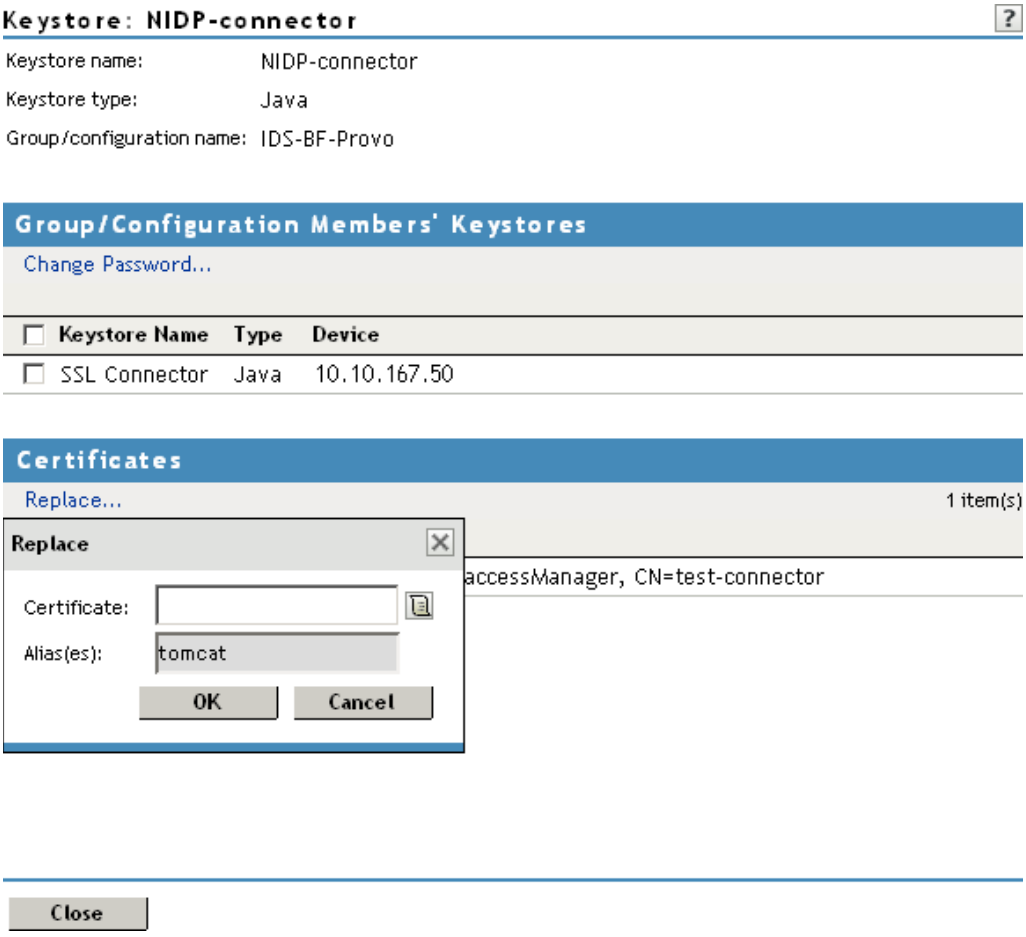
To configure SSL:

1. In the Administration Console, click *Access Manager* > *Identity Servers* > *Configuration*.
2. Change *Protocol* to HTTPS (the system changes the port to 8443).

3 Copy the domain name of your Identity Server configuration to the Clipboard, or take note of the name. It must match the common name of the new certificate.

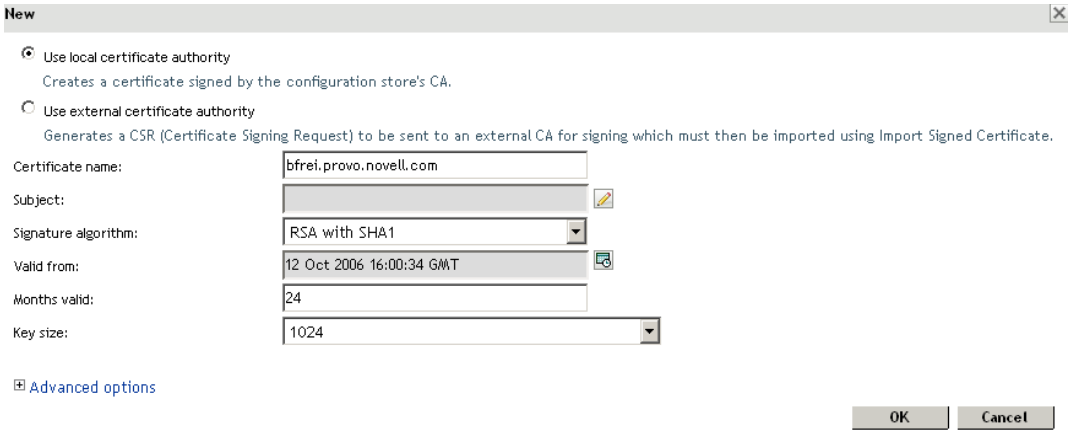


4 Click *Select SSL Certificate*, then click *Replace*.



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

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



7 Click *Use local certificate authority*.

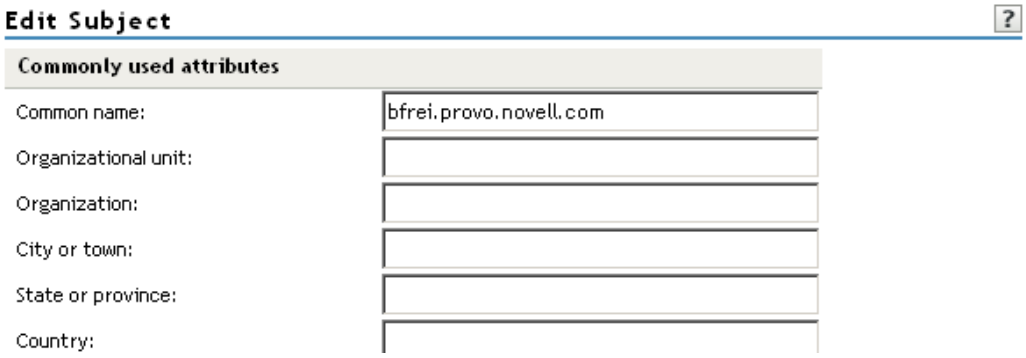
This option creates a certificate signed by the local CA (or Organizational CA), and creates the private key. For production environments, you can select *Use external certificate authority*, which generates a certificate that you must have signed by the external CA.

8 Fill in the following:

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

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

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

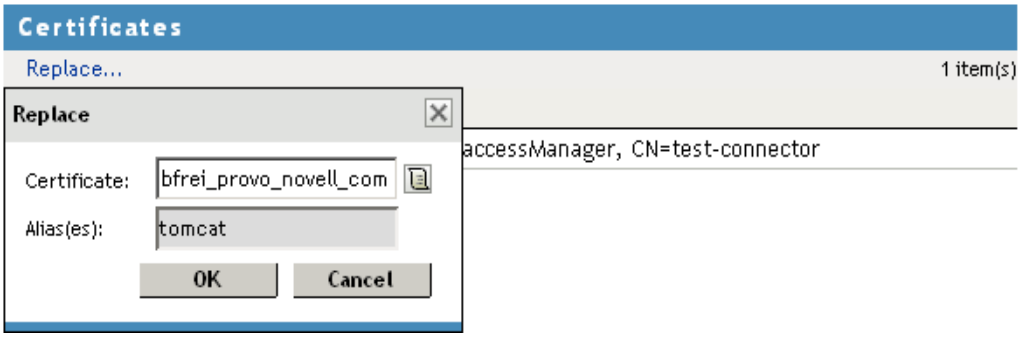


9 Click *OK*.

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

The new certificate is displayed on the Select Certificate page.

11 Click *OK*.



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

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

You should wait about thirty seconds for the restart, and then you can refresh the browser and log in to the Administration Console.

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

15 Click the *Setup* tab, then click *Update Servers*.

Re-establish Trust with the Access Gateway ESP

When you change the base URL of the Identity Server, including changing from HTTP to HTTPS, the trust model is broken between the Identity Server and the embedded service provider on the Access Gateway. You must reset this in the Access Gateway.

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

2 In the *Identity Server Configuration* option, select *None*.

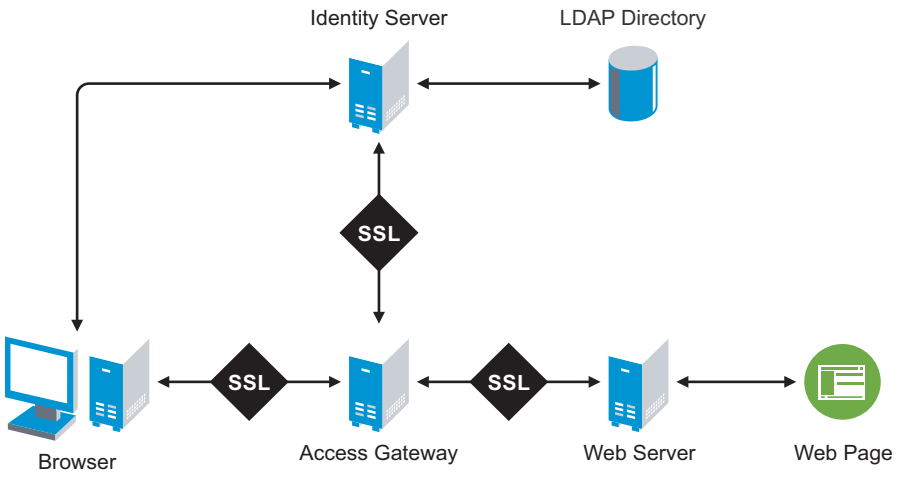
3 Click *OK* to apply the change.

4 In the *Identity Server Configuration* option, re-select the Identity Server configuration, then click OK.

2.2 Configuring the Access Gateway for SSL

You can configure the Access Gateway to use SSL in its connections to the Identity Server, to the browsers, and to its Web servers. Figure 2-1 illustrates these communication channels.

Figure 2-1 *Setting up SSL for the Access Gateway communication channels*



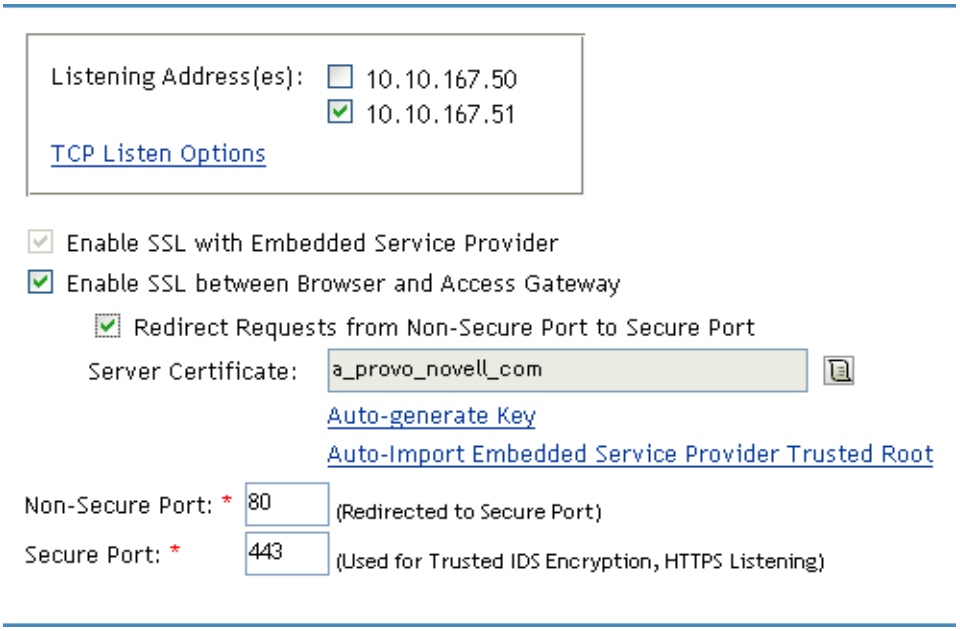
The Identity Server needs to be configured for SSL before configuring other devices to use it for authentication. See Section 2.1, “Configuring Secure Communication on the Identity Server,” on page 27.

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

- Section 2.2.1, “Configuring SSL Communication with the Browsers and the Identity Server,” on page 32
- Section 2.2.2, “Enabling SSL between the Reverse Proxy and its Web Servers,” on page 34

2.2.1 Configuring SSL Communication with the Browsers and the Identity Server

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



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

Enable SSL with Embedded Service Provider: Select this option to encrypt the data exchanged for authentication (the communication channel between the Identity Server and the Access Gateway). This option is only available for the reverse proxy which 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 data that the Access Gateways retrieves from the back-end Web servers to use a non-secure channel. This saves processing overhead if the data on the Web servers is not sensitive.

Enable SSL between Browser and Access Gateway: Select this option to require SSL connections between your clients and the Access Gateway. SSL must be configured between the browsers and the Access Gateway before you can configure SSL between the Access Gateway and the Web servers. For this process, see Section 2.2.2, "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 To auto-generate a certificate key using the Access Manager CA, click *Auto-generate Key*, then click *OK* twice. 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*, then in the pop-up, click *OK*.

Whenever you enable SSL or select a certificate, you need to restart the Access Gateway embedded service provider. That process is explained in Step 13, after you have completed all the required configuration changes.

6 Click *Protected Resources*.

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

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

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

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

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

10 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 configuration 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.

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

12 On the *Configuration* page, click *Apply Changes*, then in the pop-up window, click *OK*.

13 When the changes have been applied, restart the embedded service provider. Click *Access Gateways > [Name of Access Gateway] > Actions > Restart Service Provider >OK*.

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

15 (Optional) To test this configuration from a client browser, enter the published DNS name as the URL in the browser. For example, enter

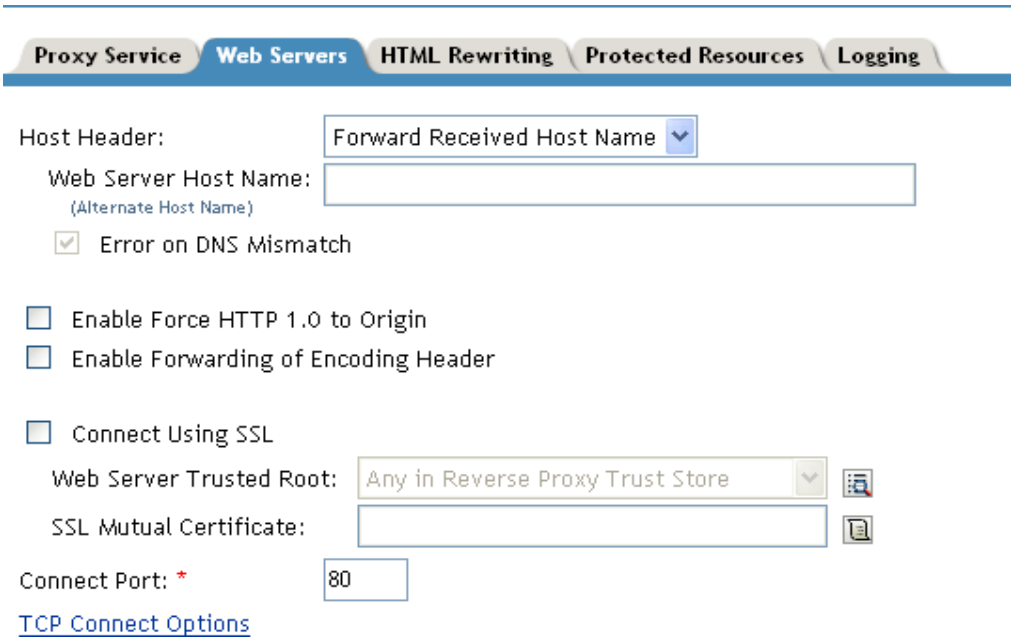
```
https://www.mytest.com
```

Click the links that require authentication for access.

2.2.2 Enabling SSL between the Reverse Proxy and its Web Servers

SSL must be enabled between the Access Gateway and the browsers before you can enable it between the Access Gateway and its Web servers.

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



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

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

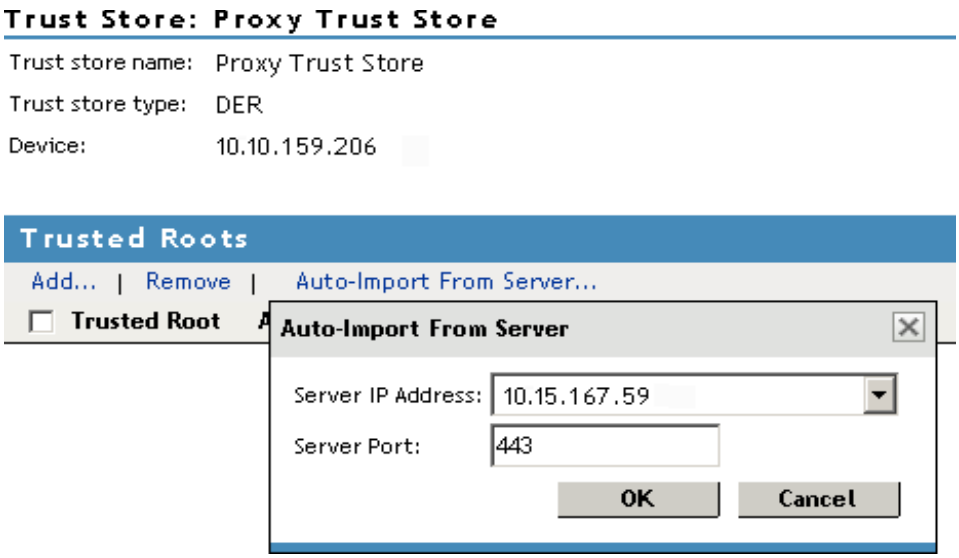
4 Configure how you want the certificate verified. The Access Gateway platforms support different options:

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

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

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

4c The auto import screen appears.



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

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

6 Click *OK*.

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

7 Specify an alias, then click *OK*.

All the certificates displayed are added to the trust store.

8 Click *Close*.

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

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

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

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

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

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

11 On the *Configuration* page, click *Apply Changes*, then in the pop-up window, click *OK*.

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:

`https://www.mytest.com`

Click the links that require authentication for access.

2.3 Configuring Access Manager to Use Certificates Signed Externally

By default, all Access Manager components (Identity Server, Access Gateway, SSL VPN, and J2EE Agents) trust the certificates signed by the local CA. However, if the Identity Server is configured to use an SSL certificate signed externally, the trusted store of the service provider for each component must be configured to trust this new CA. Import the public certificate of the CA into the following trust stores:

- For an Access Gateway, click *Access Manager > Access Gateways > [Edit] > Service Provider Certificates > Trusted Roots*.
- For a J2EE Agent, click *Access Manager > J2EE Agents > Edit > Trusted Roots*.
- For an SSL VPN server, click *Access Manager > SSL VPNs > Edit > SSL VPN Certificates > Trusted Root*.

If an Access Gateway, a J2EE Agent, or an SSL VPN server is configured to use an SSL certificate signed externally, the trusted store of the Identity Server must be configured to trust this new CA. Import the public certificate of the CA into the Identity Server configuration that the component is using for authentication.

In the Administration Console, click *Access Manager > > Identity Servers > [Configuration Assignment] > Security > NIDP Trust Store* and add the certificate to the Trusted Roots list.

NOTE: Whenever you replace certificates on a device, you must update the Identity Server configuration (by clicking *Update Servers* on the Setup page) and restart the embedded service provider of the Access Gateway, J2EE Agent, or SSL VPN server.

Configuring SSL VPN to Protect an Application

3

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

3.1 Prerequisites

- You have installed the SSL VPN server. See “Installing SSL VPN” in the *Novell Access Manager 3.0 Installation Guide*.
- You have configured a basic Access Manager system with a functional Identity Server and Access Gateway. See Chapter 1, “Setting Up a Basic Access Manager Configuration,” on page 9.
- You have configured some Identity Server roles. The roles you create depend upon the requirements of your application. See “Creating Roles” in the *Novell Access Manager 3.0 Administration Guide*.

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

- You have a TCP-based application that you want to protect with SSL VPN. To do this on an example Web server, see “Configuring the SSL VPN as a Protected Resource” in the *Novell Access Manager 3.0 Digital Airlines Example Documentation*.

3.2 Accelerating SSL VPN

The SSL VPN server requires a user credential profile consisting of the following elements:

- Username and password information
- A proxy session cookie
- The roles assigned to the current user for authentication information

Each element added to the custom header requires a name with an “X-” prefix. The name you enter is specific to the application using the custom header, and might be case sensitive. You need to obtain this information from the application before creating the custom header.

The SSL VPN server requires the following three headers:

- Authentication header containing the username and password credential profile

- Custom header containing a proxy session cookie element named X-SSLVPN-PROXY-SESSION-COOKIE
- Custom header containing roles for current user element, named X-SSLVPN-ROLE

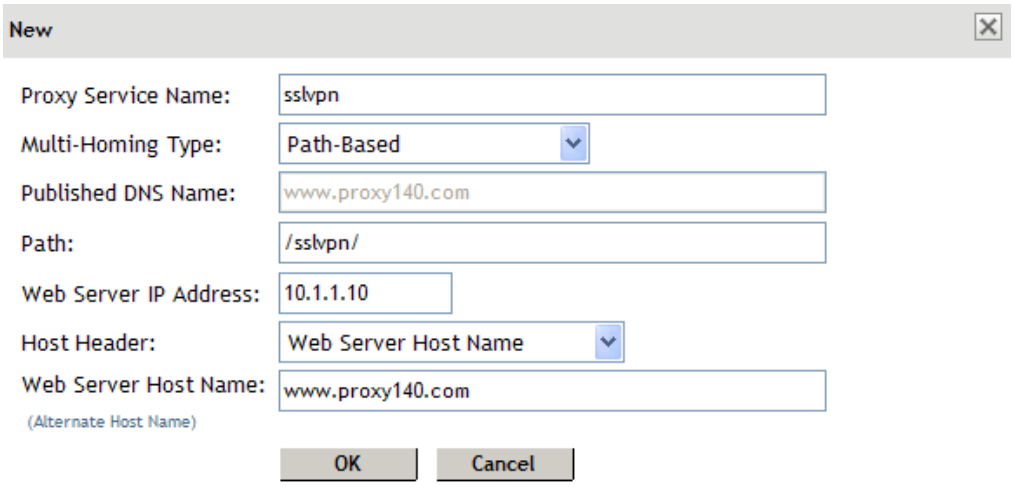
The policy engine allows you to add these and other elements to a custom header and the reverse proxy injects these headers into the SSL VPN server.

3.3 Injecting the SSL VPN Header

The example in this section explains how to accelerate SSL VPN server in a Path-Based Multi-homing configuration.

Before you begin, make sure you have already created a proxy service and an authentication procedure. For more information on creating proxy service and authentication procedure, see Section 1.4.1, “Configuring a Reverse Proxy,” on page 16.

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



3. Fill in the following fields.

   Proxy Service Name: Specify a name for proxy service.

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

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

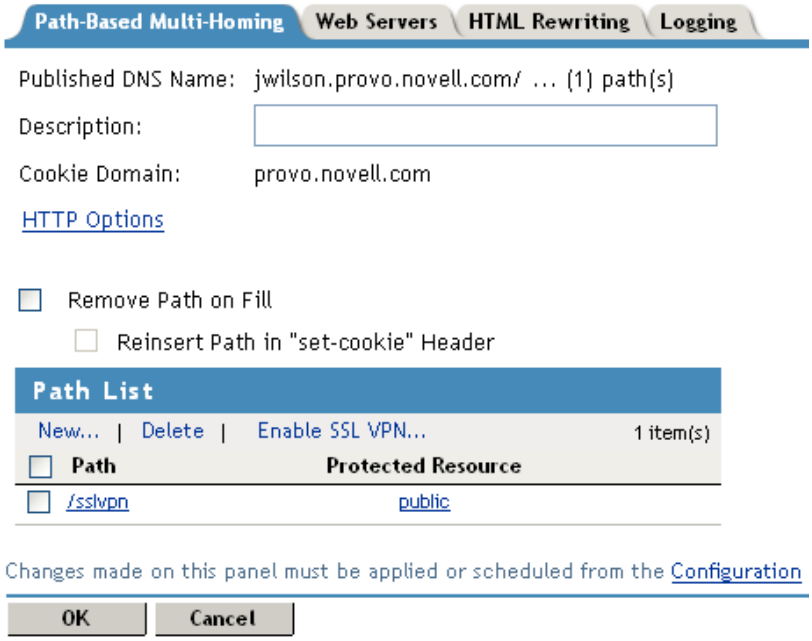
   Path: Specify the URL to the SSL VPN resource as `/sslvpn/`

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

   Host Header: Specify a host header name. This name is forwarded to the Web server in the host header.

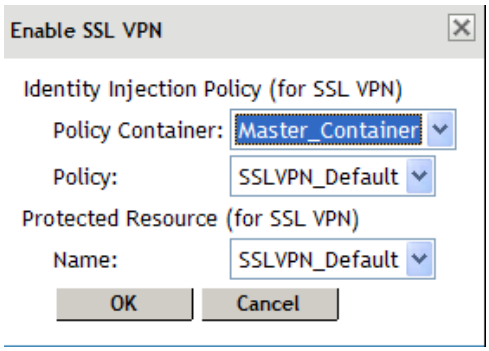
   Web Server Host Name: Specify the alternate host name.
4. Click *OK*.

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



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

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



8 Fill in the following fields:

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

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

10 Select the *Web Servers* tab.

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

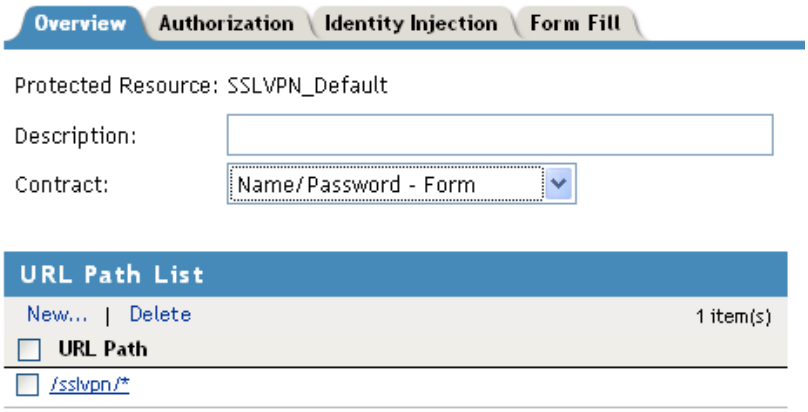
12 In the *Proxy Service List* section, click the name of the parent proxy service of the newly created SSL VPN proxy service. This host does not have a multi-homing value.

13 Select the *Protected Resources* tab.

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

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

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



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

---

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

18 On the *Configuration* page, select *Apply Changes*, then click *OK*.

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

20 Click *Close*.

Clustering Identity Servers

4

To add capacity and for failover, you can cluster a group of Identity Servers and configure them to act as a single server. A cluster of Identity Servers should reside behind an L4 switch. Clients access the virtual IP (VIP) 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, 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.

Authentication Server

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

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

Prerequisites

- ❑ An L4 server installed. You can use the same server for Identity Server clustering and Access Gateway clustering, provided that you use different virtual IPs. The LB algorithm can be anything (hash/sticky bit), defined at the Real server level.
- ❑ Persistence (sticky) sessions enabled on the L4 server. Normally you 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 an Identity Server Configuration (Advanced Options)" in the *Novell Access Manager 3.0 Administration Guide* for information about creating an Identity Server configuration. See "Assigning an Identity Server to a Configuration" in the *Novell Access Manager 3.0 Administration Guide* for information about assigning identity servers to configurations.

  The base URL DNS name of this configuration must resolve via DNS to the IP address of the L4 virtual IP address. The L4 balances the load between the identity servers in the cluster.
- ❑ Ensure that the L4 administration server using port 8080 has the following ports open:
  - 8443 (secure Administration Console)
  - 7801 (TCP)
  - 636 (for secure LDAP)
  - 389 (for clear LDAP, loopback address)
  - 524 (network control protocol on the L4 machine for server communication)

  The identity provider ports must also be open:
  - 8080 (nonsecure login)

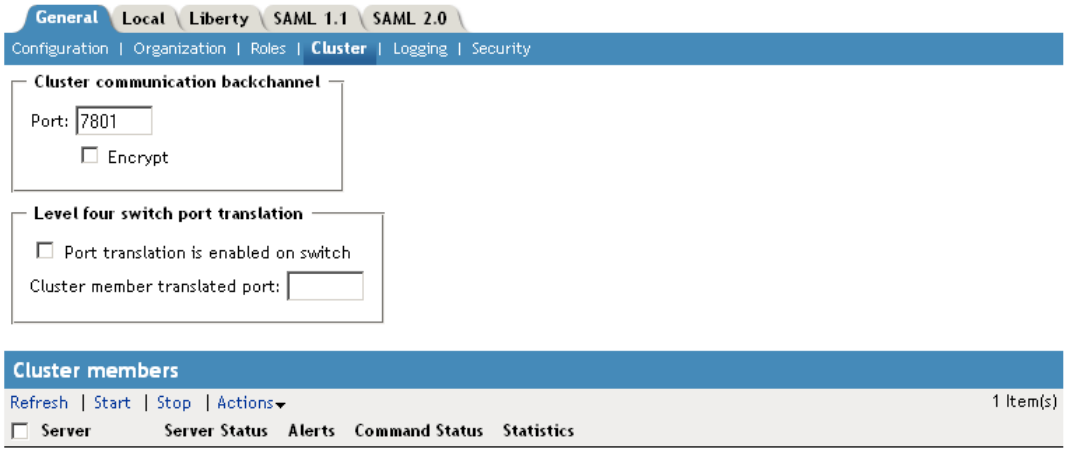
- 8443 (secure login)
- 1443 (server communication)

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

Setup

1. Install the additional Identity Servers.

   During installation, choose option 2, *Install Novell Identity Server*, from CD 1 of the Access Manager installation discs. You run the installation for each new Identity Server you want to add. 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 configuration.
3. Click the configuration name you created for the cluster under *Configuration Assignment*.
4. Click *Cluster*.



5. Fill in the following fields as required:

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

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

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

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

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

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

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

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

Real Server Settings Example

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

Configuring Access Gateways for Fault Tolerance

5

You can create a group of Access Gateways and configure them to act as a single server. A group of Access Gateways should reside behind a Layer 4 switch (L4). Clients access the virtual IP on the L4, and the L4 alleviates server load by balancing traffic across the group 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 group, as traffic necessitates.

Figure 5-1 *Grouping Access Gateways*

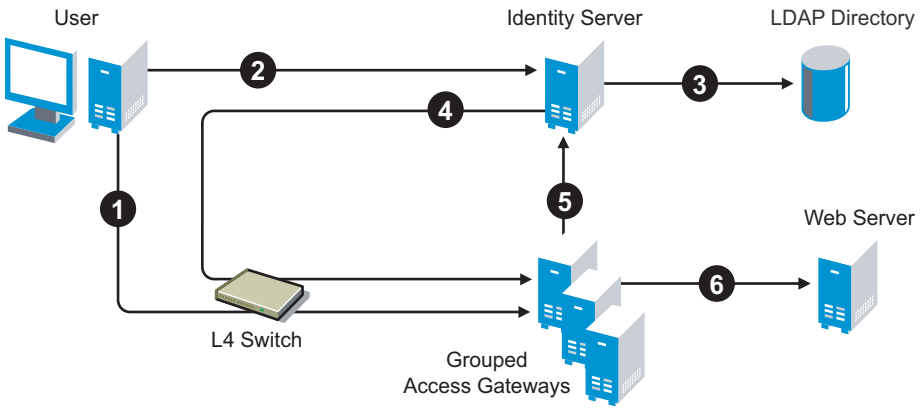


Figure 5-1 illustrates the flow of a user request when the Access Gateways are grouped behind an L4 switch.

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 group.
2. The Access Gateway redirects the request to the Identity Server for authentication. The Identity Server presents the user with a login page, requesting a user name and a password.
3. The Identity Server verifies the user's credentials with the directory.
4. The validated credentials are sent through the L4 switch to the same Access Gateway that first received the request
5. The Access Gateway verifies the user credentials with the Identity Server
6. If the credentials are valid, the Access Gateway forwards the request to the Web server.

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

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

- Section 5.1, "Prerequisites," on page 46
- Section 5.2, "Configuring a Group," on page 46

5.1 Prerequisites

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

  When you install each new Access Gateway, configure it to use the same Administration Console.
- Your DNS server needs to be configured to resolve the published DNS names that you specify for your proxy services to the L4 switch.
- Persistent (sticky) sessions enabled 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 group, 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 group. If you have created configurations for the other servers in the group, these configurations are overwritten.

5.2 Configuring a Group

To create a new group:

1. In the Administration Console, click *Access Manager > Access Gateways > Groups* tab.
2. Click *New* and fill in the following fields:
   - **Group Name:** Specify a display name for the group.
   - **Type:** Select whether the group contains NetWare Access Gateways or Linux Access Gateways. A group cannot contain a mixture of these two types.
   - **Group Description:** (Optional) Provide a description of the purpose of this group.
3. In the *Server Name* list, select the servers that you want to be members of the group.

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

   Each server you add to the group adds about 30 seconds to the time it takes to configure the group because certificates must be synchronized and configuration options must be sent to that server. If you create a very large group of twenty servers, it can take up to ten minutes to configure and create the group.
4. In the *Primary Cluster Server* field, select the server that is to be the primary server in the cluster.

   The list is empty until you select the servers for the group. The configuration of the primary server is pushed to the other servers in the group. If any of the selected servers have been configured, their configurations are lost.
5. Click *OK*.
6. After the group has been created, each server in the group needs be restarted.
7. To configure the group, click *Access Gateways > Edit: [Name of Group]*.

   A group 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 group.

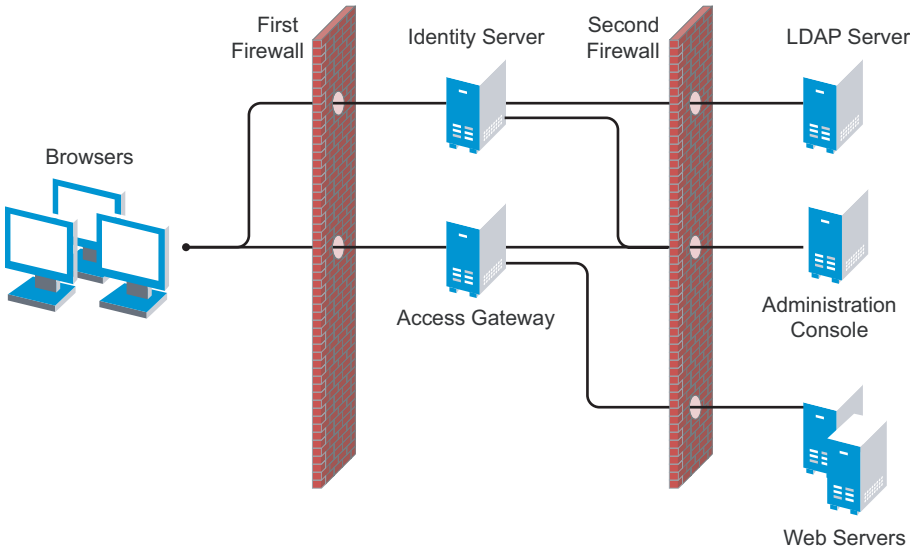
Applying the configuration to a group is slightly different. You have the option of applying the changes to all servers in the group, or to apply it to one server before selecting another server in the group. See "Applying Configuration Changes to a Group" in the *Novell Access Manager 3.0 Administration Guide*.

Setting Up Firewalls

6

Access Manager is not a firewall; it should be used with firewalls. Figure 6-1 illustrates a simple firewall set up for the basic Access Manager configuration of an Identity Server, an Access Gateway, and an Administration Console.

Figure 6-1 *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 6.1, “Required Ports,” on page 49
- Section 6.2, “Sample Configurations,” on page 56

6.1 Required Ports

The following tables list the ports that need to be opened when a firewall separates one component from another. The tables are redundant, in that some combinations appear in more than one table, but this allows you to discover the required ports whether you are thinking that the firewall is separating an Access Gateway from the Administration Console or that 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 6-1, “When a Firewall Separates an Access Manager Component from a Global Service,” on page 50
- Table 6-2, “When a Firewall Separates the Administration Console from a Component,” on page 50

- Table 6-3, “When a Firewall Separates the Identity Server from a Component,” on page 51
- Table 6-4, “When a Firewall Separates the Access Gateway from a Component,” on page 52
- Table 6-5, “When a Firewall Separates the SSL VPN from a Component,” on page 54
- Table 6-6, “When a Firewall Separates the J2EE Agent from a Component,” on page 55

Table 6-1 *When a Firewall Separates an Access Manager Component from a Global Service*

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

Table 6-2 *When a Firewall Separates the Administration Console from a Component*

Component	Port	Description
Access Gateway, Identity Server, SSL VPN, or J2EE Agent	TCP 1443	For communication from the Administration Console to the devices.
	TCP 8444	For communication from the devices to the Administration Console.
	TCP 289	For communication from the devices to the Novell Audit server on the Administration Console.
	TCP 524	For NCP certificate management with NPKI from the devices to the Administration Console.
	TCP 636	For secure LDAP communication from the devices to the Administration Console.

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

Table 6-3 *When a Firewall Separates the Identity Server from a Component*

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

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

Table 6-4 *When a Firewall Separates the Access Gateway from a Component*

Component	Port	Description
Identity Server	TCP 8080 or 8443	For authentication communication from the Access Gateway to the Identity Server. TCP 8080 and 8443 are the default ports. They are configurable. You need to open the port of the Base URL of the Identity Server. See "Translating the Identity Server Configuration Port" in the *Novell Access Manager 3.0 Administration Guide*.
Administration Console	TCP 1443	For communication from the Administration Console to the Access Gateway. This is configurable.
	TCP 8444	For communication from the Access Gateway to the Administration Console.
	TCP 289	For communication from the Access Gateway to the Novell Audit server on the Administration Console.
	TCP 524	For NCP certificate management with NPKI from the Access Gateway to the Administration Console.

Component	Port	Description
	TCP 636	For secure LDAP communication from the Access Gateway to the Administration Console.
SSL VPN	TCP 8080	For HTTP communication from the Access Gateway to the SSL VPN.
	TCP 8443	If SSL has been enabled between the Access Gateway and the SSL VPN, TCP 8443 needs to be opened for HTTPS communication from the Access Gateway to the SSL VPN.
J2EE Agent	Only required if the Access Gateway is configured to protect the J2EE server as a Web server.	
	TCP 8080, 8443	For communication from the Access Gateway to the JBoss server. These are the default ports. They are configurable.
	TCP 9080, 9443	For communication from the Access Gateway to the WebSphere server. These are the default ports. They are configurable.
	TCP 7001, 7002	For communication from the Access Gateway to the WebLogic server. These are the default ports. They are configurable.
Access Gateway	Not a supported configuration. All members of an Access Gateway group need to be on the same side of the firewall.	
Browsers/Clients	TCP 80	For HTTP communication from the client to the Access Gateway. This is configurable.
	TCP 443	For HTTPS communication from the client to the Access Gateway. This is configurable.
	UDP 8880	For RDB communication from the client to the Access Gateway. Only required if you enable RDB on the NetWare Access Gateway
	TCP 23	For Telnet communication from the client to the Access Gateway. Only required if you enable Telnet on the NetWare Access Gateway.
	TCP 21	For FTP communication from the client to the Access Gateway. Only required if you enable Mini FTP on the NetWare Access Gateway.
	TCP 524	For SFTP communication from the client to the Access Gateway. Only required if you load the ncpip.nlm for SFTP on the NetWare Access Gateway.
Web Servers	TCP 80	For HTTP communication from the Access Gateway to the Web servers. This is configurable.
	TCP 443	For HTTPS communication from the Access Gateway to the Web servers. This is configurable.

Table 6-5 *When a Firewall Separates the SSL VPN from a Component*

Component	Port	Description
Access Gateway	TCP 8080	For HTTP communication from the Access Gateway to the SSL VPN.
	TCP 8443	If SSL has been enabled between the Access Gateway and the SSL VPN, TCP 8443 needs to be opened for HTTPS communication from the Access Gateway to the SSL VPN.
Identity Server	N/A. The SSL VPN never communicates directly with the Identity Server.	
Administration Console	TCP 1443	For communication from the Administration Console to the SSL VPN. This is configurable.
	TCP 8444	For communication from the SSL VPN to the Administration Console.
	TCP 289	For communication from the SSL VPN to the Novell Audit server on the Administration Console.
	TCP 524	For NCP certificate management with NPKI from the SSL VPN to the Administration Console.
	TCP 636	For secure LDAP communication from the SSL VPN to the Administration Console.
J2EE Agent	N/A. The SSL VPN never communicates with the J2EE Agent.	
Browsers	TCP 7777	This is the default port for access to the SSL VPN, but it can be configured to use TCP 443.
SOCKS server	TCP 2010	For SOCKS communication from SSL VPN to the SOCKS server. This port is configurable.
Application Servers (E-mail, Telnet, Thin Client, etc.)	TCP 22	For SSH communication from the SSL VPN to the application server.
	TCP 23	For Telnet communication from the SSL VPN to the application server.
	Application ports	Specific to the application SSL VPN is providing access to.

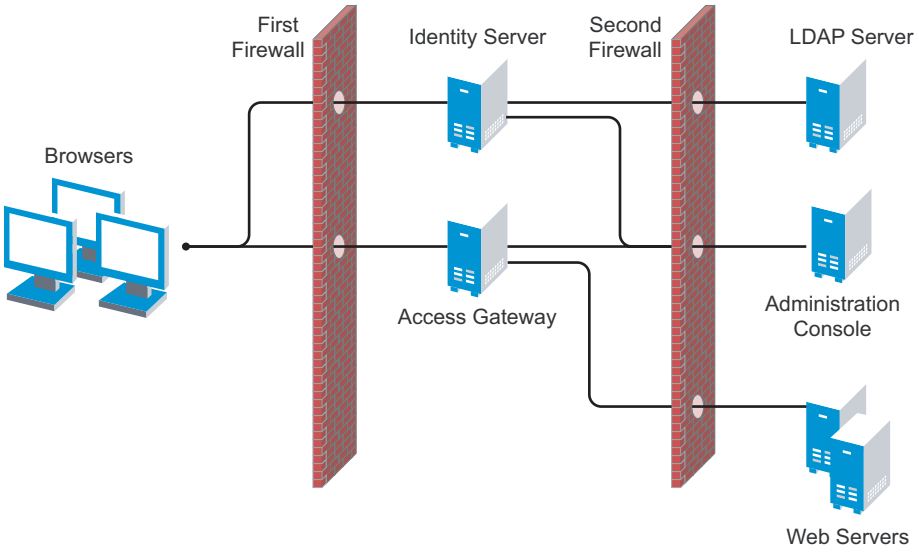
Table 6-6 *When a Firewall Separates the J2EE Agent from a Component*

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

6.2 Sample Configurations

6.2.1 The Access Gateway and Identity Server in the DMZ

Figure 6-2 *The Identity Server and the Access Gateway in the Same Firewall Zone*



First Firewall

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

Table 6-7 *Ports to Open in the First Firewall*

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

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

Second Firewall

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

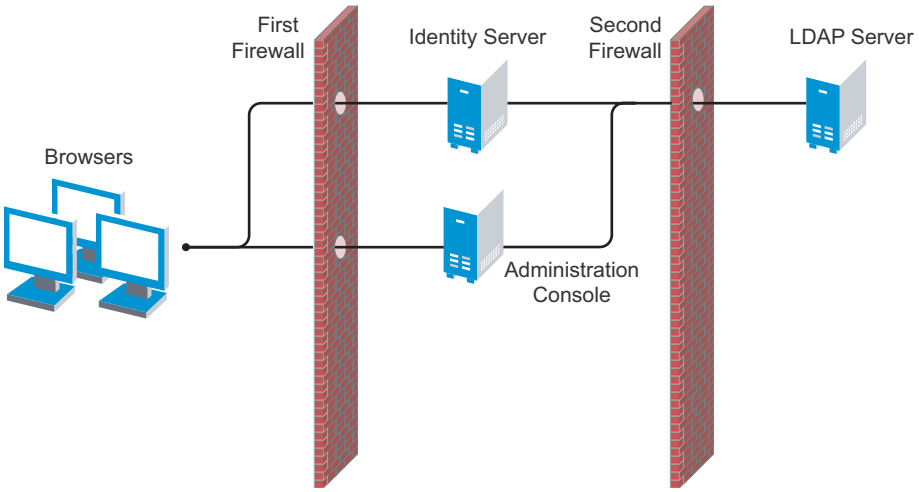
Table 6-8 *Ports to Open in the Second Firewall*

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

6.2.2 A Firewall Separating Access Manager Components from the LDAP Servers

You can configure your Access Manager components so that your Administration Console is on the same side of the firewall as your Access Manager components and have a firewall between them and the LDAP servers, as illustrated in Figure 6-3.

Figure 6-3 *A Firewall Separating the Administration Console and the LDAP Server*



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

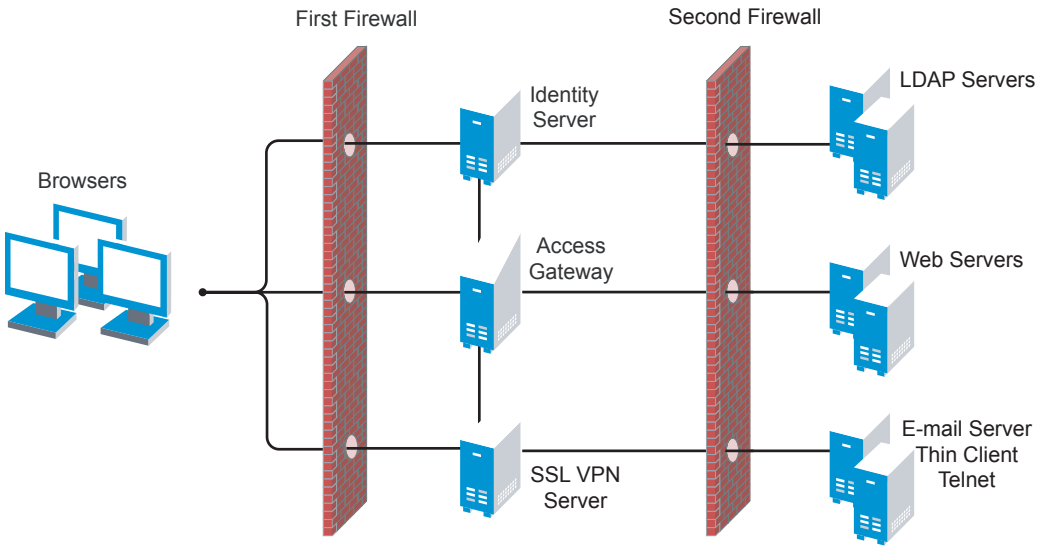
Table 6-9 *Ports to Open in the Second Firewall*

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

6.2.3 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 6-4 *SSL VPN Server and Firewalls*



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

Table 6-10 *Ports to Open in the First Firewall for SSL VPN*

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

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

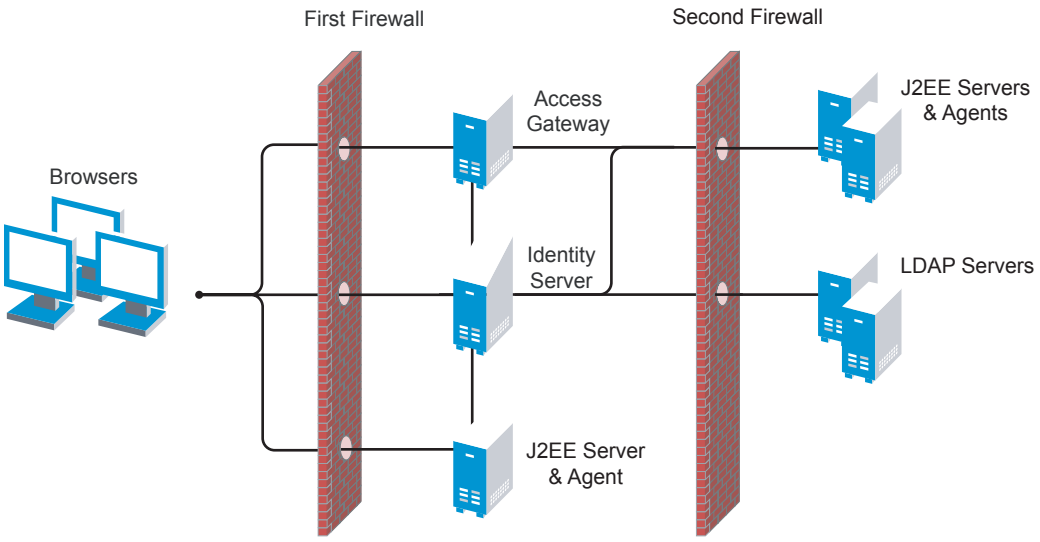
Table 6-11 *Ports to Open in the Second Firewall for SSL VPN*

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

6.2.4 Configuring the Firewall for the J2EE Agent

The J2EE Agent is installed on a J2EE server running either JBoss or WebSphere. You can configure it to be a protected resource of the Access Gateway or you can allow direct access. Figure 6-5 illustrates these configurations.

Figure 6-5 *J2EE Agent and Firewalls*



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

Table 6-12 *Ports to Open in the First Firewall for the J2EE Agent*

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

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

Table 6-13 *Ports to Open in the Second Firewall for the J2EE Agent*

Port	Purpose
TCP 8080	For non-secure connections to a JBoss server.

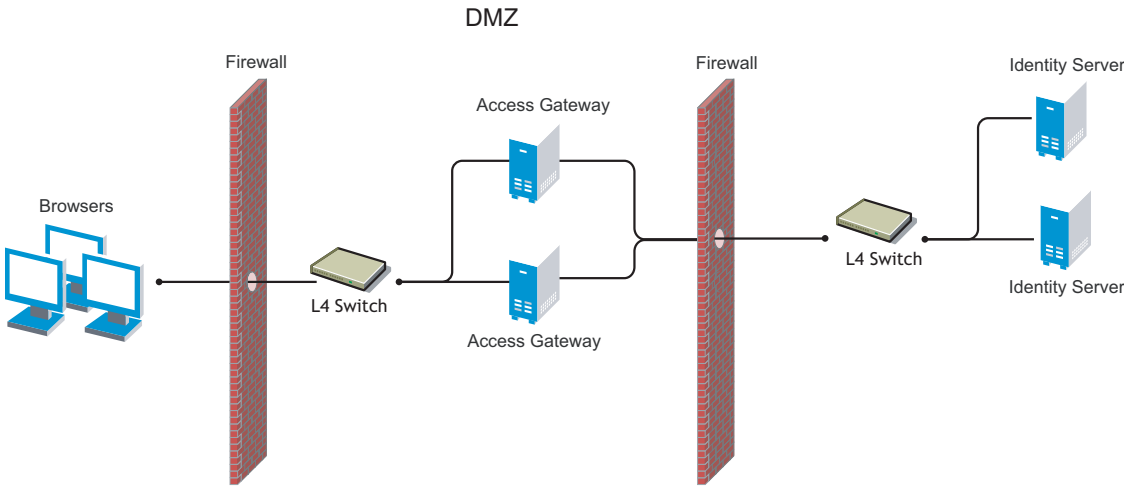
Port	Purpose
TCP 8443	For secure connections to a JBoss server.
TCP 9080	For non-secure connections to a WebSphere server.
TCP 9443	For secure connections to a WebSphere server.
TCP 7001	For non-secure connections to a WebLogic server.
TCP 7002	For secure connections to a WebLogic server.
TCP 8080 or 8443	For authentication communication. The port of the Base URL of the Identity Server needs to be open.

Protecting an Identity Server with an Access Gateway

7

For security reasons, you might want to set up your Access Manager configuration so that the Identity Server (and user store) is a resource protected by an Access Gateway. Such a 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*



The following features are not supported in this configuration:

- The Identity Server cannot respond to Identity Provider introductions.
- The proxy service that is protecting the Identity Server cannot be configured to use mutual SSL.

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

1. Change the port of the Base URL of the Identity Server to 80. If you are using SSL, use port 443. See Creating an Identity Server Configuration (http://www.novell.com/documentation/novellaccessmanager/adminguide/data/b59br8f.html#b59br8f) .

   In this configuration, the domain name of the Base URL must match the public DNS of the proxy service set up in the Access Gateway.

2. Set up a proxy service on the Access Gateway for the Identity Server. See "Creating a Reverse Proxy and Proxy Service" in the *Novell Access Manager 3.0 Administration Guide*.

   When creating the proxy service, set the following fields to the specified values:

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

The reverse proxy and proxy service combination can be used as the authentication proxy service. If proxy service is not the first proxy service of the reverse proxy, you can use either domain-based or path-based multi-homing. If you select path-based, the *Path* must be set to /nidp and the *Remove Path on Fill* option should not be selected.

3. Configure a protected resource for the proxy service. See "Configuring Protected Resources" in the *Novell Access Manager 3.0 Administration Guide*.

   Set the *Contract* field to *None*. The Identity Server needs to be set up as a public resource.

   Set the *URL Path* of the protected resource to /nidp/*.

4. Configure the Web servers of the proxy service. See "Configuring the Web Servers of a Proxy Service" in the *Novell Access Manager 3.0 Administration Guide*.

   Set the *Connect Port* to 8080 for clear text or to 8443 for SSL.

5. Create a host entry for the Identity Server. See "Configuring Hosts" in the *Novell Access Manager 3.0 Administration Guide* and add the DNS name of the Base URL of the Identity Server to the list.

   If your Access Gateway belongs to a group, make an entry for each Access Gateway in the group.

6. Configure the Pin List so that the Identity Server pages are not cached. In the list, create a *URL Mask* of /nidp/* and set the *Pin Type* to *Bypass*. See "Configuring a Pin List" in the *Novell Access Manager 3.0 Administration Guide*.

7. Set up the Access Gateway to use SSL between the browsers and the Access Gateway. See "Configuring SSL Communication with the Browsers and the Identity Server " in the *Novell Access Manager 3.0 Administration Guide*.

8. Set up SSL between the proxy service that is protecting the Identity Server and the Identity Server. See "Configuring SSL between the Proxy Service and the Web Servers" in the *Novell Access Manager 3.0 Administration Guide*. Use the following settings:

   - Select the *Connect Using SSL* option
   - Configure a *Web Server Trusted Root*.
   - Do not configure an *SSL Mutual Certificate*.
   - Set the *Connect Port* to 8443.

9. Create a wildcard certificate to be used by the Identity Server and the Access Gateway, and assign the certificate to both servers.

   For example, `*.novell.com`, where the Identity Server DNS is `idp.novell.com` and the Access Gateway DNS is `esp.novell.com`.

10. If necessary, set up SSL between the firewall and L4 switch. This must be done for each firewall/L4 used in the configuration.