HP Authentication Web Server

Administrator's Guide

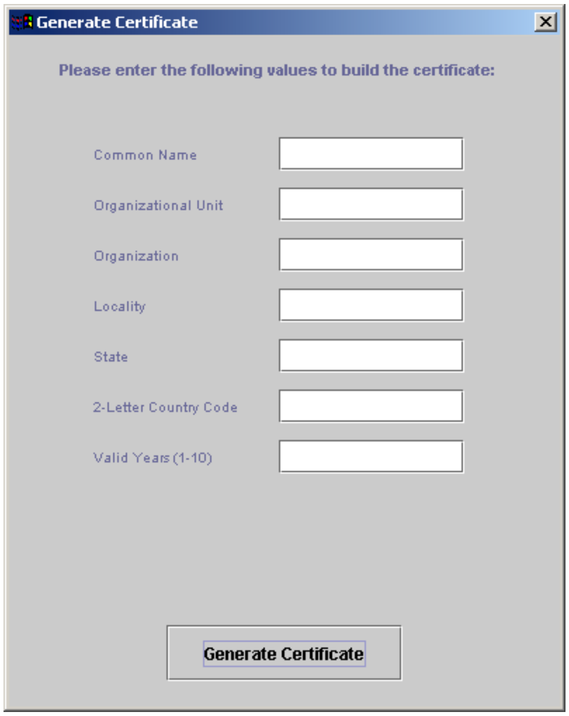
Contents

1. Generating Certificates for SSL Connections

The Authentication Server can be used for SSL connections through the digital sender. The Authentication Server requires a Server Certificate to serve SSL, and a Trusted Root Certificate Authority to sign the certificate. During the Authentication Server installation, Hewlett-Packard acts as the certificate authority and generates the Trusted Root Certificate. The Generate Certificate tool creates the Server Certificate (SADC) for the Authentication Server and automatically uses the Trusted Root to sign it.

To generate the certificate, click **Start,** click **Programs,** click **HP Authentication Web Server**, and then click **Generate Certificate**.

The following screen appears:



Please enter the following values to build the certificate:

Note: Each time the Generate Certificate tool is used, the new certificate (marked with the date on which it was generated and the expiration date) overwrites any previous certificates that the tool had generated.

Type the required information and click **Generate Certificate**. The certificate is generated automatically and the window disappears.

Field	**Description**
Common Name	The fully qualified hostname of the server on which the certificate is being installed
Organizational Unit	An administrator-selected identifier (for example, the department name)
Organization	An administrator-selected identifier (for example, the company name)
Locality	The name of the city or town where the server is located

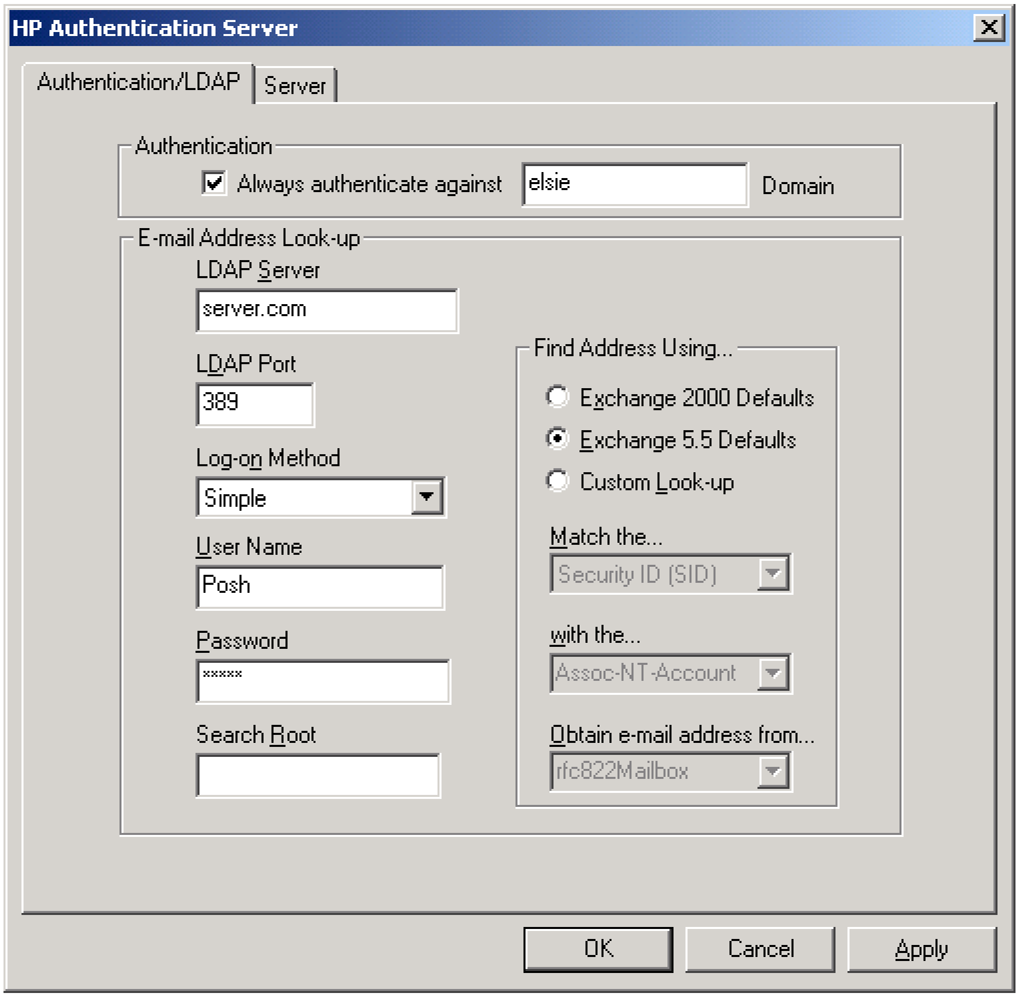
State	The full name of the state in which the server is located (do not abbreviate)
2-Letter Country Code	The two-letter code for the country in which the server is located (for example, US)
Valid Years(1-10)	The length of time during which the certificate is to be valid

2. Using the HP Authentication Web Server Control Panel Applet

The Authentication Server is an NT service that must be configured the first time it is used. Use the HP Authentication Web Server Control Panel Applet to configure the Authentication Server. To open the applet, click **Start,** click **Settings,** click **Control Panel,** and then click **HP Authentication Web Server**.

Authentication/LDAP Tab

Use the Authentication/LDAP tab to configure the HP Authentication Web Server LDAP parameters.



Authentication
☑ Always authenticate against: elsie Domain

E-mail Address Look-up

LDAP Server: server.com

LDAP Port: 389

Log-on Method: Simple

User Name: Posh

Password: *****

Search Root:

Find Address Using...

○ Exchange 2000 Defaults
● Exchange 5.5 Defaults
○ Custom Look-up

Match the... Security ID (SID)

with the... Assoc-NT-Account

Obtain e-mail address from... rfc822Mailbox

Authentication Domain

The Authentication Server authenticates against several different options for the domain.

If the **Always authenticate against *X* domain** check box is clear (not selected), the Authentication Server uses the following procedure to retrieve the domain:

a) If the digital sender provides a domain with the userid, then that domain is used for authentication. (If the domain is not the computer's default domain, a trust relationship must be set up between the domains.)

b) If the digital sender does not provides a domain with the userid, then the default domain of the computer on which the Authentication Server resides is used for authentication.

If the **Always authenticate against *X* domain** check box is selected, the Authentication Server uses the following procedure to retrieve the domain:

a) If the domain provided is a valid domain, the Authentication Server uses that domain for authentication.

b) If the domain provided does not exist, the Authentication Server authenticates against the local computer.

c) If a domain is not provided, the Authentication Server authenticates against the default domain of the local computer.

E-mail Address Look-up

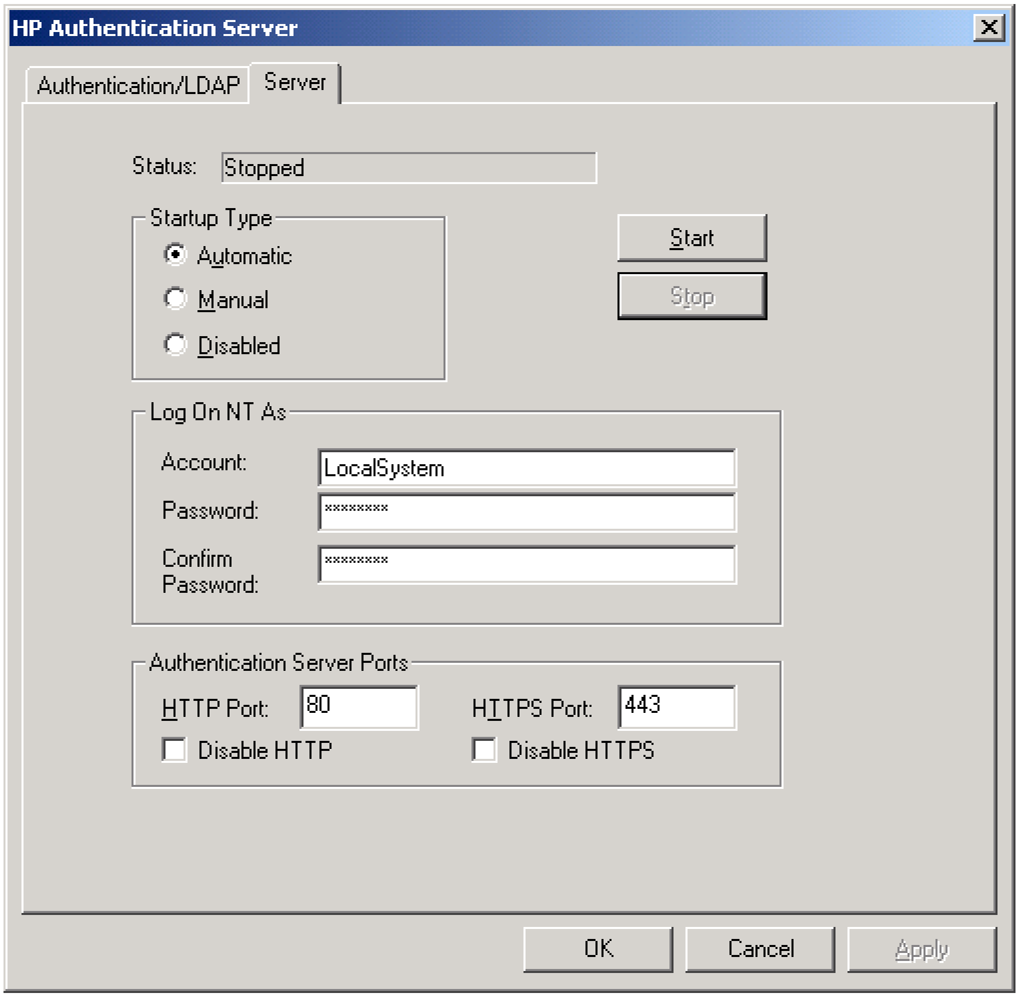
After the Authentication Server authenticates a user, it seeks the user's e-mail address from the LDAP Server. The Authentication Server must have the following information in order to connect to and query the LDAP Server:

Field	Description
LDAP Server	The IP address or domain name of the LDAP Server.
LDAP Port	The port that the LDAP Server listens to for queries. The default LDAP port is 389 (for use with Anonymous and Simple log-on methods). The LDAP port for SSL is 636 (for use with the SSL log-on method only).
Log-on Method	The method that the Authentication Server uses to bind to the LDAP server. The following choices are provided: 1. **Anonymous**. No user name or password is provided to the LDAP Server. The LDAP Server must allow the anonymous log on, and the anonymous log on must have sufficient access rights to perform the queries. See "Anonymous Binding to LADP Servers" for configuration information. 2. **Simple** (Clear Text). The user name and password are sent from the Authentication Server to the LDAP Server in plain-text form (unencrypted). 3. **SSL**. SSL is used to encrypt the user name and password that are sent from the Authentication Server to the LDAP Server. The proper certificates must be generated and then installed on the LDAP Server. See "SSL Binding to LADP Servers" for configuration information.

User Name	The Authentication Server uses this user name to bind to the LDAP Server. The user must have the proper access and rights to the LDAP Server. For Exchange 2000, the **User Name** must be prefixed by the domain name in the following format: domain\user.
Password	The LDAP user's password
Search Root	The LDAP search root. This is where the query will begin. For Exchange servers, the Search Root might look like this: cn=Users,dc=domainName, dc=com
Exchange 2000 Defaults	Information in this field resets the LDAP Query fields to the Exchange 2000 defaults as follows: Match the **User Name** with the **samAccountName;** Obtain e-mail address from **mail**
Exchange 5.5 Defaults	Information in this field resets the LDAP Query fields to the Exchange 5.5 defaults as follows: Match the **Security ID (SID)** with the **Assoc-NT-Account;** Obtain e-mail address from **rfc822Mailbox**
Custom Look-up	Information in this field allows Custom LDAP Query fields to be selected.
Match the *X*	Information in this field is used to build the LDAP Query that retrieves the e-mail address. The value in this field is matched against an LDAP field to find a specific user. The following are possible values for the field: 1. **Security ID (SID)**. The Windows Security ID associated with the authenticated user. 2. **Username**. The user name associated with the authenticated user. 3. **Domain/Username**. The domain/user name associated with the authenticated user.
With the *X*	The name of the LDAP field that the Match the *X* field is matched against. The following common LDAP field names are provided. If the necessary field is not in the list, it can be typed. 1. uid 2. cn 3. sn 4. givenName 5. Assoc-NT-Account 6. samAccountName
Obtain e-mail address from *X*	This is the name of the field that the LDAP Server uses to store e-mail addresses. The following field names are provided: 1. rfc822Mailbox 2. mail

Server Tab

Use the Server tab to specify the service startup type, assign a logon account, start and stop the service, and configure the Authentication Server ports for authentication with the digital sender. First, configure the ports for authentication. (See “Starting the Authentication Server” for more information.)



Status: Stopped

Startup Type
● Automatic
○ Manual
○ Disabled

Log On NT As
Account: LocalSystem
Password: ********
Confirm Password: ********

Authentication Server Ports
HTTP Port: 80
HTTPS Port: 443
□ Disable HTTP
□ Disable HTTPS

Startup Type Description

Choose the startup type:

Automatic (service starts every time the system starts)
Manual (service can be started by a user or a dependent service)
Disabled (service cannot be started)

Start the service after all settings discussed in this document are configured. **Stop** the service to edit settings.

The **Log On NT As** fields are completed by default when the Authentication Server is installed. Edit these fields only if a different logon account is required.

Configure the Authentication Server Ports for Authentication with the Digital Sender

The HP Authentication Web Server can be set up to accept HTTP requests on the HTTP port and/or SSL requests on the HTTPS port. The following information must be provided to the Authentication Server:

Field	Description
HTTP Port	The Authentication Server listens for HTTP requests on this port. The default HTTP port is 80. If you choose port 80, make sure no other Web service is running on this port.
HTTPS Port	The Authentication Server listens for HTTPS requests on this port. The default HTTPS port is 443.

3. Configuring the LDAP Server

Anonymous Binding to LDAP Servers

When binding to LDAP Servers anonymously, certain Authentication Server query fields might not be visible. The following sections describe how to make these fields visible on Exchange 5.5 and Exchange 2000 Servers.

Anonymous Binding to the Exchange 2000 Server

1. Click **Start,** click **Programs,** click **Administrative Tools,** and then click **Active Directory Users and Computers**.
2. Right-click **Users**, and then click **Properties**.
3. On the **Security** tab, click the **Everyone** group.
4. Make sure the **Read-Allow** check box is selected.

Anonymous Binding to the Exchange 5.5 Server

Anonymous connections do not automatically have access to all Exchange 5.5 fields. Specifically, they do not have access to the Assoc-NT-Account field that the Authentication Server uses to query Exchange 5.5 for a user. Use the following procedure to make this field visible to LDAP:

1. Run the Exchange admin tool in raw mode (for example, c:\exchsrvr\bin\admin.exe /r).
2. Click **View,** and then click **Raw Directory.** A new folder named Schema appears.
3. Click the Schema folder to get a list of attributes. Scroll to **Primary Windows NT Account** and double-click. Click **yes** to display the raw properties.
4. Select **Heuristics** from the **Object Attributes** list.

5. Change the value from 12 to 14. This turns on bit 1. The bits correspond roughly to the following:

   Bit 0: Replicate between sites
   Bit 1: Attribute visibility through LDAP
   Bit 2: Attribute access by authenticated clients
   Bit 3: Attribute is an operational attribute
6. Click **OK**.

SSL Binding to LDAP Servers

The HP Authentication Web Server supports communication to LDAP servers through SSL. This ensures that the authentication information is not being sent over the network in clear-text format. In order for this to work, a certificate must be installed on the LDAP Server. This certificate must also be installed on the Authentication Server in order for that server to trust the LDAP Server.

While it is possible to use third-party server certificates, only the procedures for using Microsoft Certificate Authority/Server on Exchange 2000 and Exchange 5.5 Servers are described in the following sections. If SSL communication over LDAP is already enabled, proceed to "Importing the LDAP Certificate to the HP Authentication Web Server."

SSL Binding to Exchange 2000

Use the following procedures to enable Active Directory support for SSL:

Install Certificate Services to Create a Server Certificate

Install Microsoft Certificate Services. This creates a Server Certificate and an Enterprise Certificate Authority.

Bind SSL to LDAP

1. Click **Start,** click **Programs,** click **Administrative Tools,** and then click **Active Directory Users and Computers**.

2. Right-click the domain, and then click **Properties.**

3. On the **Group Policy** tab, double-click **Default Domain Policy**.

4. Under **Computer Configuration**, expand **Windows Settings**.

5. Expand **Security Settings**, and then expand **Public Key Policies**.

6. Right-click **Automatic Certificate Request Settings,** click **New,** and then click **Automatic Certificate Request…**.

7. Use the **Automatic Certificate Request Wizard** to add a certificate template for Domain Controllers. Select the certificate installed above.

SSL Binding to Exchange 5.5 Server on Windows NT 4.0

Use the following procedure to enable Exchange 5.5 Server to accept SSL authentication:

<u>Install IIS, Certificate Server, and Exchange Server</u>

1. Make sure that Microsoft Windows NT 4.0 is installed with Service Pack 3.
2. Install Microsoft Internet Information Server (IIS) version 3.0 or later and Microsoft Certificate Server. **Important:** IIS must be installed before Exchange Server. If installation is not performed in this order, the protocols that Exchange Server supports will not be available in the IIS Key Manager. See Microsoft Support document Q175439 at http://www.microsoft.com.
3. Install Exchange Server version 5.0 or later.

<u>Select the Authentication Settings for LDAP</u>

1. In the **Exchange Server Administrator** program, expand the **Configuration** container, and click the **Protocols** object.
2. Double-click **LDAP**.
3. On the protocol property pages, click the **Authentication** tab, and then set the authentication levels.
4. Click **OK** to save the settings.

<u>Use the IIS Key Manager to Create a key request.</u>

1. Open **Internet Information Server**.
2. Click the **Key Manager** icon on the toolbar.
3. Locate the icon for your Exchange server, and select **LDAP**.
4. On the **Key** menu, click **Create New Key**.
5. Select the option to send the request automatically to a certificate authority.

6. Continue through the wizard and type the appropriate information in the fields.

7. When the wizard is complete, click **Finish**. The request is automatically sent to the MS Certificate Server and the key (Server Certificate) appears under the LDAP protocol.

8. If you are running IIS 4.0, you must specify the **server IP Address** or specify to bind the certificate to **Default**.

9. Close **Key Manager** and select **OK** to save the changes.

Importing the LDAP Certificate to the HP Authentication Web Server

After the certificate is installed on the LDAP Server, use the following procedure to import it to the Authentication Server:

For Windows 2000 Server

1. Click **Start,** click **Programs,** click **Administrative Tools,** and then click **Certification Authority**.

2. Right-click the certificate authority, and then click **Properties**.

3. Click the **View Certificate** button. The **Microsoft Certificate Viewer** opens.

4. On the **Details** tab, click the **Copy to File** button.

5. Specify to export the certificate in DER Encoded Binary X.509 (CER) format.

6. Browse to the Authentication Server installation directory and name the file **Exchange.cer**.

7. Click **Finish** when the wizard is complete.

8. Click**Start,** click **Programs,** click **HP Authentication Web Server,** and then click **Import LDAP Certificate**. The Exchange.cer file is automatically imported into Authentication Server's Trusted Root Certificate store.

For Windows NT 4.0 Server

1. Click **Start,** click **Find,** and then click **Files or Folders**…

2. Search on the file **cacerts.htm**.

3. Double-click the file. The .htm page opens and displays a link for the **Certificate Authority**.

4. Click the link and specify to open the file. The **Microsoft Certificate Viewer** opens.

5. On the **Details** tab, click the **Copy to File** button.

6. Specify to export the certificate in DER Encoded Binary X.509 (CER) format.

7. Browse to the Authentication Server installation directory and name the file **Exchange.cer**.

8. Click Finish when the wizard is complete.

9. Click **Start,** click **Programs,** click **HP Authentication Web Server,** and then click **Import LDAP Certificate**. This automatically runs the importCertificate.cmd batch file, which imports the Exchange.cer into Authentication Server's Trusted Root Certificate store.

Note: The password for the Authentication Server's Trusted Root Certificate store included in the batch file, pass123, is not protected. This does not create a security breach, because private keys are not stored in the Trusted Root Certificate store.

The SSL authentication method uses public/private key technology to ensure privacy. The SSL protocol resides at the Open Systems Interconnection (OSI) presentation layer and moves data from the application layer to the TCP transport layer. The SSL protocol is responsible for authentication, encryption, and verification of data integrity.

The authentication function ensures that the data is being sent to the correct server, and that the server is secure. Encryption ensures that no one other than the target server user can read the data. Data integrity ensures that the data has not been corrupted or altered in transit.

4. Starting the Authentication Server

Now that all settings have been configured, the HP Authentication Web Server service can be started. (See "Server Tab" for information about starting the service.)

Cluster Support

When the HP Authentication Web Server is run on a cluster, the service should be started through the Cluster Administrator, not by using the control panel applet. The Cluster Administrator will continue to show the status (started or stopped) that the Cluster Administrator last set, even if the CPL applet was used to change the status.

5. Testing the Authentication Server

The following procedures can be used to test that the Authentication Server is working properly when configured for HTTP or HTTPS:

HTTP (Clear Text) Authentication

1. Point your browser to the Authentication Server on the network that uses **HTTP** (for example, http://hostname).
2. When prompted, type a user name and password that belong to a valid user on your network. You should receive the e-mail address associated with that user name.

HTTPS (SSL) Authentication

1. Open the Authentication Server folder at **C:\program files\hewlett packard**.
2. Double click the file **CA.crt** to open the **Certificate** window.
3. Click **Install Certificate** to start the install certificate wizard.
4. Continue through the wizard, leaving all defaults selected.
5. Click **OK** on the dialog box that appears when the wizard is finished. The Trusted Root Certificate is now installed in the Trusted Root Certificate store on the computer.
6. Point your browser to the Authentication Server on the network that uses **HTTPS** (for example, https://hostname).
7. When prompted, type a user name and password that belong to a valid user on your network. You should receive the e-mail address associated with that user name.

Note: The Trusted Root Certificate installed above is already present on the digital sender.

Data passed between the digital sender and the Authentication Server is encrypted through the SSL connections when both are configured for SSL. Because the Trusted Root certificate that signed the Authentication Server certificate is installed on the digital sender, the digital sender can verify that it is communicating with the Authentication Server, and that it is not sending data to another machine. This ensures totally secure communication between the digital sender and the Authentication Server.

6. Configuring the Digital Sender for Authentication

Now that Authentication Server software has been installed and configured on your network, the digital sender must be configured to authenticate to the Authentication Server. You must have the latest version of digital sender firmware, version 5.01, which can be found on the 5.1 product CD-ROM or downloaded from http://digitalsender.hp.com.

Use the following procedure to configure the digital sender to authenticate to Authentication Server:

1. Point your browser to the digital sender that you want to configure, using either the IP address or the hostname followed by port :4242
(e.g. http://15.15.15.15:4242 or http://hostname:4242).

2. Click the **Settings** menu, and then click **Authentication**.

3. On the **Authentication** screen:
    a. Make sure that **Enable Login** is selected.
    b. Type the fully qualified hostname of the Authentication Server in the **URL** field.
        i. Use **HTTP** for Clear Text Web Authentication.
        ii. Use **HTTPS** for SSL Web Authentication.
    c. In the **Default Domain** field, type the default Domain Name that the Authentication Server uses.
    d. Fill in the **Proxy Address** and **Proxy Port** fields if the Authentication Server is outside the firewall. If the server is inside the firewall on your company intranet, leave these fields blank.

4. Click the **Apply** button at the bottom of the screen.

5. Click the **Configure "From:" Filed Address** link.

6. On the **E-mail Settings** screen, select **HP Auth Web Server** in the **E-mail "From:" Field Data Source:** field.
Note: Although **HP Auth Web Server** is the default for Authentication Server, the other options in this menu can be also used. If you select **LDAP, Login,** or **Suffix** in this menu, you *must* make sure that LDAP is disabled on the Authentication Server. Click **Help** on the **E-mail Settings** page for details about the other options.

7. Click the **Apply** button at the bottom of the screen.

8. Click **Authentication** on the navigation menu.

9. On the **Authentication** screen, click the **Test Login to Authentication Server** button.

10. On the **Test Login** screen, type the user name and password you used in step 1, and then click **Apply**. You should receive a message that says "Login Successful!" and the e-mail address associated with that user name.

11. After you have successfully logged in from the Web Access tool, you can go to the digital sender and log in at the control panel.

To configure multiple digital senders to authenticate to the HP Authentication Web Server, replicate the **E-mail Settings** and **Authentication Settings** by using the **Replicate** tool in Web Access. Click **Help** on the **Replicate** page in Web Access for more information.