Novell Access Manager

3.0

www.novell.com

DIGITAL AIRLINES EXAMPLE

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 7

1 Installation Overview 9

1.1 Installation Architecture . . . 10
1.2 Deployment Steps . . . 11
1.3 Prerequisites . . . 11
1.4 Installing Apache and PHP Web Server Components . . . 12
1.5 Installing Digital Airlines Components . . . 13

2 Configuring Digital Airlines 15

3 Implementing Example Web Services 19

3.1 Enabling an Authentication Procedure . . . 19
3.2 Accessing the Corporate Mail Portal . . . 21
3.3 Accessing the Medical Benefits Portal . . . 22
3.4 Configuring a User Policy . . . 22
3.4.1 Adding a Description to Your Configuration . . . 23
3.4.2 Creating a Sales Role . . . 24
3.4.3 Assigning the Sales Role in the Access Gateway Configuration . . . 26
3.5 Creating a New User with a Sales Role . . . 29
3.6 Configuring an Identity Injection Policy . . . 30
3.6.1 Disabling Restrictive Access Policies . . . 34
3.7 Initiating a VPN Session . . . 35
3.7.1 Configuring the SSL VPN as a Protected Resource . . . 36
3.7.2 Creating an SSL VPN Protected Resource . . . 36
3.7.3 Configuring the SSL VPN Identity Injection Policies . . . 37
3.7.4 Testing the SSL VPN Basic Configuration . . . 39
3.7.5 Configuring a Traffic Policy . . . 40

4 Modifying the Digital Airlines Example 43

4.1 Prerequisites . . . 43
4.2 Understanding the Example Files . . . 43
4.3 Updating Static Graphics . . . 44
4.4 Updating Mouse-Over Links . . . 46
4.5 Deploying Your Updated Example Web Service . . . 47

About This Guide

The Digital Airlines Example is designed to help network administrators understand the basic concepts of Novell® Access Manager by installing and configuring a relatively simple implementation of the software. The example serves as a primer for a more comprehensive production installation of Access Manager. The document consists of the following sections:

- Chapter 1, "Installation Overview," on page 9
- Chapter 2, "Configuring Digital Airlines," on page 15
- Chapter 3, "Implementing Example Web Services," on page 19
- Chapter 4, "Modifying the Digital Airlines Example," on page 43

Audience

This guide is intended for experienced network administrators who understand identity-based Web security services, such as Novell iChain™.

Feedback

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

Documentation Updates

For the most recent version of the *Airlines Example*, visit the Novell Access Manager Demos Wiki site (http://developer.novell.com/wiki/index.php/Nam-demos).

Additional Documentation

For documentation on other Novell Access Manager topics, see the Access Manager Documentation Web site (http://www.novell.com/documentation/lg/novellaccessmanager/index.html). You might also reference other information related to identity-based Web services, including the Novell iChain Web site (http://www.novell.com/documentation/ichain23/index.html).

Documentation Conventions

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

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

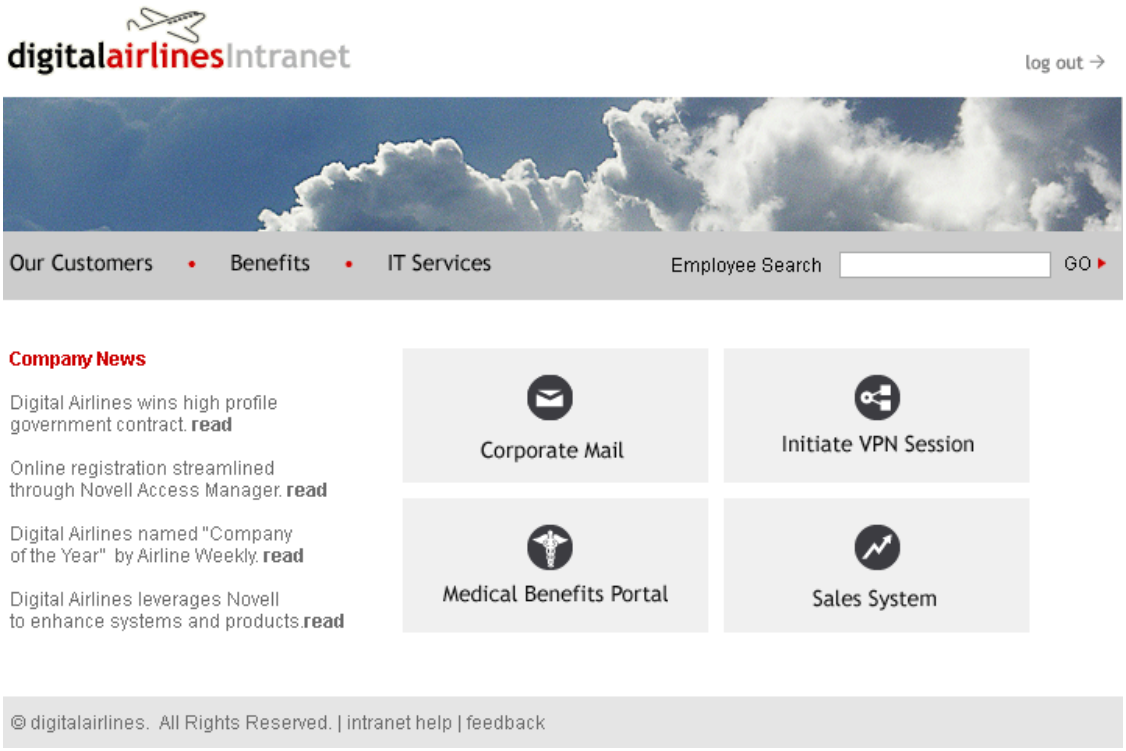
When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux or UNIX, should use forward slashes as required by your software.

Installation Overview

1

This document explain how to use Access Manager to protect a sample Web site as shown in Figure 1-1:

Figure 1-1 *Digital Airlines Web Services*



The first page of the Digital Airlines Example Web site is a public page, while the links to *Corporate Mail*, *Medical Benefits Portal*, *Initiate VPN Session*, and *Sales System* are protected Access Manager resources.

Before installing this example, you should already be familiar with the components and process flow that make up a basic Access Manager configuration. For more information, see the *Novell Access Manager 3.0 Setup Guide*.

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

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

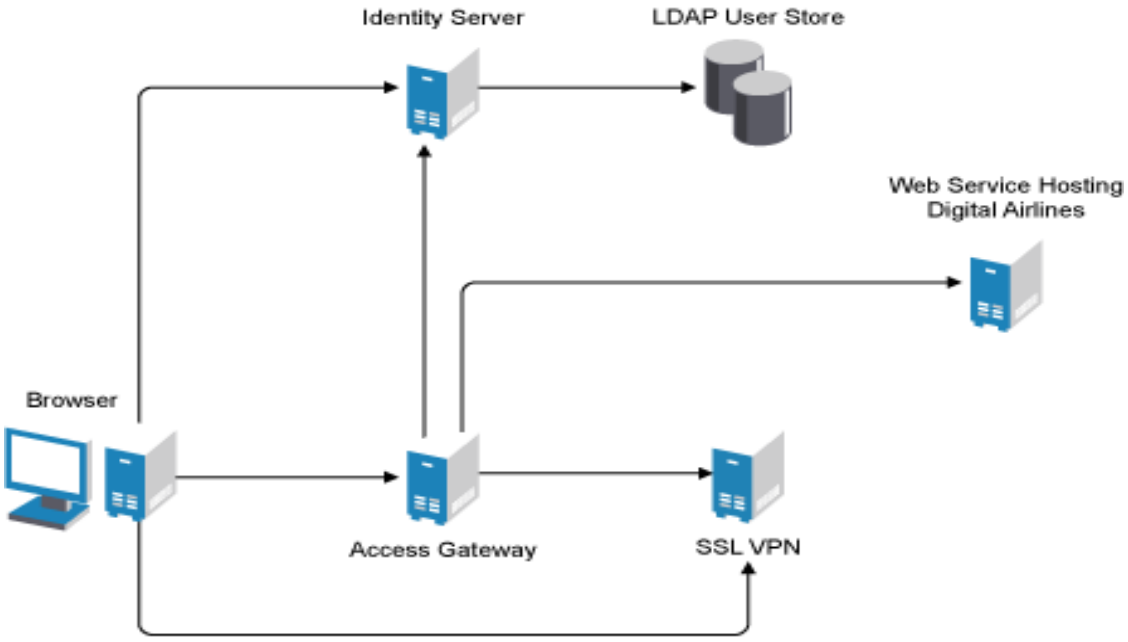
- Section 1.1, “Installation Architecture,” on page 10
- Section 1.2, “Deployment Steps,” on page 11
- Section 1.3, “Prerequisites,” on page 11

- Section 1.4, “Installing Apache and PHP Web Server Components,” on page 12
- Section 1.5, “Installing Digital Airlines Components,” on page 13

1.1 Installation Architecture

The high-level architectural diagram below illustrates how the example Digital Airlines service provider is integrated into the Access Manager schema. The diagram shows how the Digital Airlines example can be hosted on separate Web servers, including virtual servers.

Figure 1-2 *Digital Airlines Architecture*



This documentation describes hosting the Digital Airlines Web service and the Identity Server on a single machine and the Access Gateway on a second machine, as summarized in the table below:

Table 1-1 *Novell Access Manager Components and External Components**

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

The simplified configuration described in this document is just one of a number of possible installation options. Your actual configuration of the Digital Airlines example depends on how you installed your Access Manager components. For a more detailed explanation of how data flows between components, “Understanding an Access Manager Configuration” in the *Novell Access Manager 3.0 Setup Guide*.

After deploying the Digital Airlines example, you should understand the concepts required to deploy Access Manager in a number of other configurations. In a production environment, install the necessary Access Manager components according to your specific requirements. For more

information about other possible installation configurations, see "Setting Up a Basic Access Manager Configuration" in the *Novell Access Manager 3.0 Setup Guide*.

1.2 Deployment Steps

To deploy the Digital Airlines example, you must perform the following tasks:

1. Previously install the Novell Access Manager Administration Console, Identity Server, Access Gateway, and SSL VPN as described in the *Novell Access Manager 3.0 Installation Guide*.
2. Meet the system requirements for all Access Manager components. See Section 1.3, "Prerequisites," on page 11.
3. Download the Digital Airlines (`htdocs.tar.gz`) example directory from the Novell Access Manager Demos Wiki site (http://developer.novell.com/wiki/index.php/Nam-demos).
4. Install the example components as described in Section 1.5, "Installing Digital Airlines Components," on page 13.
5. Configure the example Web server, as described in Chapter 2, "Configuring Digital Airlines," on page 15.
6. Test the Access Gateway-protected example Web service, as described in Chapter 3, "Implementing Example Web Services," on page 19.
7. (Optional) Modify the Digital Airlines GUI, as described in Chapter 4, "Modifying the Digital Airlines Example," on page 43.

1.3 Prerequisites

- ❑ A Firefox browser (1.5.*x* or above) with popups enabled to access and administer the network connections among all of the network resources (the Identity Server, the Access Gateway server, and the Digital Airlines Web server).
- ❑ An installed and properly configured Novell® Access Manager Identity Server.

  For more information about installing the Identity Server, see "Installing the Novell Identity Server" in the *Novell Access Manager 3.0 Installation Guide*. For configuration details, see "Creating a Basic Identity Server Configuration" in the *Novell Access Manager 3.0 Setup Guide*.
- ❑ An installed and properly configured NetWare® Access Gateway server.

  For more information about the Access Gateway, see "Installing the NetWare Access Gateway" in the *Novell Access Manager 3.0 Installation Guide*. For configuration details, see "Configuring the Access Gateway" in the *Novell Access Manager 3.0 Setup Guide*.

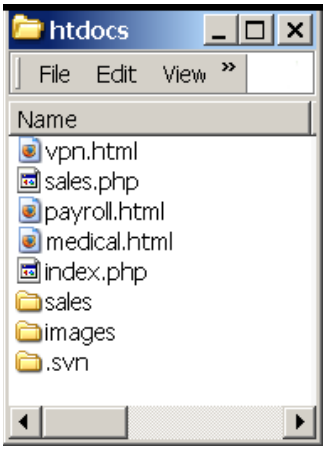
  NOTE: Although this example documents procedures only for NetWare Access server, you would follow similar procedures for Linux Access Gateway.

- ❑ PHP and Apache Web servers installed on your Identity Server.

  For more information, see Section 1.4, "Installing Apache and PHP Web Server Components," on page 12.

- ❑ The installed Digital Airlines example package, located in the `htdocs.tar.gz` sample directory, which contains the following components:

Figure 1-3 *Directory Structure of Digital Airlines Sample Components*



- **`vpn.html`:** Specifies the GUI interface page for initiating a VPN session.
- **`sales.php`:** Contains the sales PHP database files associated with the example.
- **`payroll.html`:** Specifies the GUI interface page for initiating a payroll session.
- **`medical.html`:** Specifies the GUI interface page for initiating a VPN session.
- **`index.php`:** Contains the welcome HTML index file for establishing secure authentication.
- **sales:** Specifies a PHP database containing example sales records for the example and associated Subversion files.
- **images:** Contains all image files associated with the example.
- **.svn:** Contains the associated Subversion files necessary for revision control.

See Section 1.5, “Installing Digital Airlines Components,” on page 13.

1.4 Installing Apache and PHP Web Server Components

1 Download and install the Apache 2 and PHP 4 Web server modules:

1a On your SUSE Linux 9.x server, click on the *YaST Control Center* icon, provide your root password if requested, then click *OK*.

1b In the YaST left navigation window, click the Software icon, then click Install and Remove Software.

The YaST software Search screen should open.

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

All available Apache 2 software packages are listed.

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

apache2: Specifies the Apache 2.0 Web server.

apache2-mod_php4: Specifies the PHP4 module for Apache 2.0.

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

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

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

1f Click *Accept*.

YaST should install the selected Apache server components.

1g To install the required PHP server components, repeat Step 1b on page 12.

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

All available PHP software packages are listed.

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

apache2-mod_php4: Installs the PHP 4 module for Apache 2.0.

php4: Installs the PHP 4 core files.

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

1k Click *Accept*.

YaST should install the selected PHP server components.

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

2a If necessary, repeat Step 1a on page 12.

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

2c In the HTTP Server Configuration window, click *Enabled* > *Finish*.

1.5 Installing Digital Airlines Components

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

1 Download the Digital Airlines directory from the Novell Access Manager Forge link:

1a Open a browser and enter Novell Access Manager Demos Wiki site (http://developer.novell.com/wiki/index.php/Nam-demos).

1b Download the `htdocs.tar.gz` to the server where you want to deploy the example.

This documentation explains how to deploy the Digital Airlines example and the Identity Server on the same machine. Although there are other possible configuration options, we recommend you use the single-machine install until you fully understand the Access Manager installation and configuration process described in this document.

2 Extract `htdocs.tar.gz` to a root directory on the server you want to protect.

NOTE: When deploying the example on the default Apache 2 and SLES 9 servers, `srv/www/htdocs/` is the correct directory in which to extract these files.

See "Prerequisites" on page 11 for additional details on the directory structure and example files.

3 Determine the DNS name and IP address of the SUSE Linux server on which your example files are installed:

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

3b Click *Network Services* > *Host Names*, then write down and remember the IP Address and Host Name of your host server:

IP Address: _____

Host Name: _____

As required later in the installation (see Step 4 on page 16), you must provide the host name and server configuration information to establish the network connection between the Web server you are protecting (the server where your Web service components are located) and the Novell Access Gateway access management server recommended in this example implementation.

After you install your Access Manager, Digital Airlines, and other required components, go to Chapter 2, "Configuring Digital Airlines," on page 15.

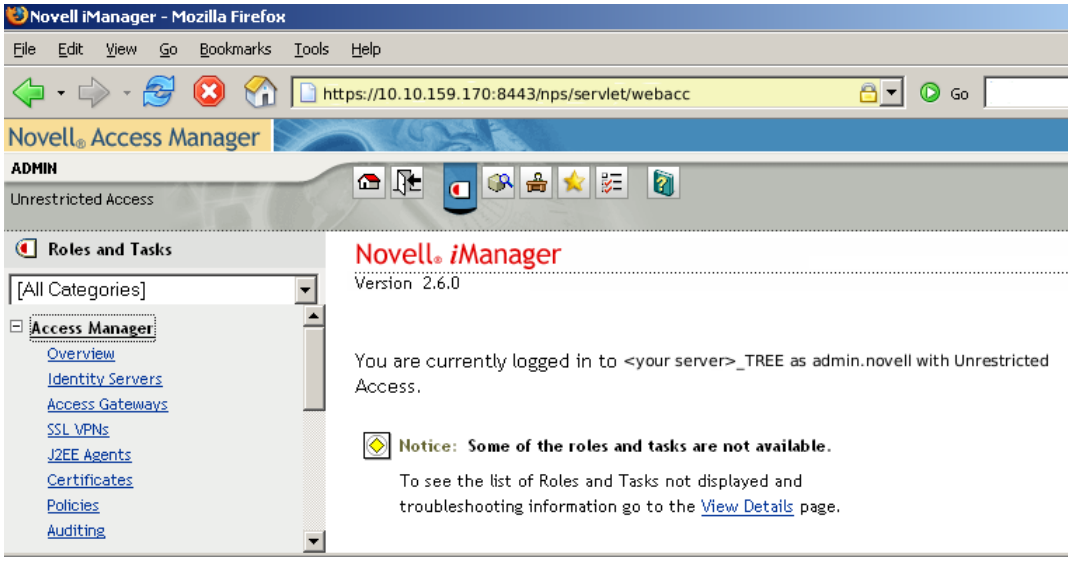
Configuring Digital Airlines

2

This section describes the procedure for deploying the Digital Airlines example with Identity and Access Gateway servers. You should have already created basic configurations for these servers, as described in "Setting Up a Basic Access Manager Configuration" in the *Novell Access Manager 3.0 Setup Guide*.

After you download and install the Digital Airlines example, you configure it by the following procedure:

1 Open a browser and log in to the Novell Access Manager Console (Access Console).

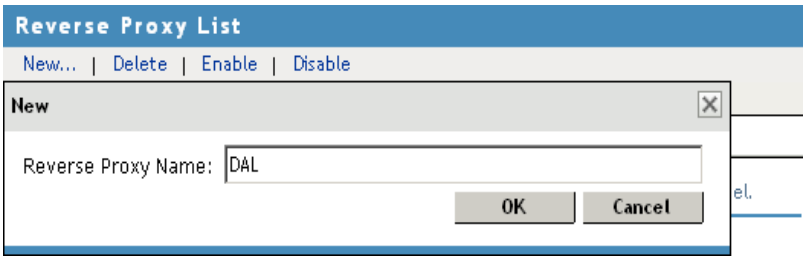


Use the log in URL you created when you initially installed your Access Manager (see "Record the login URL." in the *Novell Access Manager 3.0 Installation Guide*.

2 In the Access Console, click the *Access Gateways* link.

The IP address and server status of previously configured Access Gateway servers should be listed in the display window.

3 Click *Edit*, click *Reverse Proxy / Authentication*, click *New*, enter *DAL* as the new *Reverse Proxy Name*, then click *OK*.



4 In the Reverse Proxy window, under Proxy Service list, click *New* and specify the following information for the public host:

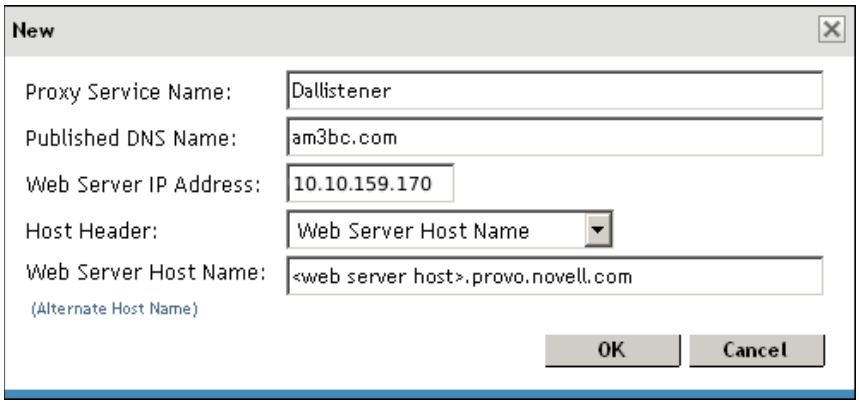
Proxy Service Name: Provide any name that intuitively identifies this connection to your Access Gateway server. For this example, use *Dallistener*.

Public DNS Name: The published DNS name of the Web server you are protecting. For this example, use *am3bc.com*.

Web Server IP Address: The IP address of the Web server where your Digital Airlines Web service files are installed.

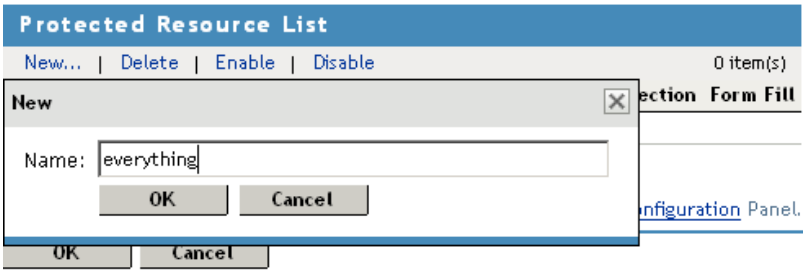
Host Header: The *Web Server Host Name*. Select this option from the drop-down menu.

Web Server Host Name: Specify the host name of the Web server where your Digital Airlines Web service files are installed.



5 Click *OK*.

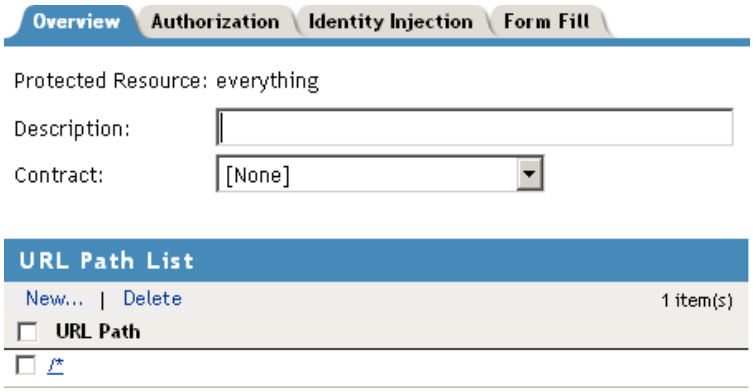
6 In the Reverse Proxy window, under the Proxy Service List, click *Dallistener*, then select the *Protected Resources* tab.



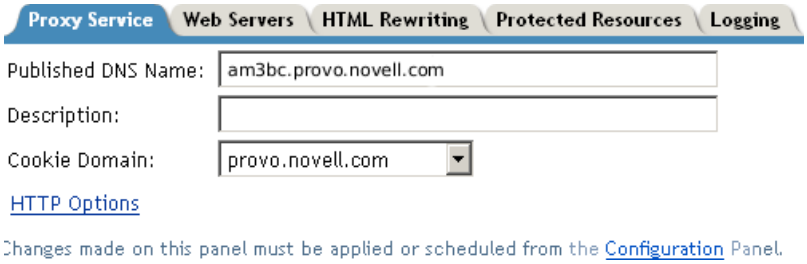
7 Click *New*, type `everything` in the Name field, then click *OK*.

8 In the Contract field, select *None* from the drop-down menu.

Under *URL Path List*, you should see /*, which includes everything on that server.



Later on, you will easily change the *Contract* field to a *Name/Password - Form*, but for now, we want you to learn how the example works without any authentication.



9 Click the *Configuration* Panel link at the bottom of the screen to save the changes and go to the Configuration Panel > click *OK*.

10 Add the host entries for the server where your Digital Airlines example files are installed. Do either of the following:

- From the Linux Access Gateway Configuration, select *Hosts* and add the following host entries for the server where your Digital Airlines example files are installed:

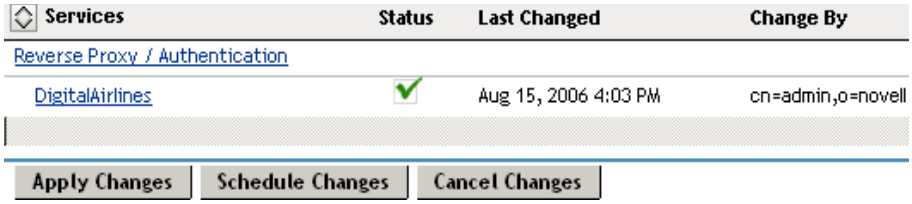
  `[Host IP address]  [Host dns name]`

- For the NetWare® Access Gateway, you must edit this information directly:
  - Unlock the NetWare console. If you need help, see "Unlocking the NetWare Access Gateway Console " in the *Novell Access Manager 3.0 Installation Guide*.
  - At the NetWare command line, enter: `edit SYS:\ETC\HOSTS.`
  - In the NetWare GUI, enter the host entries for the host server where your Digital Airlines example files are installed:

    `[Host IP address]  [Host dns name]`
  - Press the *Esc* key to save and exit.

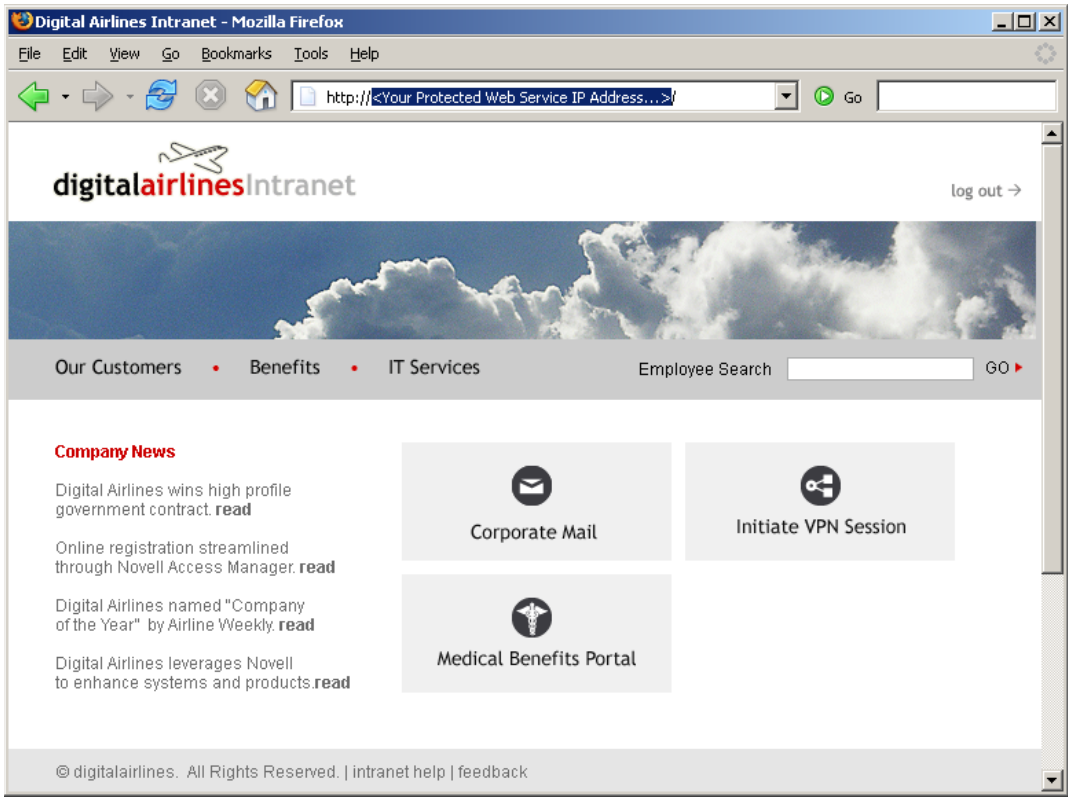
11 Return to the Access Gateway Server Configuration window.

12 Click *Apply Changes* at the bottom of the page.



13 To test the results, open a new browser tab or window and enter `www.am3bc.com`.

You should see the Digital Airlines sample application, which was formerly accessible only by entering the IP address.



Implementing Example Web Services

3

After you establish the reverse proxy connection, you should be able to directly access the Digital Airlines sample Web site through a browser. The reverse proxy hides the internal address of the Web server.

To test the example, open a new tab or browser window and enter www.am3bc.com. If you get an error, check the time on the Access Gateway and Identity Server. They must be within 5 minutes of each other.

If you get a Gateway Timeout error or the Access Gateway server becomes unresponsive, try restarting Tomcat. On the Linux box, enter `/etc/init.d/novell-tomcat4` restart.

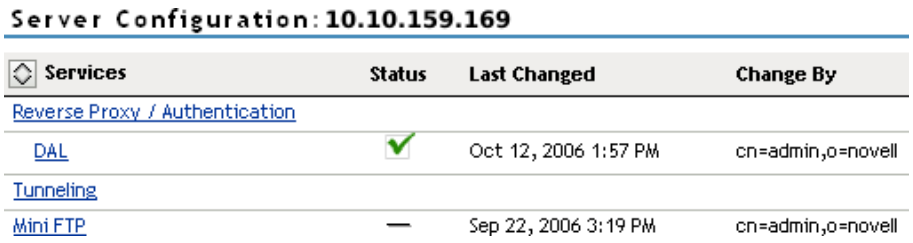
Here are other tasks you can do after configuring the Digital Airlines example:

- Section 3.1, “Enabling an Authentication Procedure,” on page 19
- Section 3.2, “Accessing the Corporate Mail Portal,” on page 21
- Section 3.3, “Accessing the Medical Benefits Portal,” on page 22
- Section 3.4, “Configuring a User Policy,” on page 22
- Section 3.5, “Creating a New User with a Sales Role,” on page 29
- Section 3.6, “Configuring an Identity Injection Policy,” on page 30
- Section 3.7, “Initiating a VPN Session,” on page 35

3.1 Enabling an Authentication Procedure

After hiding the internal Web server behind the Access Gateway, you can add an authentication method to the Web site by using the following procedure:

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

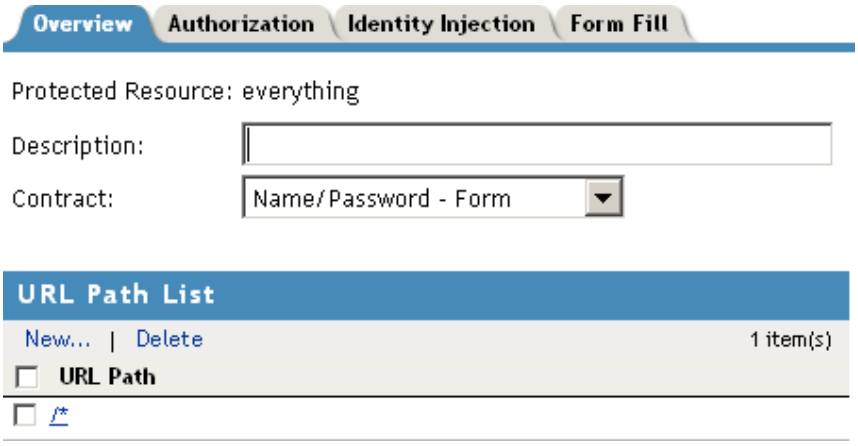


2 Click *DAL*, then click the *Dallistener* service *Protected Resources* tab, then click *everything*.

3 In the *Contract* field, select *Name/Password Form*, which triggers the wizard to initiate a Name and Password request to access the Web server.

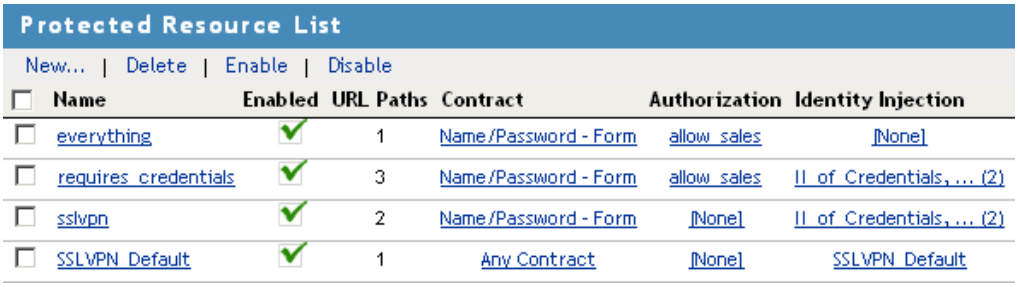
IMPORTANT: Make sure to select the *Name/Password - Form* from the drop-down menu. *Secure Name/Password* does not work correctly if the base URL for the Identity Server (IDS) is HTTP.

4 Use the default path /*, which allows access to everything on the Web Server. To delete or alter the path list, see Step 7 on page 17.



5 Click *OK* to return to the Protected Resources page.

6 In the Protected Resource List, click the *everything* check box, then click *Enable*.



7 Click *OK* to return to the Reverse Proxy window.

8 At the bottom of the page, select *Configuration Panel*, then click *OK* to the confirmation request.

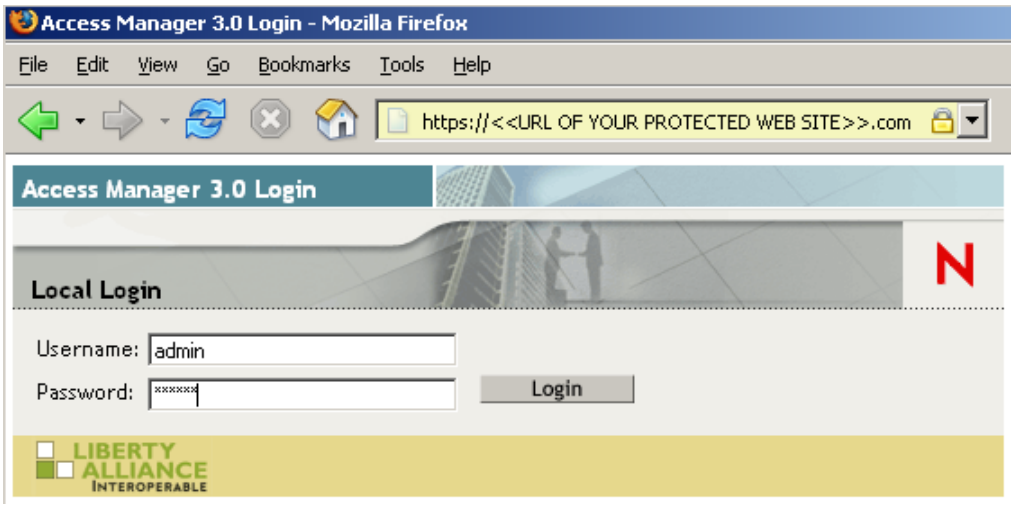
9 On the Server Configuration page, select *Apply Changes* > click *OK*.

This pushes the new configuration to the server. When the configuration process is complete, the server returns the status of the changes.

10 To update the Identity Server to use secure connections, click *Identity Servers* > *Setup* > *Update Servers*.

To test the results, open a new browser tab or window and enter the URL of your Web site, which should now be protected and should require you to log in using the name and password credentials

you specified in this procedure. In this example, you enter *admin* and the *password* you specified earlier in this procedure.



3.2 Accessing the Corporate Mail Portal

The Corporate Mail feature of the Digital Airlines example shows how mail services might be provided to users through your own Web portal. It is configured to access a user's local mail application on their machine after they log in to the Digital Airlines site and initiate a mail session by pressing the *Corporate Mail* selection on the Web page:

The Web server redirects the request to initiate a mail session to the user's default email application and injects the log in credentials to provide access the user's protected, Web-based email account.

3.3 Accessing the Medical Benefits Portal

The *Medical Benefits Portal* is one of three menu options accessible through the Digital Airlines example. It demonstrates how authorized users can securely access a protected Web service from the example Web site.

In a production environment, you install your own components as you have done for this example. You then create your own protected Web site and establish portals for users to securely access information for which they are authorized in the following procedure:

1. In the main Digital Airlines Web page, press the *Medical Benefits Portal* button.
2. Enter admin *name* and the *password* you created when you previously configured the Access Gateway.

3.4 Configuring a User Policy

Previously in the Digital Airlines example, you learned how to set up and configure Access Manager to protect a basic Web service. Access Manager also uses role-based access control (RBAC) to conveniently assign a user to a particular job function or set of permissions within an enterprise, in order to control access.

Access Manager enables you to assign users roles, based on attributes of their identity, and then associate authorization policies to the role. In this section, we create a simple policy that allows only users with a sales role to access the Digital Airlines Web services. When you complete this procedure, users attempting to access Digital Airlines will be denied and instructed to log in as a sales user, with a previously assigned sales role.

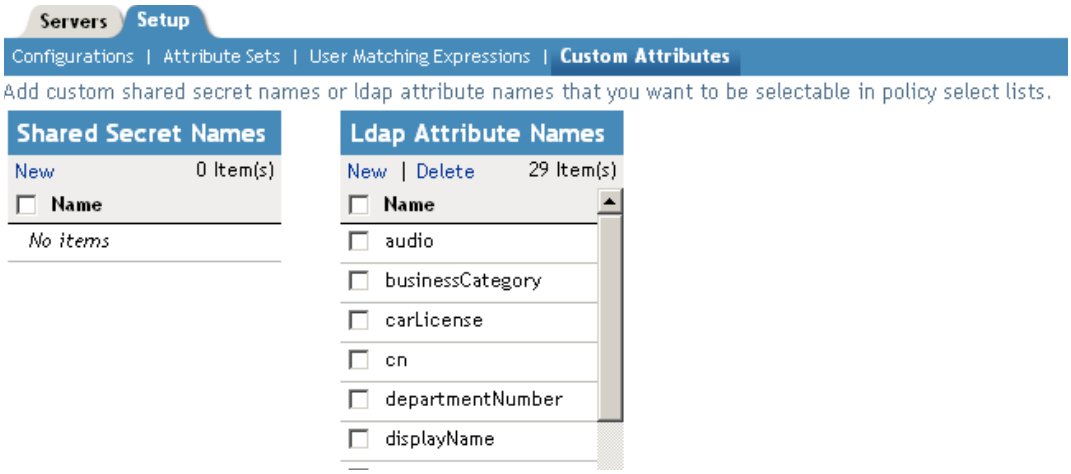
In designing your own actual production environment, you need to decide which roles you need (for example, sales, administrative, accounting, etc.) and which roles allow access to your protected resources. You then create policies which use the roles and assign to your users in your LDAP user store. For more information about creating role-based policies, see "Policy Management" in the *Novell Access Manager 3.0 Installation Guide*.

Configure a user policy using the following steps:

1. Add a description of an LDAP attribute to your configuration.
2. Based on the user's LDAP description, create a Sales role.
3. Assign the Sales role in the Reverse Proxy to limit access to the Web site to only members with that role.
4. Create a policy to add the user's credentials and roles into the Web header.

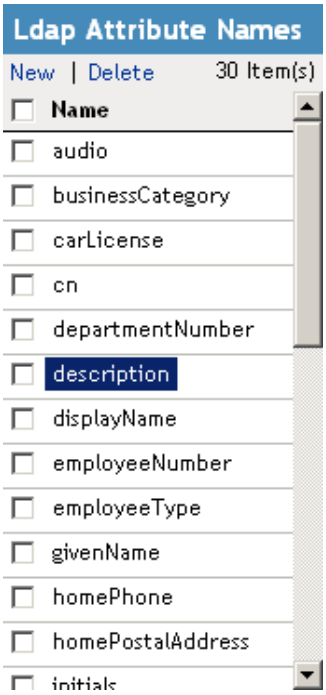
3.4.1 Adding a Description to Your Configuration

1 In the Novell Access Manager window, click *Identity Servers* > select the *Setup* tab > select *Custom Attributes*.



2 In the *Ldap Attribute Names* window, click *New* > enter "description" in the *Name* field > click *OK*.

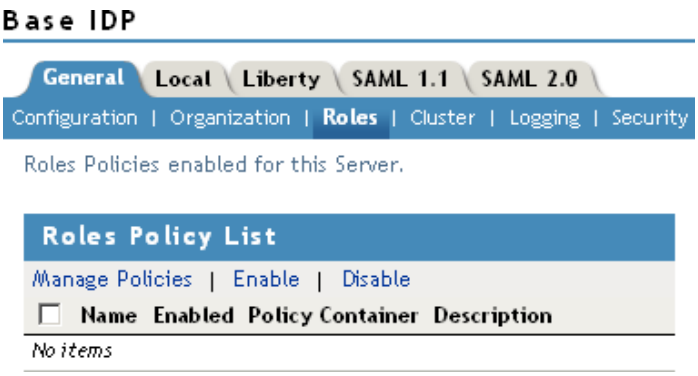
This adds the *description* attribute to the Policy Builder's list of available LDAP attributes. You can now create a new user sales role, which will later be accessible through your Digital Airlines Web browser.



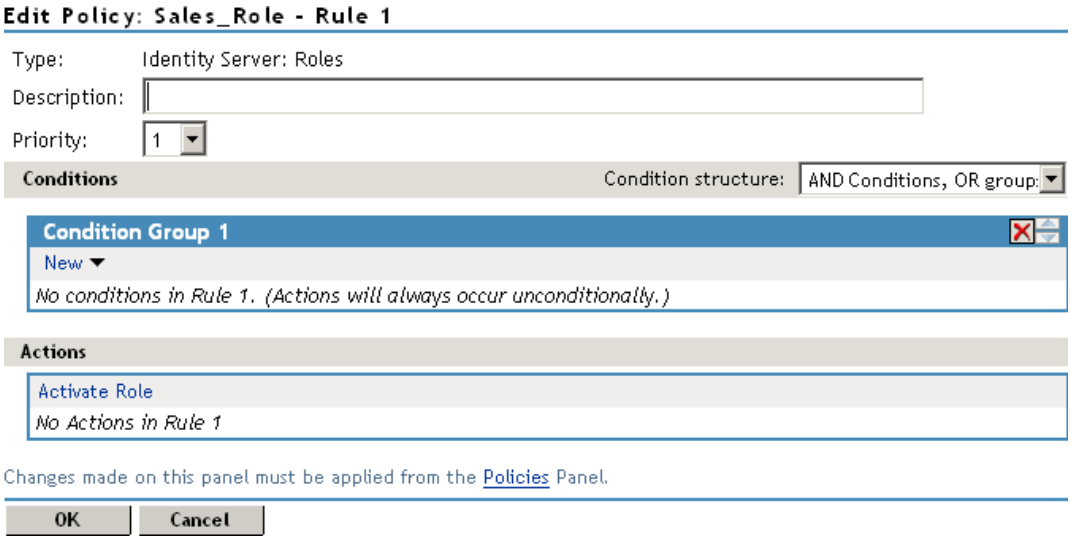
3.4.2 Creating a Sales Role

Use the following procedure to create a sales role in the Digital Airlines example. For more information, see "Creating Role Policies" in the *Novell Access Manager 3.0 Administrative Guide*.

1 In the Novell Access Manager window, click *Identity Servers* > click the *Setup* tab > select *DAL Server* > click the *General* tab > click *Roles*.



2 In the *Roles Policy List* window, click *Manage Policies* > click *New...* to create a new role > specify *Sales_Role* in the *Name* field > select *Identity Server: Roles* from the drop-down menu in the *Type* field > click *OK* to open the policy editor.



3 In the *Edit Policy* window, under *Condition Group 1*, click *New* > select *LDAP Attribute* from the list > in the *Condition Group 1* window, assign the following values:

LDAP Attribute: *description* (If *description* is not included in the LDAP Attribute list, add it by following the procedure in Step 3a and Step 3b on page 25.)

Comparison: *String: Equals*

Mode: *Case Sensitive*

Value: *Data Entry Field* (select from the drop-down box and enter *Sales* as the value)

Result on Condition Error: *False*

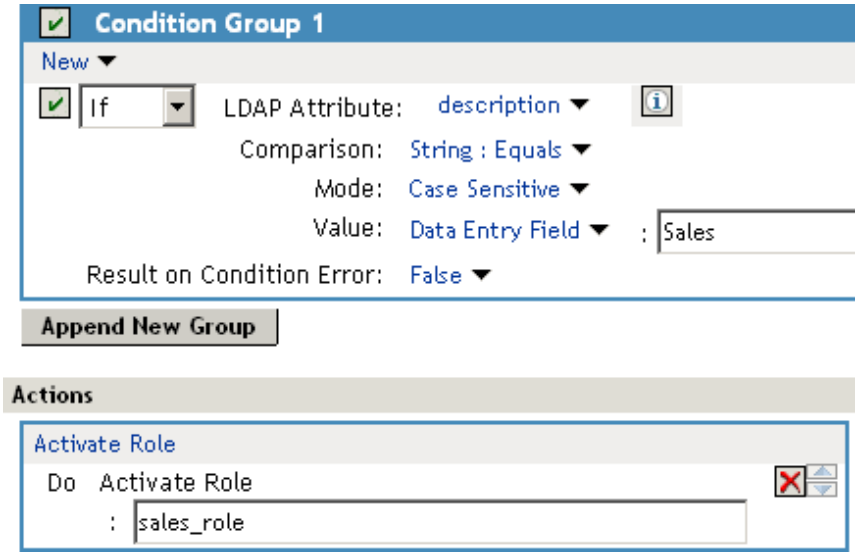
If the *description* value is not listed in the LDAP Attribute drop-down menu, create it by following this procedure:

3a In the *Condition Group 1* window, click the drop-down *LDAP Attribute* > click *New* at the bottom of the list > enter *description* in the *Name* field > click *OK*.

Because this is a case-sensitive LDAP attribute, use lowercase for this value.

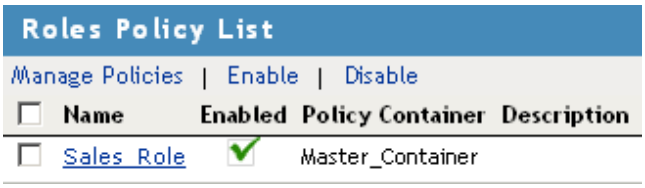
3b In the *LDAP Attribute* field, select *description* from the drop-down menu.

4 In the *Actions* window, click *Activate Role* > enter *sales_role* in the *Do Activate Role* field.



5 Click *OK* to close the Rule editor > click *OK* to close the Rule List > click *Apply Changes* > click *Close* to return to the Roles Policy List.

6 In the Roles Policy List window, select *Sales Role* > click *Enable*.



7 Click *OK* to return to the Identity Servers Configuration window.

8 In the Identity Servers window, click the Setup tab > click *Update Servers* on the DAL_Server link.

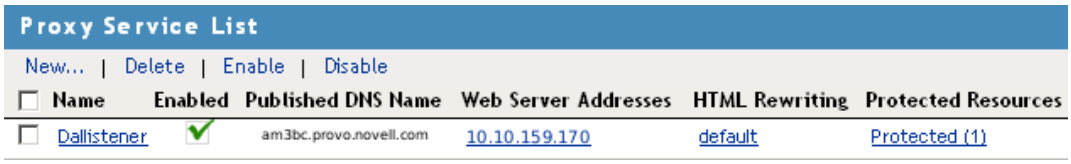
The Identity Server console window returns to the *Servers* tab and the Server Status should change to green in about 1 minute.

3.4.3 Assigning the Sales Role in the Access Gateway Configuration

Use the following procedure to map an LDAP Description of Sales to the Sales role and limit access to the entire Digital Airlines Web site, based on the Sales role. For more information about role-based access control (RBAC), see "Understanding RBAC in Access Manager" in the *Access Manager 3.0 Administrative Guide*.

1 In the Access Console, click *Access Gateways* > click *Edit* > click your Digital Airlines reverse proxy (*DAL*).

2 In the Proxy Service List window, click *Protected (1)* under the Protected Resources heading > click *OK* when prompted to update the configuration.



3 In the Protected Resource List window, click *everything* > select the *Authorization* tab > click *Manage Policies* (your Sales Role policy should be listed) > click *New...* > enter the following values:

Name: *allow_sales* (notice lower case)

Type: *Access Gateway: Authorization* (select from the drop-down menu)

The values will be accepted and the Edit Policy window will open.

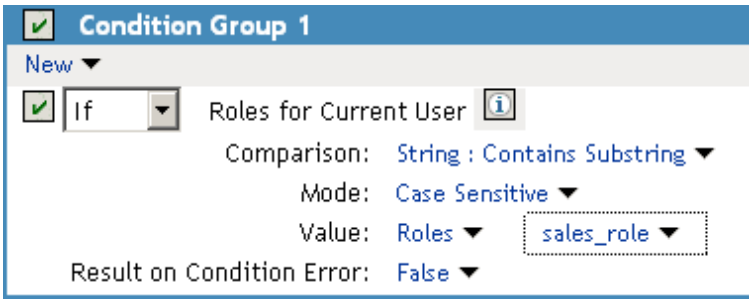
4 In the Edit Policy window, under the *Condition Group 1* heading, click *New* > select *Roles for Current User* from the menu > enter the following values from the drop-down menus:

Comparison: *String: Contains Substring*

Mode: *Case Sensitive*

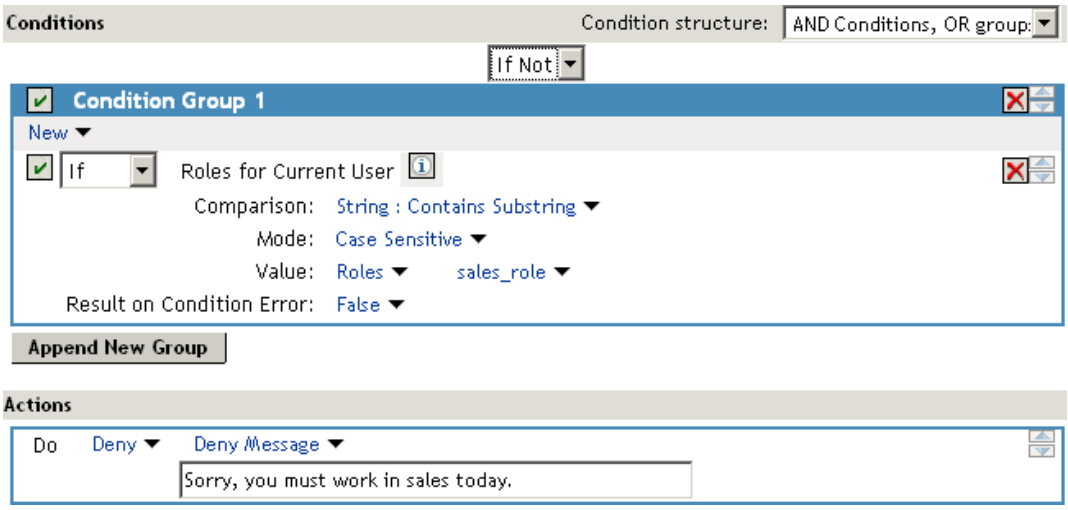
Value: *Roles: sales_role*

Return on Condition Error: *False*



5 In the Actions window, click *Permit* > select *Deny* > click *Display Default Deny Page* > click *Deny Message* > enter the deny message, *Sorry, you must work in sales today.*

6 At the top rule editor, above the Condition Group 1 window, change the condition from *If* to *If Not* > click *OK* to close the rule editor.



7 Click *OK* to close the Rule List.

8 In the Policy List window, click *Apply Changes*.

After the configuration changes are imported into Access Manager, the Access Gateways window will display.

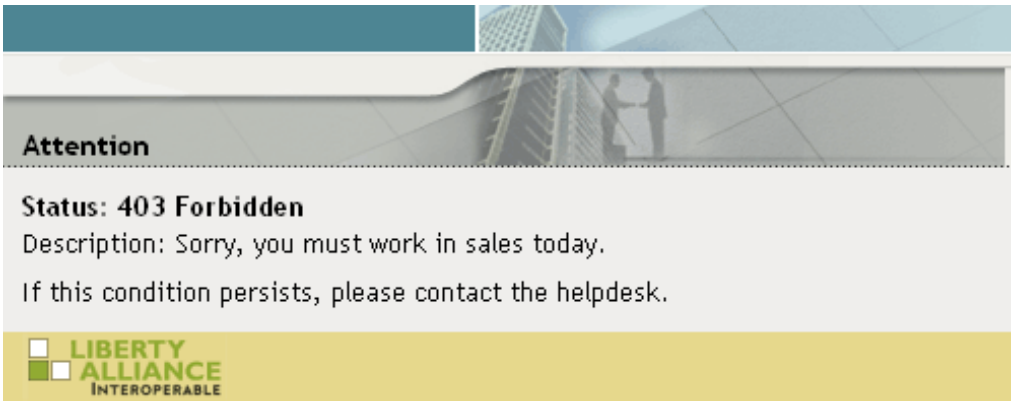
9 Test the results using the following procedure:

9a Open a new browser > enter the URL of the Digital Airlines Web site you've created.

In this example, it is *www.am3bc.com*.

9a When prompted for user ID and password from Access Manager, enter *admin* and *novell*.

You should receive the following response window with the message derived from the Access Gateway you just configured:



Now, only users with an assigned Sales role can access the Digital Airlines Web site, as explained in Section 3.5, “Creating a New User with a Sales Role,” on page 29.

3.5 Creating a New User with a Sales Role

After you have created a user policy, only users provisioned with that policy can access the protected Web resource. This section describes how to create a Digital Airlines user with the protected Sales role:

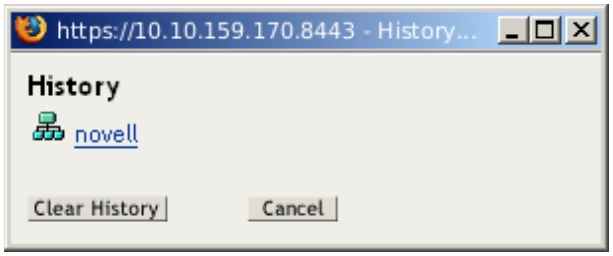
1. In the Administration Console, click *Users* > *Create User* > enter the following user information:

   Username: *Tom*

   First name: *Tom*

   Last name: *Tester*

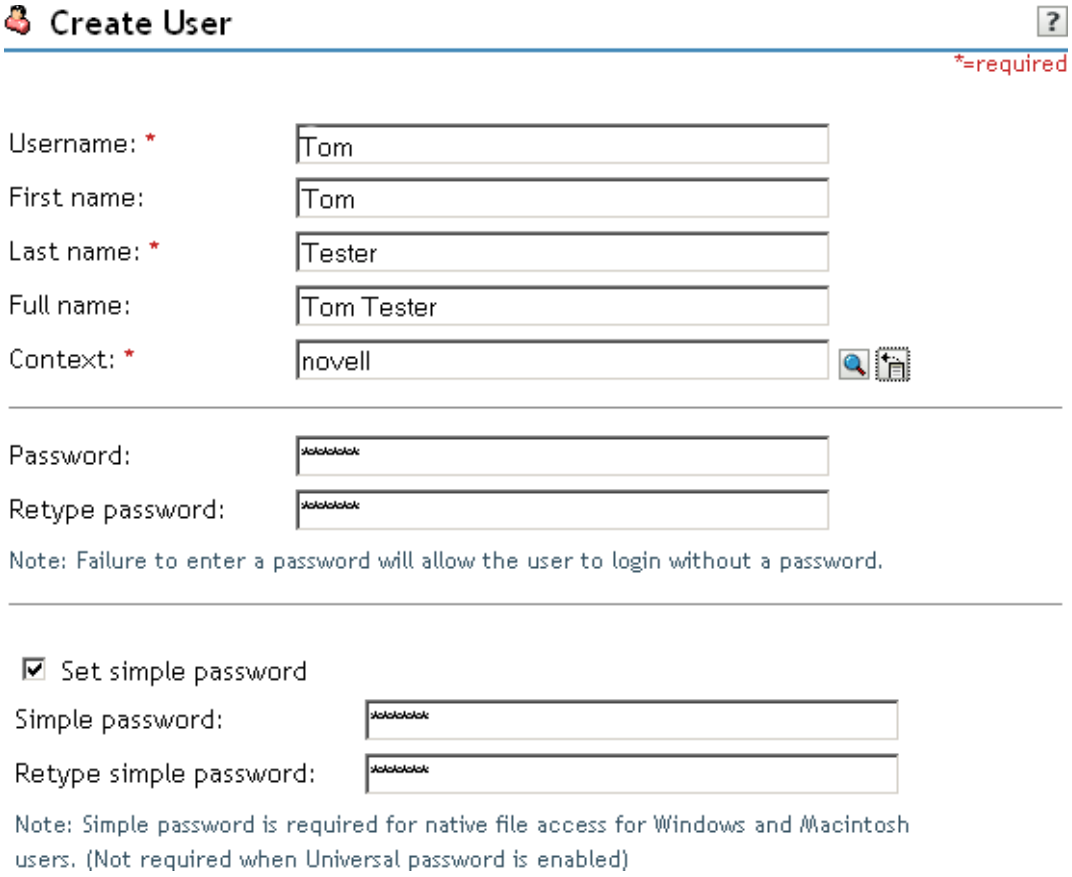
   Context: Enter the Context name of your protected network by clicking the *Object History* icon  > click the *History* icon in the pop up window that displays the Context name of your protected Web server, as shown below. The Context name will automatically populate the Context field.



   Password: *Assign a password*.

   Retype password: *Retype the assigned password.*

   Set simple password: Click the *Set simple password* box, which automatically populates the the Simple password fields.



2. In the Description field, click the + icon.
3. In the Add Value window, enter *Sales* (uppercase) > click *OK* to return to the Create User window.
4. In the Create User window, click *OK*.

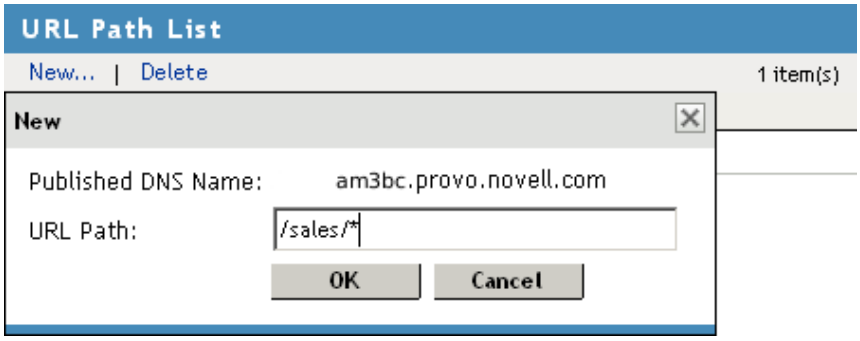
3.6 Configuring an Identity Injection Policy

You can inject the user name and password into the HTTP authentication header and you can inject the user's roles into a custom header. This enables the Digital Airlines sample Web site to respond to that customer header.

1. In the Administration Console, click *Access Manager* > *Access Gateways* > *Edit* > *DAL* > *Protected (1)*.
2. In the Protected Resource List window, click *New...*, type *requires_credentials*, then click *OK*.

   This creates a new case-sensitive Protected Resource object.
3. In the Contract field, select *Name/Password Form* from the drop-down menu.

4 In the URL Path List, click *New,* type */sales/**, then click *OK*.



5 Click the *Identity Injection* tab > *Manage Policies* > *New*.

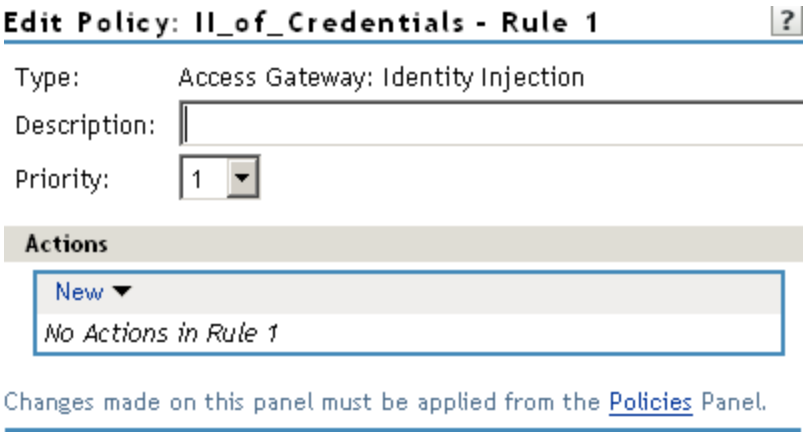
6 For the new policy, provide the following information:

Name: *II_of_Credentials*

Type: Select *Access Gateway: Identity Injection* from the drop-down menu.

7 Click *OK*.

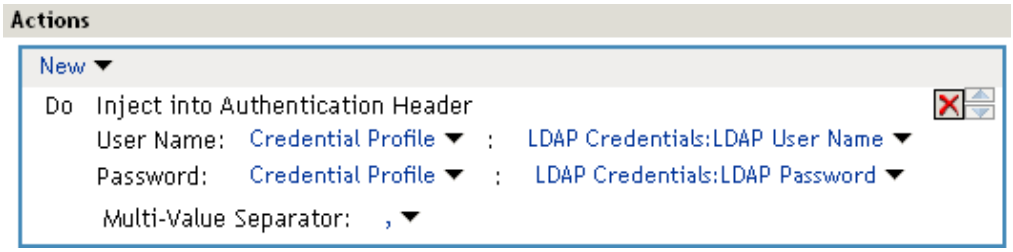
The Edit Policy window opens for you create a new rule for the *II_of_Credentials* policy.



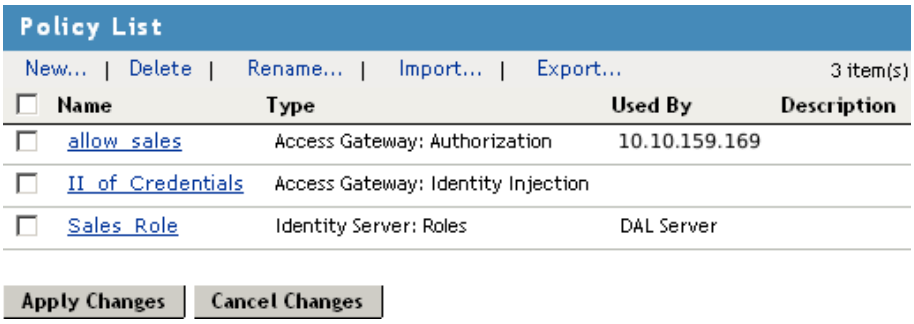
7a Click *New*, select *Inject Into Authentication Header* from the drop-down menu, then select the following values from the drop-down menus:

User Name: From the *Credential Profile* list, select *LDAP Credentials: LDAP User Name.*

Password: From the *Credential Profile* list, select *LDAP Credentials: LDAP Password*.



7b Click *OK* to return to the *Edit Policy: II_of_Credentials* window, then click *OK* to close the Rule List and return to the Policies window.



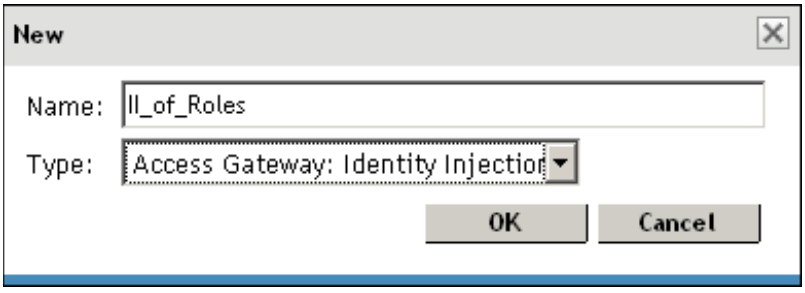
8 Click *Apply Changes* to save the new Identity Injection policy, then click *Close* to return to the *Identity Injection* window.

9 Select the *II_of_Credentials* policy check box, click *Enable*, then click *OK* to return to the Protected Resource list.

10 Click *everything* > *Identity Injection* > *Manage Policies* > *New* to create a new policy with the following values:

Name: Type *II_of_Roles*.

Type: Select *Access Gateway: Identity Injection* from the drop-down menu.



11 Click *OK*, which opens the *Edit Policy* window for the *II_of_Roles rule* to create a new action for the rule.

11a In the Actions window, click *New*, then select *Inject into Custom Header*, then specify the following values:

Custom Header Name: *X-Role*.

Value: *Select Roles for Current User* from drop-down menu.

11b Click *Policies* to apply the changes, then click *OK* to save changes and go to the Policies Panel.

11c In the Policy List window, select the *II_of_Roles* check box, click *Apply Changes*, then click *OK*.

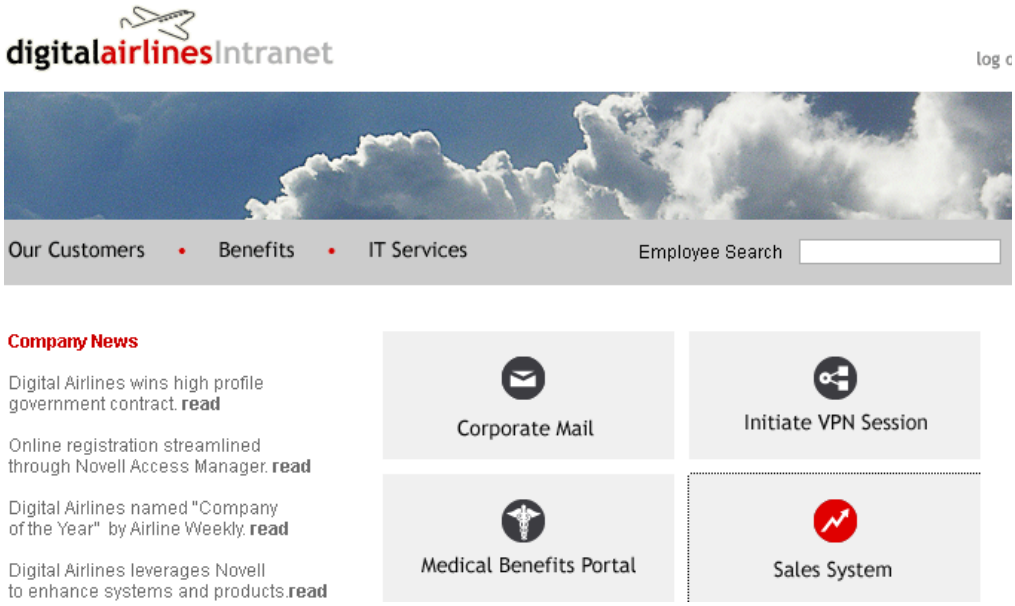
12 Test the configuration:

12a Open a new browser to start a new session and enter *www.am3bc.com*.

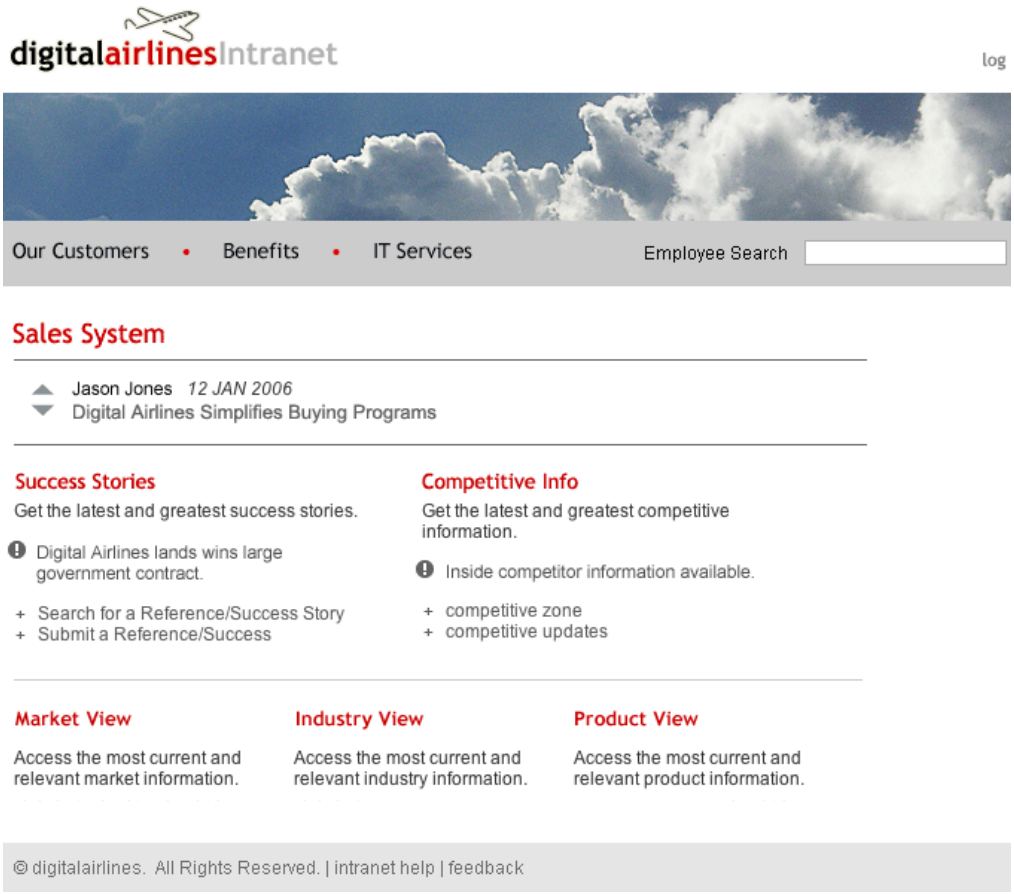
In Firefox, you must close all browsers before starting a new session.

12b Enter the username *Tom* and enter the *password* for the user you assigned the Sales role in Section 3.5, “Creating a New User with a Sales Role,” on page 29.

You should now gain access to the Web application with the newly injected *Sales System* access button as shown below:



12c Click the *Sales System* button and access the Digital Airlines example Sales System Web site, as shown below:



For more information about Identity Injection Policies, see "Creating Identity Injection Policies" in the *Novell Access Manager 3.0 Administrative Guide*.

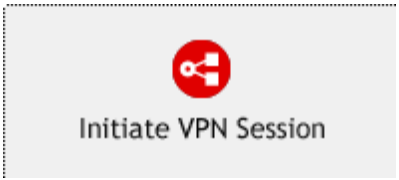
3.6.1 Disabling Restrictive Access Policies

The injection policies you have created in this task limit access to the Sales section of the Digital Airlines example Web site. To facilitate other tasks in this example, disable the *allow_sales* authorization policy to allow all users to access the main Digital Airlines site.

3.7 Initiating a VPN Session

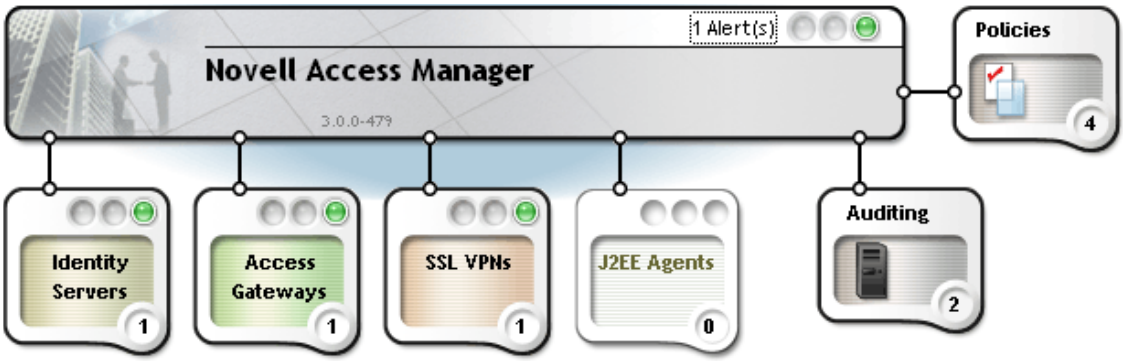
This section explains how to initiate a SSL Virtual Private Network (VPN) connection in the Digital Airlines example. The VPN agent secures access to non-HTTP applications.

Figure 3-1 *GUI Button to Initiate an SSL VPN Session*



Before performing this task, you must have the SSL VPN agent installed on either your Identity Server or on your Linux Access Gateway (LAG) server. Your Access Manager console should appear similar to the green state shown in Figure 3-2 on page 35:

Figure 3-2 *Access Console Indicating Installation Status of Access Manager Components*



For more information about installing and configuring the SSL VPN agent, see "Configuring the SSL VPN Gateway ".

In the Digital Airlines example, you will perform the following tasks:

1. Configure the SSL VPN as a protected resource behind your Access Gateway.
2. Configure Identity Injection policies for a user's credentials, session cookie, and roles.
3. Use the roles to control access to applications behind the SSL VPN.
4. Test the SSL VPN with a traffic rule and client integrity check.

3.7.1 Configuring the SSL VPN as a Protected Resource

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

1 In the Administration Console, click *Access Manager* > *Access Gateways* > *Edit*, then select your Digital Airlines reverse proxy (*DAL*).

2 In the Proxy Service List window, click *New*, then provide the following values:

Proxy Service Name: *Select sslvpn*.

Multi-Homing Type: *Select Path-Based* from drop-down menu. (For more information about accessing multiple resources, see "Using Multi-Homing to Access Multiple Resources" in the Novell Access Manager 3.0 Administration Guide.)

Path: */SSLVPN*.

Web Server IP Address: *xxx.xx.xxx.xxx*. Provide the server address of SSL VPN.

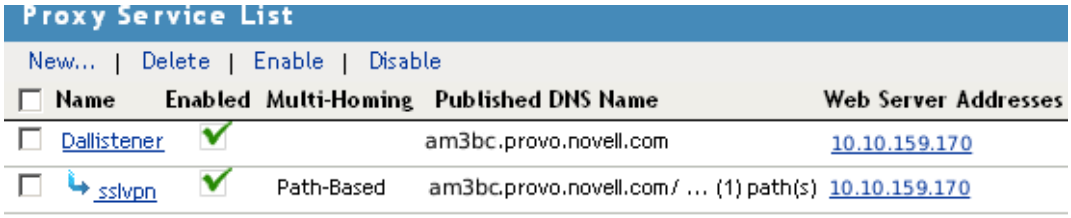
Host Header: *Select Web Server Host Name* from drop-down menu.

Web Server Host Name: *[Alternative Host Name].provo.novell.com*.

3 Click *OK*.

The Reverse Proxy window is displayed.

4 In the Proxy Service List window, click the *[IP link]* for sslvpn Web Server Addresses.



5 Change the *Connect Port* from *80* to *8080*, then click *OK*.

The reverse proxy object for the SSL VPN is complete after the Reverse Proxy window is displayed.

6 Continue "Creating an SSL VPN Protected Resource" on page 36.

3.7.2 Creating an SSL VPN Protected Resource

Because a path-based accelerator doesn't get any protected resources, you must use the parent's protected resource list using the following procedure:

1 In the Proxy Service List window, click *Dallistener* > *Protected Resources* tab > *New* > enter the name *sslvpn* > click *OK* to get to the Overview window.

2 From the drop-down *Contract* field, change the value from *[None]* to *Name/Password - Form*.

3 In the URL Path List window, click *New* > change the URL Path to */sslvpn/** > click *OK*.

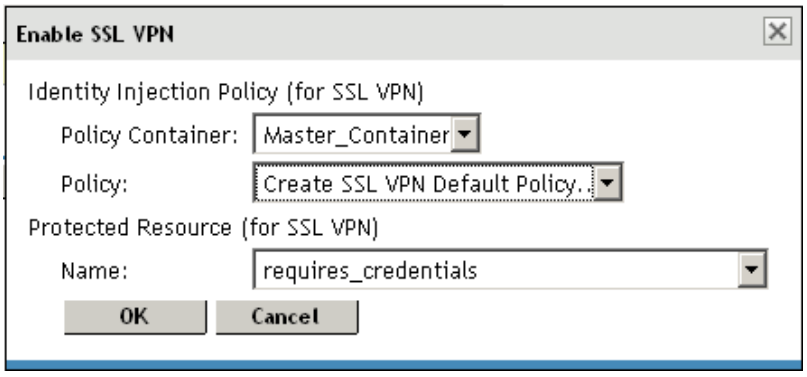
After you have created the protected resource for the SSL VPN, you must configure its identity injection policies in "Configuring the SSL VPN Identity Injection Policies" on page 37.

3.7.3 Configuring the SSL VPN Identity Injection Policies

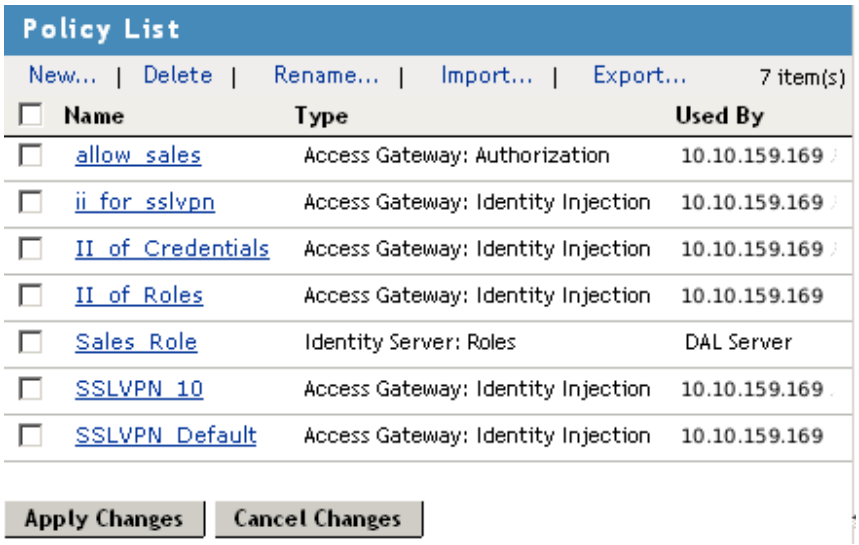
1. In the Administration Console, click *Access Manager* > *Access Gateways* > *Edit* > *DAL*.
2. In the Proxy Server List pane, select the *sslvpn* check box, then click *Enable SSL VPN*.
3. Create the SSL VPN Identity Injection Policy by entering the following values in the drop-down menus:

   Policy Container: *Master_Container*.

   Policy: Create SSL VPN Default Policy.



After you select the Create SSL VPN Default Policy, a Policies window opens:



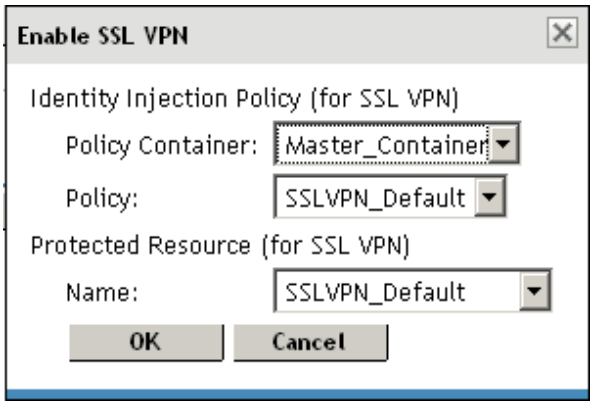
4. Select the *SSL_VPN_Default* check box, then click *Apply Changes*.
5. Click *OK* on the Alert message.
6. In the Policy List window, click *Close*.
7. In the Enable SSL VPN policy resource pane, in the Protected Resource Name field, select *Create SSL VPN Default Protected Resource* from the drop-down list.

The fields in the pane should now be populated with the following values:

Policy Container: *Master_Container*.

Policy: *SSLVPN_Default*

Protected Resource: *SSLVPN_Default*

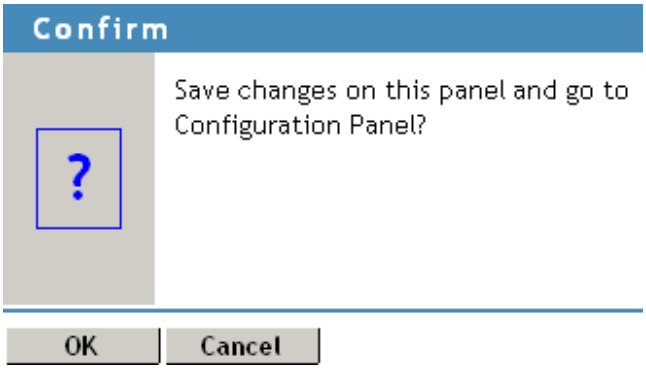


8 Click *OK*.

The */sslvpn* Path should now indicate *SSLVPN_Default* as the Protected Resource.

9 To apply the changes, click the *Configuration* Panel link.

10 Click *OK* to on the advisory pop-up to save the changes and go to the Server Configuration panel.



11 Click *Apply Changes* in the Server Configuration window, wait until the server refreshes, then click *OK* after the information screen verifies that changes are applied.

3.7.4 Testing the SSL VPN Basic Configuration

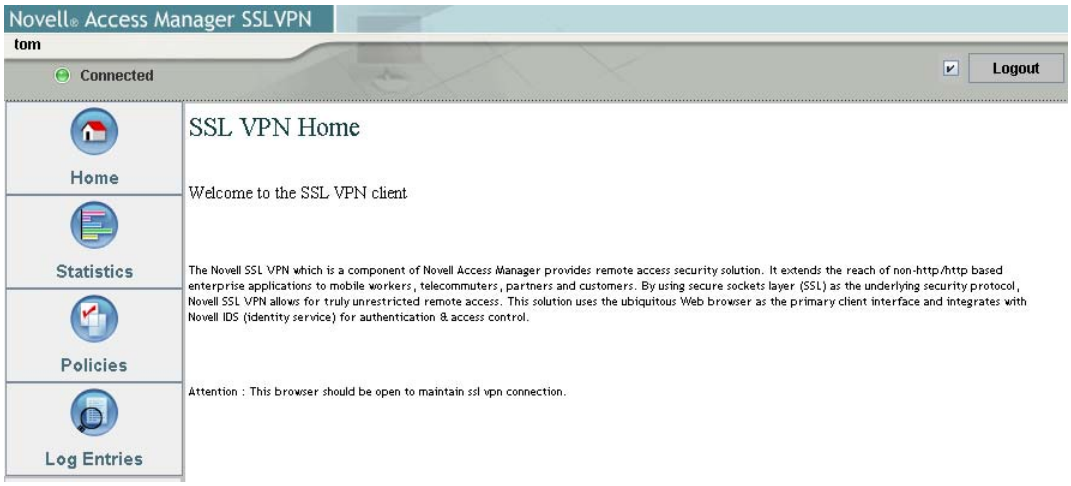
Basic configuration of the SSL VPN is complete after it is protected behind your gateway and you have built your necessary identity injection policies. Test your basic configuration with the following procedure:

1 To access the SSL VPN servlet, open a new browser and enter *http://am3bc.provo.novell.com/sslvpn/login*.

2 If requested, click *OK* to accept the certificate for the SSL VPN client.

3 Log in with any authorized user name and password that is registered within your corporate domain, including the users you created in Section 3.5, “Creating a New User with a Sales Role,” on page 29.

4 Verify that the SSL VPN client downloads, installs, and runs:



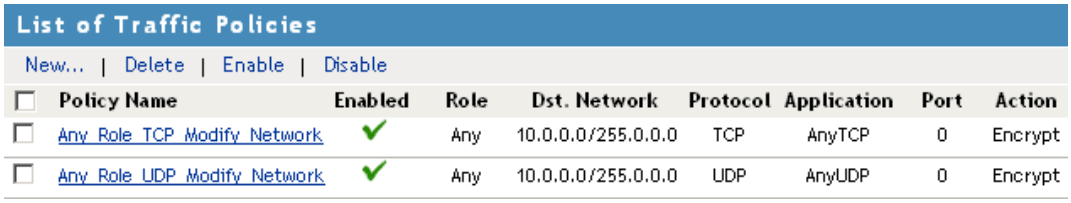
Notice that the user’s first name (“tom”) is injected into the header of the SSL VPN browser.

5 Click *Logout*, then close the Access Manager logout browser.

3.7.5 Configuring a Traffic Policy

Traffic policies allow you to control access to different networks and applications protected behind the SSL VPN. Simulate this by creating a rule that allows access to your network:

1 In the Administration Console, click *Access Manager* > *SSL VPNs* > *Edit* > *Traffic Policies*.



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

3 In the Traffic Policies list, select *sales*, then click *Enable*.

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

Role: *sales_role*. Specify this value in the Role field after clicking the + icon.

Destination Network: *10.0.0.0*. This field is usually pre-populated, or you can specify the IP address of the SSL network.

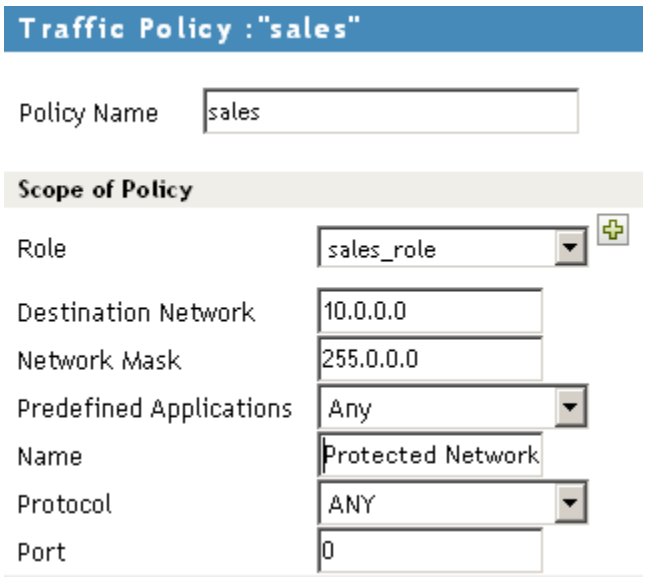
Network Mask: *255.0.0.0*. This field is usually pre-populated, or you can specify the value for your destination network.

Predefined Application: *Any.* You can also select from drop-down list to specify your network application.

Name: *Protected Network*. You can also provide any descriptive name for the SSL network.

Protocol: *Any*. Specifies if the protocol is TCP or UDP or Any.

Port: *Port*. Specifies the port number on which the service you select listens.



5 Click *OK* to save the configuration and return to the List of Traffic Policies window.

6 Select *sales_role* in the Traffic Policies list, click *Enable*, then click *OK*.

7 In the Server Configuration window, click *Apply Changes*, then *OK* after changes are applied.

8 Test the traffic rule:

8a Open a new browser session and enter *http://am3bc.provo.novell.com/sslvpn/login*.

8b Log in with a user on the system as *admin*.

8c In the left navigation window, click *Policies*.

Notice that without a sales role, the *admin* user has no access to the Digital Airlines network. Access is granted only when you log in with your *sales* credentials created in Section 3.5, “Creating a New User with a Sales Role,” on page 29.

8d Log out of the SSL VPN session.

8e Open a new SSL VPN browser session and enter *http://am3bc.provo.novell.com/sslvpn/login*.

8f Log in with your *sales* credentials created in Section 3.5, “Creating a New User with a Sales Role,” on page 29.

8g In the left navigation window, click *Policies*.

Notice that the user "*tom*" is now assigned a *sales_role* on the SSL VPN server.

For more information about Traffic Policies, see "Viewing and Modifying Traffic Policies" in the *Novell Access Manager 3.0 Administration Guide*.

Modifying the Digital Airlines Example

4

The Digital Airlines example is a relatively simple server-side Web application that consists of a pre-defined PHP framework and its associated database, HTML, and graphic files. Although creating more robust Web applications for your actual production environment is outside the scope of this document, you might want to demonstrate the capabilities of Access Manager using an example more tailored to your company.

This section explains how you change the look and feel of the Digital Airlines example by replacing its graphics with those you create yourself:

- Section 4.1, "Prerequisites," on page 43
- Section 4.2, "Understanding the Example Files," on page 43
- Section 4.3, "Updating Static Graphics," on page 44
- Section 4.4, "Updating Mouse-Over Links," on page 46
- Section 4.5, "Deploying Your Updated Example Web Service," on page 47

4.1 Prerequisites

- ❑ Down load and install the Digital Airlines example directory from the Novell Access Manager Demos Wiki site (http://developer.novell.com/wiki/index.php/Nam-demos).
- ❑ Create your own proprietary graphic files in GIF format to replace those in the default Digital Airlines example.
- ❑ Select a suitable PHP or HTML editor that enables you to open, view, and edit the example source files.

  Although you can edit files using a simple text-only editor, making changes to the example files is simpler using a more robust program that displays the source code integrated with your graphic files.

4.2 Understanding the Example Files

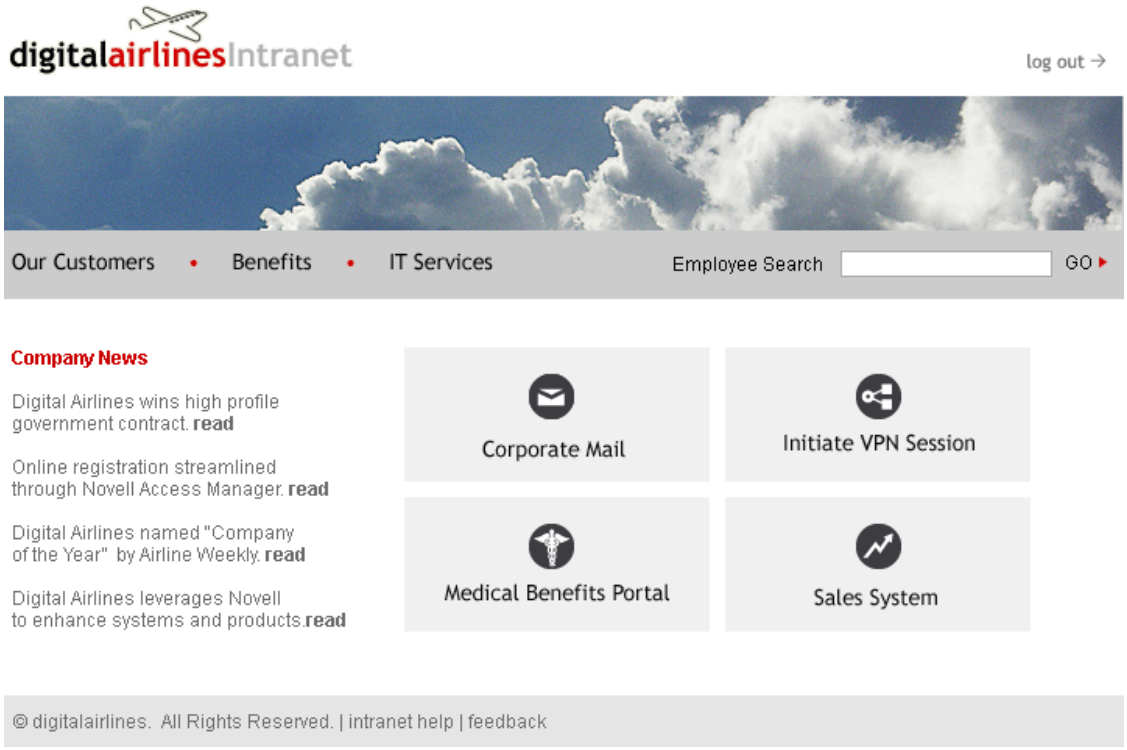
The files provided with the Digital Airlines example can be altered to meet your needs. The `index.php` and `sales.php` files in the htdocs directory are the master configuration files that define the visual appearance and functionality of the Web site. Other folders in the `htdocs` directory contain the image and database reference files required and specified by the PHP files.

Although you might change the functionality of this example by altering the PHP files, this document describes only how to integrate new graphic files into the existing database structure. By working through the Digital Airlines example, you should understand how to deploy Access Manager to protect your own Web services in a production environment.

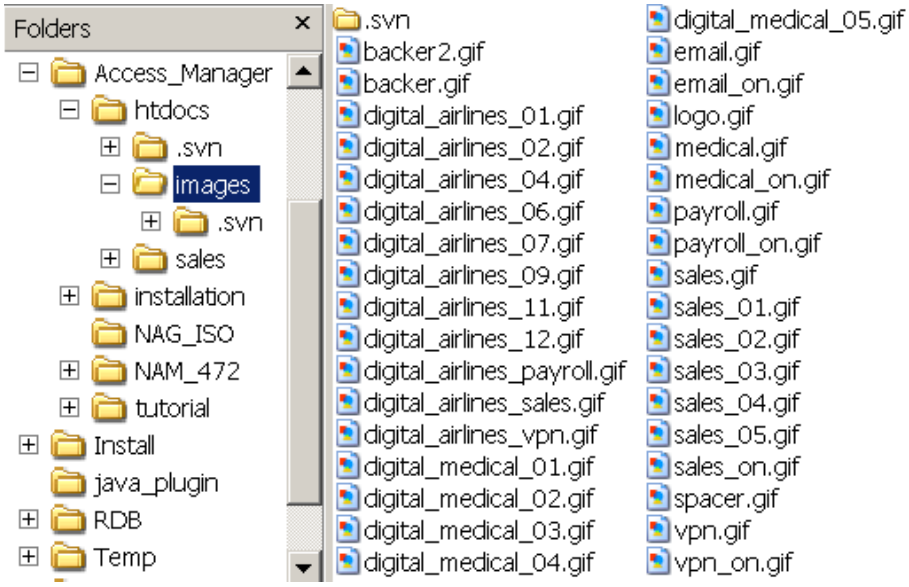
4.3 Updating Static Graphics

You can easily update any of the graphic files contained in the Digital Airlines example:

Figure 4-1 *Digital Airlines Composite GUI*



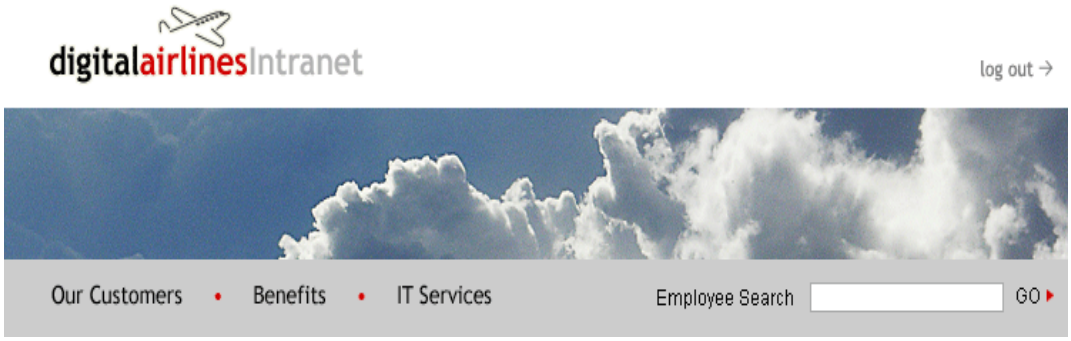
1 Navigate to the `htdocs` directory where your Digital Airlines components are located and open the `images` directory.



2 Open any of the GIF files to view which images you might want to replace.

For example, you might want to replace the Digital Airlines main header file with the look and feel of your own company:

Figure 4-2 *digital_airlines_01.gif*



3. Remember the name of this file, `digital_airlines_01.gif`.
4. Open the `index.php` file in an editor and search for `digital_airlines_01.gif`.

```
<div style="position:absolute; left:680px; top:42px;color:6a696a;font: 12px arial"> <a href="/plogout"></a></div>.
<table id="Table_01" width="747" height="700" border="0" cellpadding="0" cellspacing="0">.
        <tr>.
          <td colspan="5">.
                  <img src="images/digital_airlines_01.gif" width="747" height="233" alt=""></td>.
        </tr>.
        <tr>.
```

5. In the PHP code, notice the dimensions of the graphic are 747 pixels wide and 233 pixels high.
6. Create your own main header graphic file (*your_company*_01.gif) with approximately the same dimensions as the Digital Airlines graphic (`digital_airlines_01.gif`).

NOTE: Although your replacement graphics do not need to be exactly the same size, try to create the new files as close to the original size as possible to avoid possible display problems.

---

7. Replace the old digital_airlines_01.gif with your new *your_company*_01.gif.
8. In the PHP code editor, replace the old `digital_airlines_01.gif` name with your new *your_company*_01.gif string.

```
<div style="position:absolute; left:680px; top:42px;color:6a696a;font: 12px arial"> <a href="/plogout"></a></div>.
<table id="Table_01" width="747" height="700" border="0" cellpadding="0" cellspacing="0">.
        <tr>.
          <td colspan="5">.
                  <img src="images/your_company_01.gif" width="747" height="233" alt=""></td>.
        </tr>.
        <tr>.
```

The PHP code points to this GIF file and the Web service will display it in the proper location and format when the HTML page is called.

9. Save the `index.php` file.
10. Repeat this procedure for every graphic in your sample that you want to replace, except mouse-over links. For this procedure, see Section 4.4, “Updating Mouse-Over Links,” on page 46.

IMPORTANT: Check and update all of the sample graphics to give your own Web site a consistent look according to the design criteria of your company.

4.4 Updating Mouse-Over Links

Mouse-over links are dynamic links on your HTML Web page that change appearance when a user moves the mouse pointer over the link. Each of these links require two separate GIF files, one dormant file that displays normally on the Web page (Figure 4-3) and one active file, designated with the `_on` extension in its name, that is displayed when the mouse pointer hovers on the link (Figure 4-4).

Figure 4-3 *Dormant* `medical.gif`

Figure 4-4 *Active* `medical_on.gif`

The `index.php` file always defines where and how your GIF files are displayed on the active HTML Web page, as shown in the following code sample:

```
91          <tr>.
92                  <td><a href="http://spd.provo.novell.com:8080/nidp" onMouseOut="MM_swapImgRestore()" .
93                  onMouseOver="MM_swapImage('Image15','','images/medical_on.gif',1)">.
94                  <img src="images/medical.gif" name="Image15" width="196" height="86" border="0"></a></td>.
95                  <td>.
```

The following procedure explains how to update these mouse-over links with your own replacement graphics:

1. Follow basically the same procedure outlined in Step 1through Step 6 on page 45 for the mouse-over links that you want to update.

   Keep in the mind the pixel size requirements specified for your GIF files in `index.php`.
2. Name your new files *`[your_link]`*`.gif` and *`[your_link]`*`_on.gif`.
3. In the `htdocs/images` folder, replace the original dormant and active GIFs with your new *`[your_link]`*`.gif` and *`[your_link]`*`_on.gif` files.
4. In the PHP code editor, search for all instances of the `old medical.gif` and `medical_on.gif` files and replace with your new *`[your_link]`*`.gif` and *`[your_link]`*`_on.gif` files.
5. Save the `index.php` file.

4.5 Deploying Your Updated Example Web Service

After you have updated and saved your PHP and graphics files in the htdoc sample folder, deploy the Web service explained in Chapter 1, “Installation Overview,” on page 9.