HP-UX Directory Server administration server guide

HP-UX Directory Server Version 8.1

HP Part Number: 5900-0312
Published: September 2009
Edition: 1

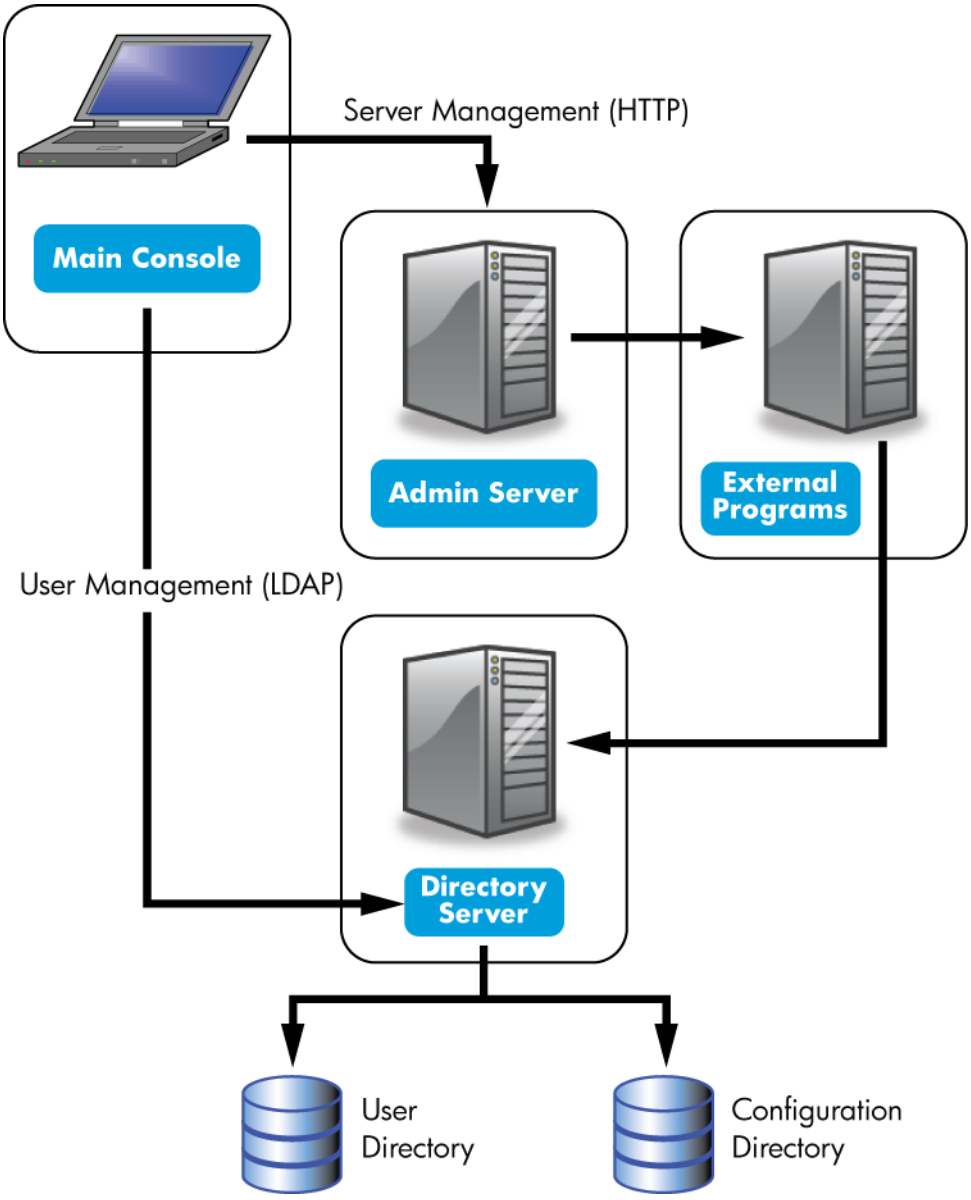
Table of Contents

1 Introduction to HP-UX Directory Server

Identity management and directory services with HP-UX Directory Server use three components, working in tandem:

- A Java-based management console
- An administration server which also functions as a web server
- An LDAP directory server

Figure 1-1 Interactions between the Console, Admin Server, and Directory Server



The Admin Server processes configuration requests for Directory Server instances and performs many common server tasks, such as stopping and starting server instances. Directory services are usually divided into two categories:

- Configuration databases, which store the Console and Admin Server settings and some Directory Server configuration.
- User databases, which contain user and group information.

These databases can be kept in the same Directory Server instance, but it is also possible to break these services into separate Directory Server instances. In that case, a Directory Server instance's configuration is stored in a separate Directory Server, called the Configuration Directory Server, and user data is stored in the User Directory Server. Because the Admin Server processes server configuration requests for the HP-UX Directory Server, the Configuration Directory Server and User Directory Server instances are both defined in the Admin Server configuration.

As a web server, the Admin Server provides all the online functions of the Directory Server, including handling connections to the Console and hosting web applications such as Admin Express. Clients connect to the Admin Server both over secure and standard connections, since the Admin Server supports both HTTP or HTTPS, if **SSL**/**TLS** is enabled.

When HP-UX Directory Server is installed, then the Admin Server is automatically installed and configured as well. There can be multiple Directory Server instances on a single machine, and all use the same instance of Admin Server.

NOTE: There can be only one Admin Server per machine. This single Admin Server instance can handle multiple instances of Directory Server and other clients which can use the Admin Server.

When the Console is opened to manage an instance of Directory Server, even if the Console is on a different machine than the server instance being managed, it contacts the local Admin Server instance to perform the requested tasks. For example, Admin Server can execute programs to modify the server and application settings that are stored in the configuration directory or to change the port number that a server listens to.

The Admin Server itself can be managed through its own Java-based interface, by editing its configuration files, or through command-line tools.

2 Admin Server configuration

The Admin Server is a separate server from the HP-UX Directory Server, although they work interdependently. The Admin Server processes, file locations, and configuration options are also separate. This chapter covers the Admin Server information, including starting and stopping the Admin Server, enabling SSL, viewing logs, and changing Admin Server configuration properties, such as the server port number.

2.1 Directory Server file locations

HP-UX Directory Server conforms to the Filesystem Hierarchy Standards. For more information on FHS, see the FHS homepage, http://www.pathname.com/fhs/.

The following table specifies the location of files and directories installed with Directory Server:

Table 2-1 Location of Directory Server files and directories

File or directory	Location
Log files	`/var/opt/dirsrv/admin-serv/log`
Configuration files	`/etc/opt/dirsrv/admin-serv`
Runtime files	`/var/opt/dirsrv/admin-serv/run`
Binaries	`/opt/dirsrv/bin` `/opt/dirsrv/sbin`
Libraries	`/opt/dirsrv/lib`

2.2 Starting and stopping the Admin Server

The Admin Server is running when the `setup-ds-admin.pl` configuration script completes. Avoid stopping and starting the server to prevent interrupting server operations.

- When starting in SSL, the start script prompts for the password for the security (SSL certificate) database. It is possible to restart in SSL without being prompted for a password by using a password file. See "Creating a password file for the Admin Server" for more information.

  If there is not password file, then the Admin Server cannot be restarted in SSL through the Console, only the command-line scripts.

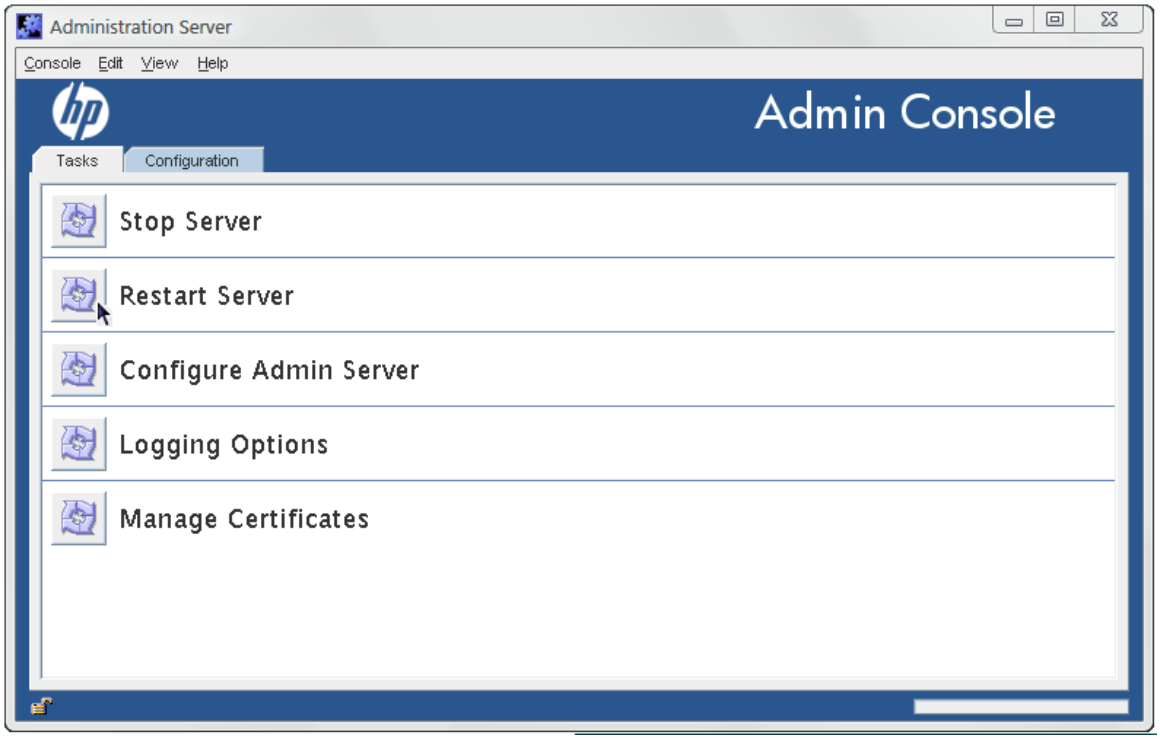
- Rebooting the host system can automatically start the Admin Server's `httpd` process. The script `/sbin/init.d/Hpds-adm` starts `httpd` if the parameter `HPDS_ADMIN` is set to `1` in `/etc/rc.config.d/Hpds-adm`. Setting `HPDS_ADMIN` to `0` disables the automatic start up.

2.2.1 Starting and stopping Admin Server from the console

1. Start the Console, and open the Admin console.

   ```
   /opt/dirsrv/bin/hpds-idm-console -a http://localhost:9830
   ```

2. In the **Tasks** tab, click **Restart Server** or **Stop Server**.



When the Admin Server is successfully started or stopped from the Console, the server displays a message box stating that the server has either started or shut down.

2.2.2 Starting and stopping Admin Server from the command Line

The following scripts start, stop, or restart the Admin Server:

Start: `/opt/dirsrv/sbin/start-ds-admin`

Stop: `/opt/dirsrv/sbin/stop-ds-admin`

Restart: `/opt/dirsrv/sbin/restart-ds-admin`

2.3 Opening the Admin Server console

Run the following script to launch the main Console:

`/opt/dirsrv/bin/hpds-idm-console`

When the login screen opens, the Admin Server prompts for the username, password, and Admin Server location. The Admin Server location is a URL; for a standard connection, this has the `http:` prefix for a standard HTTP protocol. If SSL/TLS is enabled, then this uses the `https:` prefix for the secure HTTPS protocol.

Figure 2-1 Login box

TIP:

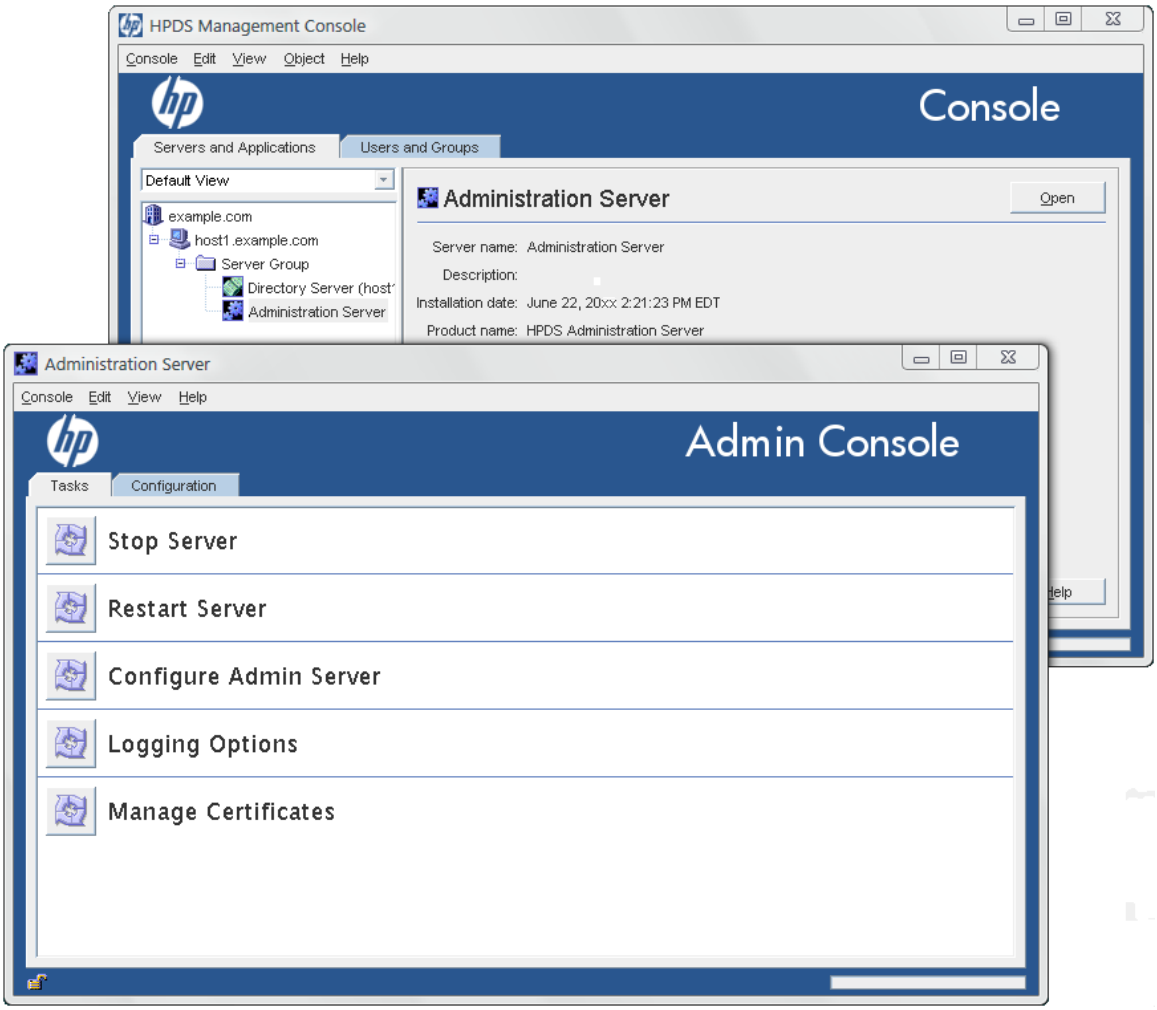
It is possible to send the Admin Server URL and port with the start script. For example:

```
/opt/dirsrv/bin/hpds-idm-console -a http://localhost:9830
```

The `-a` option is a convenience, particularly for logging into a Directory Server for the first time. On subsequent logins, the URL is saved. If the Admin Server port number is not passed with the `hpds-idm-console` command, then the server prompts for it at the Console login screen.

This opens the main Console window. To open the Admin Server Console, select the Admin Server instance from the server group on the left, then click the **Open** at the top right of the window.

Figure 2-2 The Admin Server console



2.4 Viewing logs

Log files monitor activity for Admin Server and can help troubleshoot server problems. Admin Server logs use the Common Logfile Format, a broadly supported format that provides information about the server.

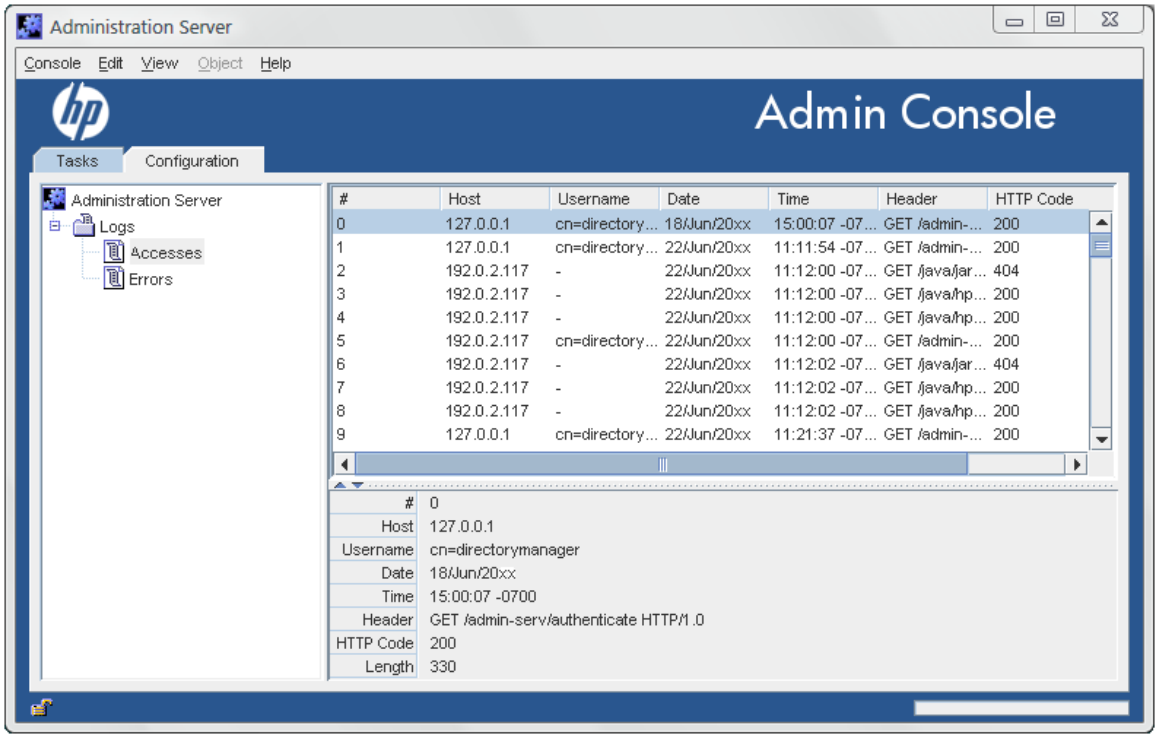
Admin Server generates two kinds of logs:

Access logs	Access logs show requests to and responses from the Admin Server. By default, the file is located at `/var/opt/dirsrv/admin-serv/log/access`.
Error logs	Error logs show messages for errors which the server has encountered since the log file was created. It also contains informational messages about the server, such as when the server was started and who tried unsuccessfully to log on to the server. By default, the file is located at `/var/opt/dirsrv/admin-serv/log/error`.

The logs can be viewed through Admin Server Console or by opening the log file.

2.4.1 Viewing the logs through the console

1. Open the Admin Server management window.
2. Click the **Configuration** tab.
3. Expand the **Logs** directory, and click the log file name, either **Accesses** or **Error**.



2.4.2 Viewing logs in the command line

The access log, by default, is at `/var/opt/dirsrv/admin-serv/log/access`. To view the access log, open it with a paging utility such as `more`.

Access logs show connections to the Admin Server based on the IP address of the client, the username, and the method that the request was sent. Each line has the following format:

`ip_address - bind_DN [timestamp -0500] "GET|POST cgi" HTTP_response bytes`

Example logs are shown in Example 2-1 “Example access logs”.

Example 2-1 Example access logs

```
127.0.0.1 - cn=directory manager [23/Dec/2009:19:32:52 -0500] "GET
/admin-serv/authenticate HTTP/1.0" 200 338
192.168.123.121 - cn=directory manager [23/Dec/2009:19:33:14 -0500] "POST
/admin-serv/tasks/Configuration/ServerSetup HTTP/1.0" 200 244
192.168.123.121 - cn=directory manager [23/Dec/2009:19:33:16 -0500] "GET
/admin-serv/tasks/Configuration/ReadLog?op=count&name=access HTTP/1.0"
200 10
```

The error log, by default, is at `/var/opt/dirsrv/admin-serv/log/error`. To view the error log, open it with a paging utility such as `more`.

Error logs record any problem response from the Admin Server. Like the access log, error logs also records entries based the client's IP adress, along with the type of error message, and the message text:

`[timestamp] [severity] [client ip_address error_message`

The *`severity`* message indicates whether the error is critical enough for administrator intervention. `[warning]`, `[error]`, and `[critical]` require immediate administrator action. Any other severity means the error is informational or for debugging.

Example logs are shown in Example 2-2 “Example error logs”.

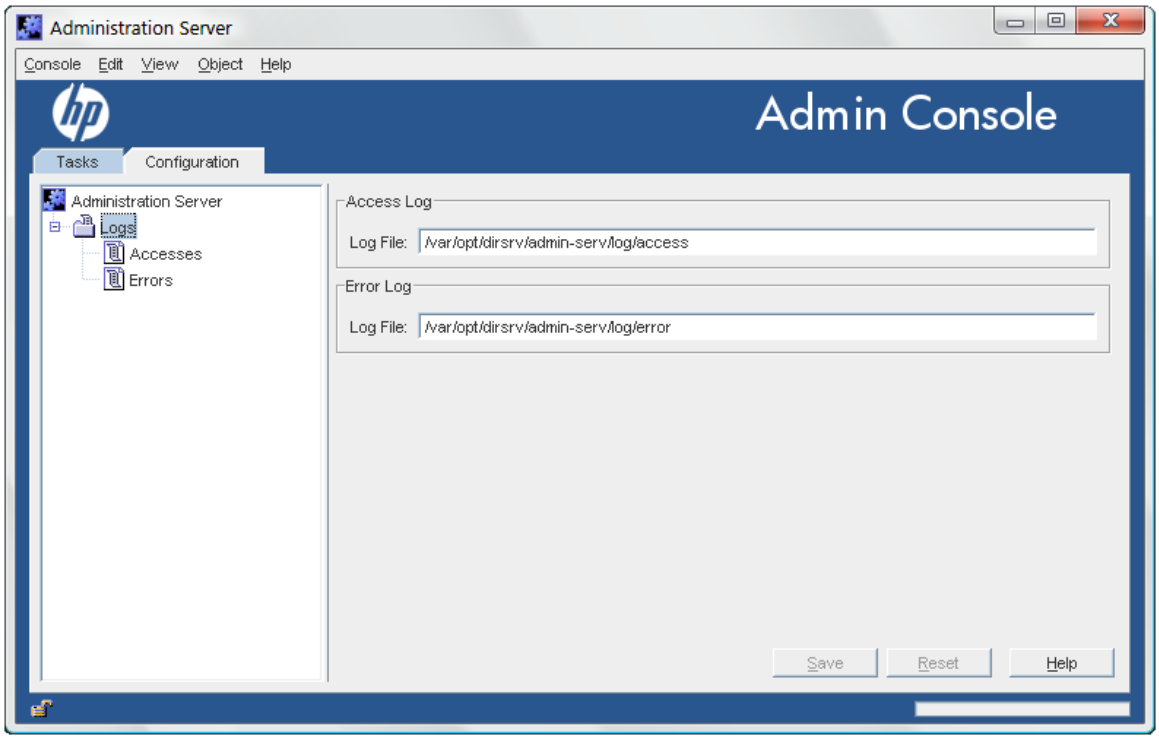
Example 2-2 Example error logs

```
[Mon Dec 22 23:44:59 2009] [notice] [client 127.0.0.1] adm\
serv_host_ip_check: ap_get_remote_host could not resolve 127.0.0.1
[Mon Dec 22 23:44:59 2009] [notice] [client 127.0.0.1] adm\
serv_host_ip_check: host [localhost.localdomain] did not match pattern
[*.example.com] -will scan aliases
[Mon Dec 22 23:44:59 2008] [notice] [client 127.0.0.1] adm\
serv_host_ip_check: host alias [localhost] did not match pattern
[*.example.com]
[Mon Dec 22 23:44:59 2008] [notice] [client 127.0.0.1] adm\
serv_check_authz(): passing [/admin-serv/authenticate] to the userauth
handler
[Mon Dec 22 23:45:16 2008] [notice] [client 192.168.123.121] adm\
serv_host_ip_check: ap_get_remote_host could not resolve 192.168.123.121
```

2.4.3 Changing the log name in the console

The access and error log files' names can be changed to rotate the files. This rotation has to be done manually to create new files if the existing log files become too large.

1. Open the Admin Server management window.
2. Click the **Configuration** tab.
3. Click **Logs** in the left panel.
4. In the **Logs** window on the right, enter the new log file name.



WARNING!

The path to the log file is absolute and cannot be changed.

5. Click **OK** to save the changes.
6. Open the **Tasks** tab, and click the **Restart Server** button to restart the server and apply the changes.

2.4.4 Changing the log location in the command line

The access and error log files' names and locations can be changed to rotate the files. This rotation has to be done manually to create new files if the existing log files become too large. The location can be changed if the default location in `/var/opt/dirsrv/admin-serv/log` does not meet the application needs.

The Admin Server configuration is stored in two locations. The main entry is an LDAP entry in the Configuration Directory Server's `o=NetscapeRoot` database. The other is the `console.conf` file. Changing the log settings requires changing both settings.

1. Edit the Admin Server configuration entry in the Configuration Directory Server.
   a. Get the name of the Admin Server entry. Because the Admin Server entry has a special **object class**, `nsAdminConfig`, it is possible to search for the entry using that object class to retrieve the DN.

      ```
      ldapsearch -D "cn=directory manager" -w secret -p 389 -h server.example.com \
      -b "o=NetscapeRoot" "(objectclass=nsAdminConfig)" dn

      version:1
      dn: cn=configuration, cn=admin-serv-example, cn=HPDS Administration
      Server, cn=Server Group, cn=server.example.com, ou=example.com,
      o=NetscapeRoot
      ```

   b. The Admin Server entry can be edited using `ldapmodify`. The access and error log settings are stored in the `nsAccessLogs` and `nsErrorLogs` attributes, respectively. For example:

      ```
      ldapmodify -D "cn=directory manager" -w secret -p 389 -h server.example.com

      dn: cn=configuration, cn=admin-serv-example, cn=HPDS Administration
      Server, cn=Server Group, cn=server.example.com, ou=example.com,
      o=NetscapeRoot
      changetype:modify
      replace:nsAccessLog
      nsAccessLog:/var/opt/dirsrv/admin-serv/log/access_new
      ```

      Click **Enter** twice to submit the operation, then **Control-C** to close `ldapmodify`.

2. Open the Admin Server configuration directory.

   ```
   cd /etc/opt/dirsrv/admin-serv
   ```

3. Edit the `console.conf` file. For the access log, edit the path and file name in the `CustomLog` parameter. For the error log, edit the path and file name in the `ErrorLog` parameter.

   ```
   CustomLog /var/opt/dirsrv/admin-serv/log/access_new common
   ErrorLog /var/opt/dirsrv/admin-serv/log/error_new
   ```

   Leave the term `common` after the access log path; this means that the access log is in the Common Log Format.

4. Restart the Admin Server.

   ```
   /opt/dirsrv/sbin/restart-ds-admin
   ```

2.5 Changing the port number

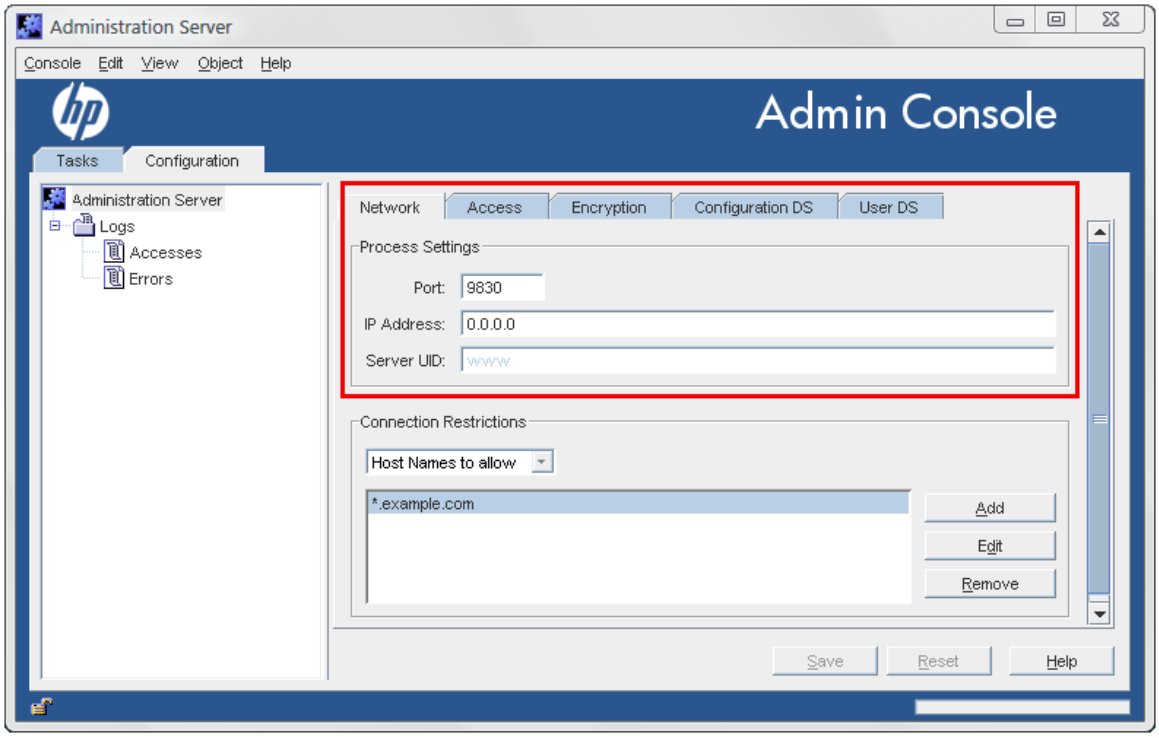
The *`port number`* specifies where an instance of Admin Server listens for messages.

The default port number for Admin Server is set when the instance is first installed and the configuration script, such as `setup-ds-admin.pl`, is run. The default port number is `9830`, although if that number is in use, then the setup program will use a randomly-generated number larger than `1024` or one can assign any port number between `1025` and `65535`.

2.5.1 Changing the port number in the console

1. Open the Admin Server management window.
2. Click the **Configuration** tab.

3. Click the **Network** tab.



4. Enter the port number for the Admin Server instance in the **Port** field. The Admin Server port number has a default number of `9830`.
5. Click **OK**.
6. Open the **Tasks** tab, and click the **Restart Server** button to restart the server and apply the changes.
7. Close the Console, then restart the Console, specifying the new Admin Server port number in the connection URL.

2.5.2 Changing the port number in the command line

The port number for the Admin Server is `9830` by default.

The Admin Server configuration is stored in two locations. The main entry is an LDAP entry in the Configuration Directory Server's `o=NetscapeRoot` database. The other is the `console.conf` file. Changing the port number requires changing both settings.

1. Edit the Admin Server configuration entry in the Configuration Directory Server.
   a. Get the name of the Admin Server entry. Since the Admin Server entry has a special object class, `nsAdminConfig`, it is possible to search for the entry using that object class to retrieve the DN.

```
ldapsearch -D "cn=directory manager" -w secret -p 389 -h server.example.com \
-b "o=NetscapeRoot" "(objectclass=nsAdminConfig)" dn

version:1
dn: cn=configuration, cn=admin-serv-example, cn=HPDS Administration
Server, cn=Server Group, cn=server.example.com, ou=example.com,
o=NetscapeRoot
```

   b. The Admin Server entry can be edited using `ldapmodify`. The port number is set in the `nsServerPort` attribute. For example:

```
ldapmodify -D "cn=directory manager" -w secret -p 389 -h server.example.com

dn: cn=configuration, cn=admin-serv-example, cn=HPDS Administration
Server, cn=Server Group, cn=server.example.com, ou=example.com,
o=NetscapeRoot
```

```
changetype:modify
replace:nsServerPort
nsServerPort:10030
```

Click **Enter** twice to submit the operation, then **Control+C** to close `ldapmodify`.

2. Open the Admin Server configuration directory.

   `cd /etc/opt/dirsrv/admin-serv`

3. Edit the `Listen` parameter in the `console.conf` file.

   ```
   Listen 0.0.0.0:10030
   ```

4. Restart the Admin Server.

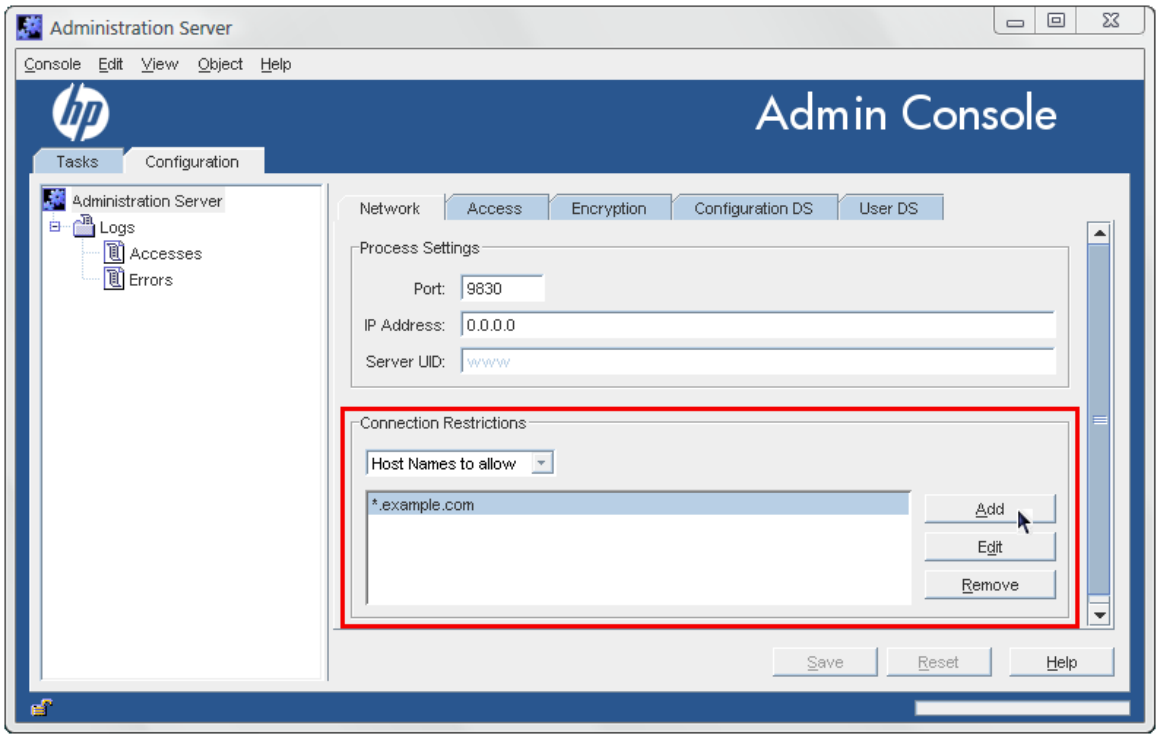
   ```
   /opt/dirsrv/sbin/restart-ds-admin
   ```

2.6 Setting host restrictions

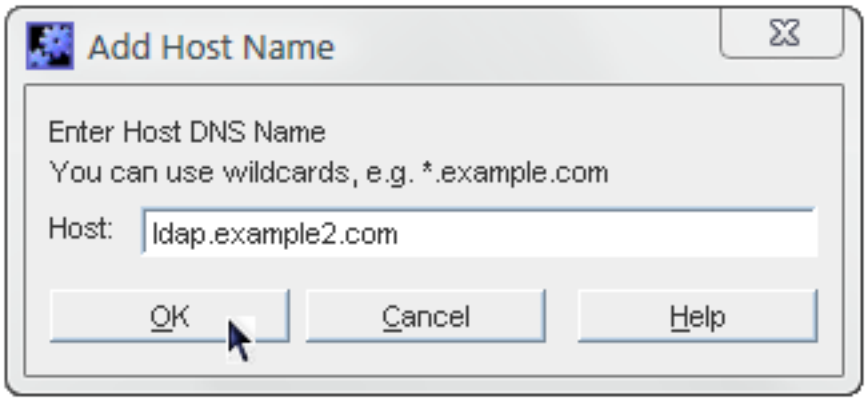
Connection restrictions specify which hosts are allowed to connect to the Admin Server. You can list these hosts by DNS name, IP address, or both. Only host machines listed within the connection restriction parameters are allowed to connect to the Admin Server. This setting allows wildcards within a domain or an IP address range to make setting connection restrictions simpler.

2.6.1 Setting host restrictions in the console

1. Open the Admin Server management window.
2. Click the **Configuration** tab.
3. Click the **Network** tab.
4. The **Connection Restrictions** area displays a list of hosts allowed to connect to the Admin Server. The drop-down list specifies whether the list entries are added by DNS name or by IP address. The list is evaluated first by host names, then by IP addresses.



5. Click the **Add** button to add another host to the list of allowed computers. To add a **host name**, make sure the drop-down list at the top reads **Host Names to allow**; to add an IP address, select **IP Addresses to allow**.
6. Fill in the host information.



The * wildcard can be used to specify a group of hosts. For instance, `*.example.com` allows all machines in the `example.com` domain to access the instance. Entering `205.12.*.` allows all hosts whose IP addresses begin with `205.12` to access the instance.

When specifying IP address restrictions, include all three separating dots. If you do not, the Admin Server returns an error message.

7. Click **OK** to close the **Add...** dialog box, then click the **Save** button to save the new host.
8. Open the **Tasks** tab, and click the **Restart Server** button to restart the server and apply the changes.

To change the information for a host or IP address listed, click the **Edit** button and change the given information. To remove an allowed host or IP address, select the host from the list, and click **Remove**. **Admin Server**.

2.6.2 Setting host restrictions in the command line

Host restrictions sets rules for what network clients can connect to the Admin Server and, therefore, to services which use the Admin Server. There are two kinds of host restrictions, restrictions based on the host or domain name and restrictions based on the IP address.

The Admin Server host restrictions are set in the main configuration entry in the Configuration Directory Server's `o=NetscapeRoot` database. There are two attributes for setting host restrictions, `nsAdminAccessAddresses` and `nsAdminAccessHosts` for IP addresses and host names, respectively.

NOTE:

The Admin Server supports both IPv4 and IPv6 addresses.

The Admin Server entry can be edited using `ldapmodify`.

To set host restrictions:

1. Get the name of the Admin Server entry. Since the Admin Server entry has a special object class, `nsAdminConfig`, it is possible to search for the entry using that object class to retrieve the DN.

```
ldapsearch -D "cn=directory manager" -w secret -p 389 -h server.example.com \
-b "o=NetscapeRoot" "(objectclass=nsAdminConfig)" dn

version:1
dn: cn=configuration, cn=admin-serv-example, cn=HPDS Administration
Server, cn=Server Group, cn=server.example.com, ou=example.com,
o=NetscapeRoot
```

2. To set IP address-based restrictions, edit the `nsAdminAccessAddresses` attribute.

```
ldapmodify -D "cn=directory manager" -w secret -p 389 -h server.example.com

dn: cn=configuration, cn=admin-serv-example, cn=HPDS Administration
Server, cn=Server Group, cn=server.example.com, ou=example.com,
```

```
o=NetscapeRoot
changetype:modify
replace:nsAdminAccessAddresses nsAdminAccessAddresses:72.5.*.*
```

Click **Enter** twice to submit the operation, then **Ctrl-C** to close `ldapmodify`.

The `nsAdminAccessAddresses` value can use wildcards to allow ranges. For example, to allow all IP addresses:

```
nsAdminAccessAddresses:*
```

To allow only a subset of addresses on a local network:

```
nsAdminAccessAddresses:192.168.123.*
```

3. To set host name or domain-based restrictions, edit the `nsAdminAccessHosts` attribute.

```
ldapmodify -D "cn=directory manager" -w secret -p 389 -h server.example.com

dn: cn=configuration, cn=admin-serv-example, cn=HPDS Administration
Server, cn=Server Group, cn=server.example.com, ou=example.com,
o=NetscapeRoot
changetype:modify
replace:nsAdminAccessHosts
nsAdminAccessHosts:*.example.com
```

Click **Enter** twice to submit the operation, then **Control+C** to close `ldapmodify`.

4. Restart the Admin Server to apply the changes.

```
/opt/dirsrv/sbin/restart-ds-admin
```

2.7 Changing the admin user's name and password

During installation, you are asked to enter a username and password for the *`Configuration Administrator`*, the user authorized to access and modify the entire configuration directory. The Configuration Administrator entry is stored in the directory under the following DN:

`uid=`*`userID`*`,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot`

The Configuration Administrator's username and password are managed through the Directory Server and are represented in an LDAP entry; this is described in the *HP-UX Directory Server administrator guide*.

During installation, the Configuration Administrator's username and password are used to automatically create the *`Administration Server Administrator`*. This user can perform a limited number of administrative tasks, such as starting, stopping, and restarting servers in a local server group. The Administration Server Administrator is created for the purpose of logging into the Console when the Directory Server is not running.

The Administration Server Administrator does not have an LDAP entry; it exists only as an entity in a local configuration file, `/etc/opt/dirsrv/admin-serv/admpw`.

Even though they are created at the same time during installation, and are identical at that time, the Configuration Administrator and Administration Server Administrator are two separate entities. If you change the username or password for one in the Console, the Console does not automatically make the same changes for the other.

The Administration Server Administrator has full access to all configuration settings in the Admin Server. The information for the admin user is set on the **Access** tab in the Console.

NOTE:

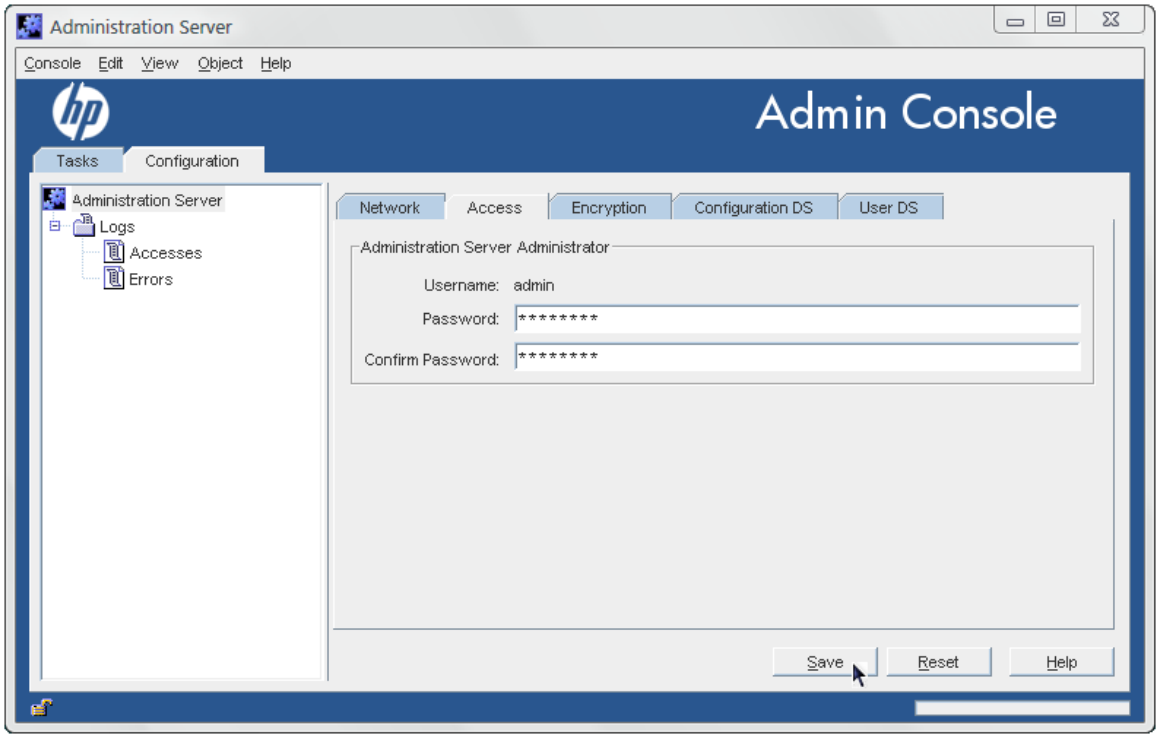
The Admin Server administrator username and password are stored in the `/etc/opt/dirsrv/admin-serv/admpw` file. For example:

```
admin:{SHA}W6ph5Mm5Pz8GgiULbPgzG37mj9g=
```

The password is encrypted and cannot be changed directly in the `admpw` file. The username can be changed in this file, but cannot be used to log into the Console unless the password is updated in the Console first. For this reason, it is better to edit the Administration Server Administrator username and password only through the Admin Server Console.

To change the Administration Server Administrator's ID or password:

1. Open the Admin Server management window.
2. Click the **Configuration** tab.
3. Click the **Access** tab.
4. Change the admin user's name or password. The username is the ID given for logging into the Admin Server.



5. Click **Save**.

2.8 Working with SSL

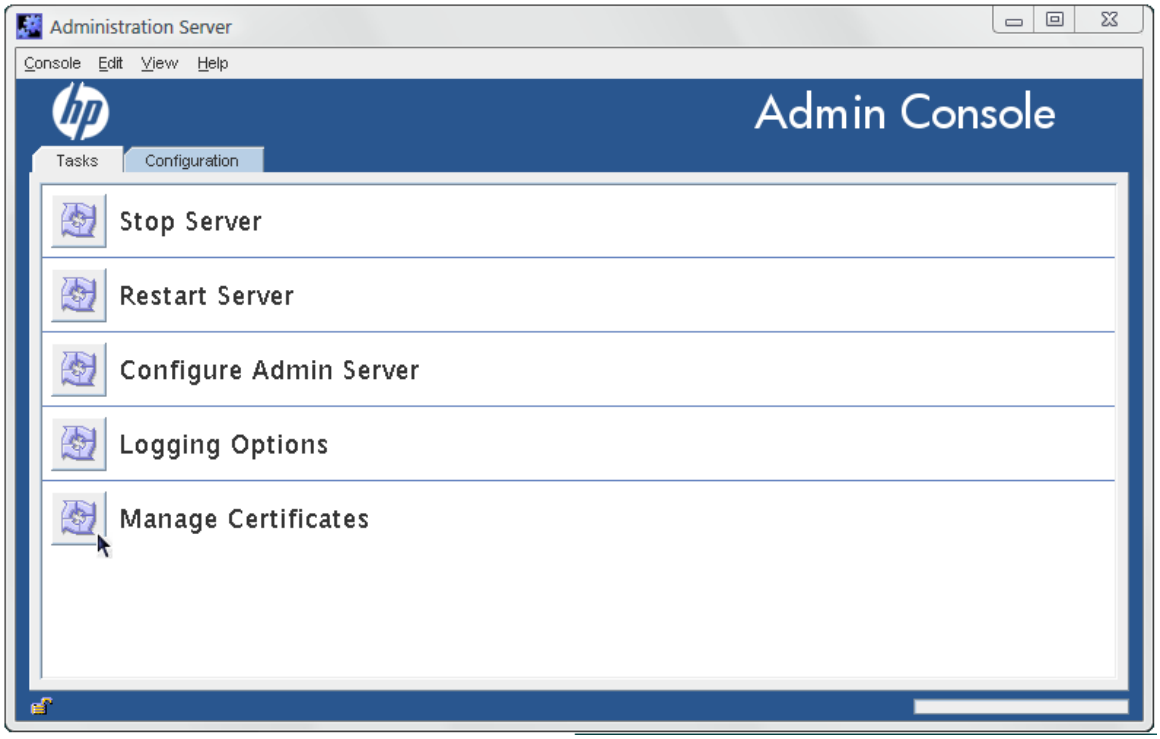
The Admin Server can run over HTTPS (secure HTTP) if SSL is enabled on the server. There are steps to enabling SSL:

1. Generating and submitting a certificate request.
2. Receiving and installing the certificate.
3. Trusting the certificate authority (CA) which issued the certificate.
4. Changing the Admin Server configuration to allow SSL connections.

2.8.1 Requesting and installing a server certificate

The Admin Server Console has a tool, the **Certificate Request Wizard**, which generates a valid certificate request to submit to any certificate authority (CA).

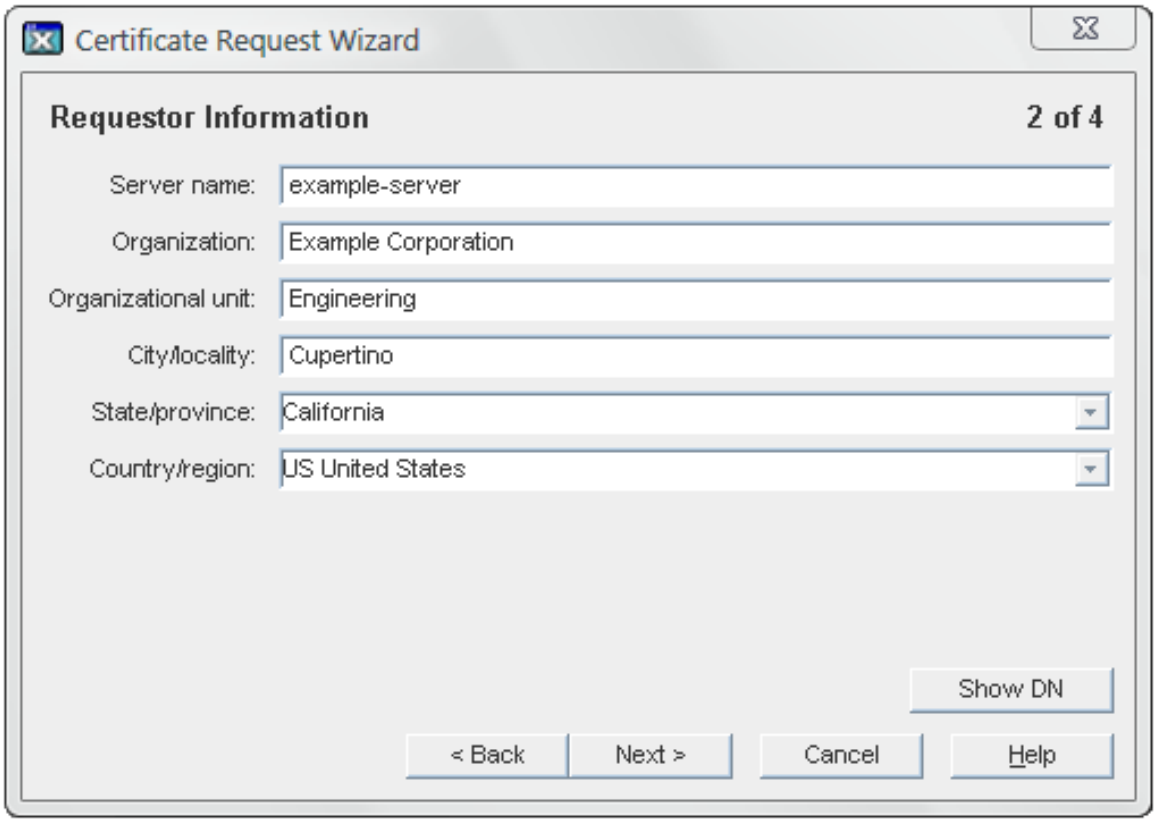
1. In the Admin Server Console, select the **Tasks** tab, and click **Manage Certificates**.



2. Create a certificate request.
   a. Select the **Server Certs** tab, and click the **Request** button.

      Click **Next**.

   b. Enter the **Requester Information** in the blank text fields, then click **Next**.



- *Server Name.*

  The fully qualified host name of the Directory Server as it is used in DNS and reverse DNS lookups; for example, `server.example.com`. The server name is critical for client-side validation to work, which prevents man-in-the-middle attacks.

IMPORTANT:

This must be a valid host name that can be resolved correctly by all Admin Server clients, or TLS/SSL will not work.

- *Organization.*

  The legal name of the company or institution. Most CAs require this information to be verified with legal documents such as a copy of a business license.

- *Organizational Unit.*

  (Optional) A descriptive name for the organization within the company.

- *Locality.*

  (Optional) The company's city name.

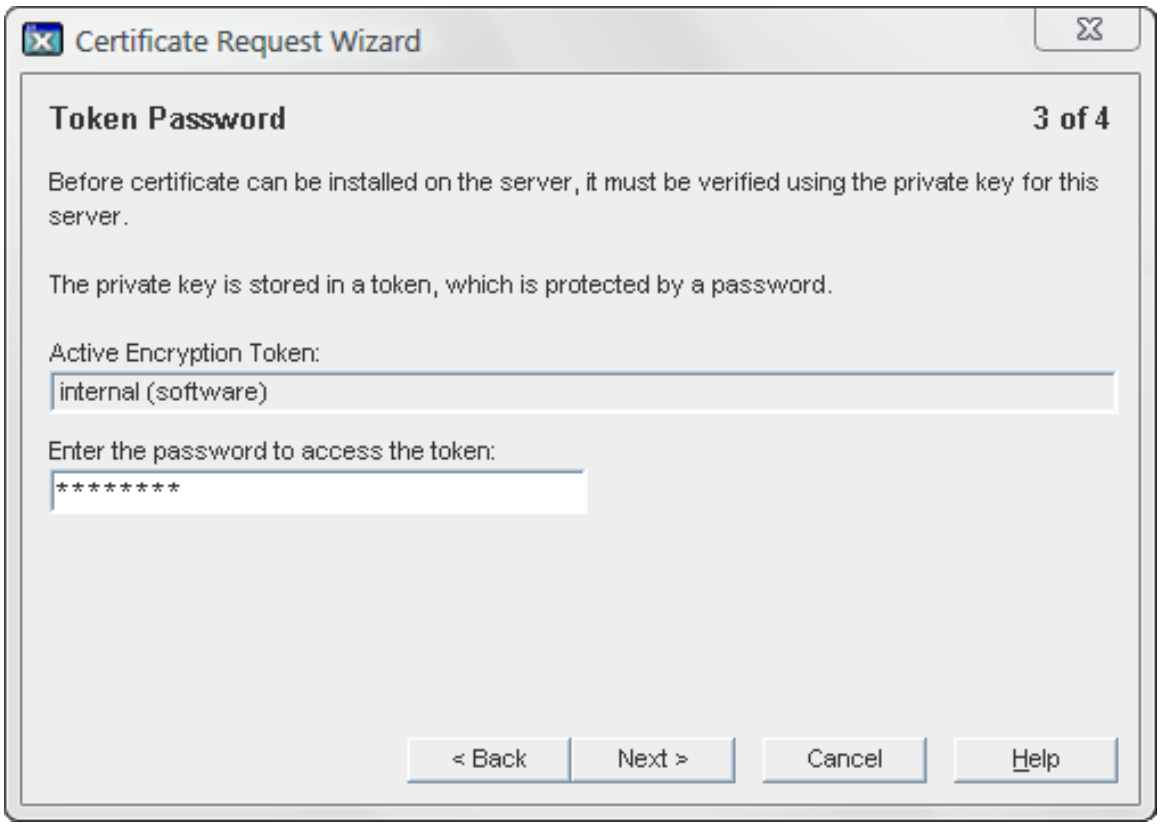
- *State or Province.*

  The full name of the company's state or province (no abbreviations).

- *Country.*

  The two-character abbreviation for the country's name (ISO format). The country code for the United States is US.

c. Enter the password that used to protect the private key, and click **Next**.



The **Next** button is grayed out until a password is supplied.

3. The **Request Submission** dialog box provides two ways to submit a request: directly to the CA (if there is one internally) or manually. To submit the request manually, select **Copy to Clipboard** or **Save to File** to save the certificate request which will be submitted to the CA.

To submit the request to a CA manually, either email it or use the web form for the CA, if one is available. Copy the certificate request information and submit it using the appropriate method.

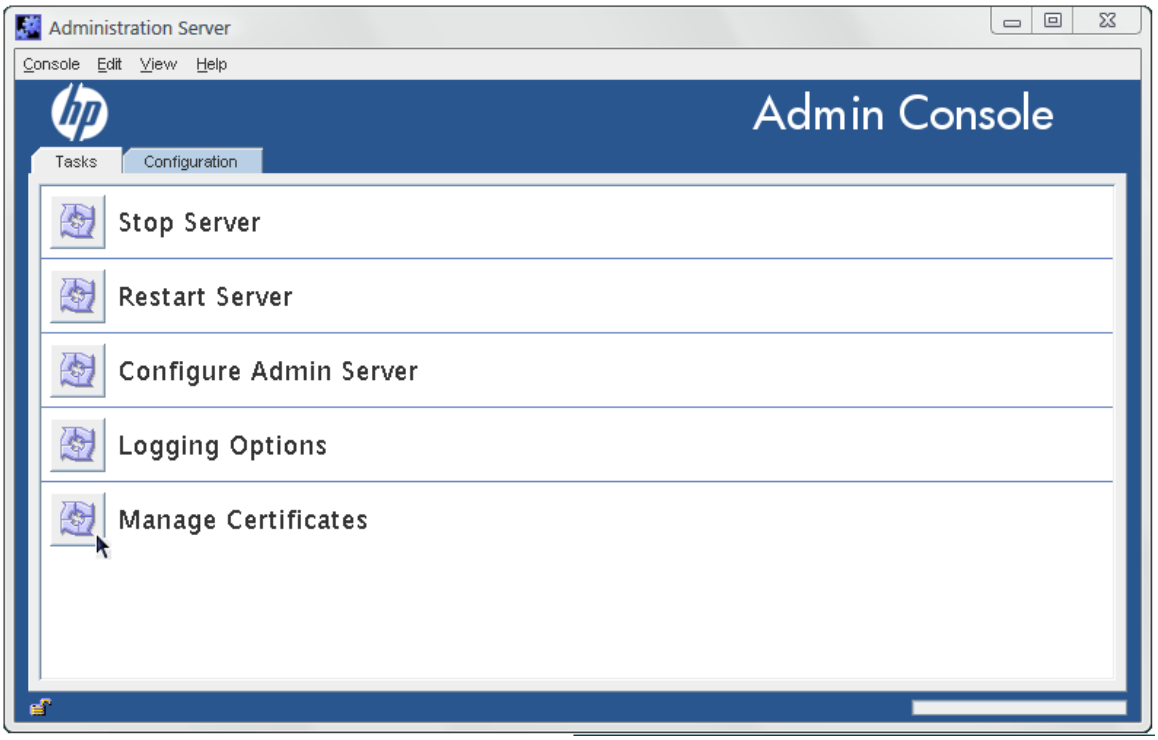
```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBrjCCARcCAQAwbjELMAkGA1UEBhMCVXMxEzARBgNVBAgTCkNBTElGT1J
OSUExLDAqBgVBAoTI25ldHNjYXBlIGNvbW11bmljYXRpb25zIGNvcnBvcmF
0aW9uMRwwGgYDVQQDExNtZWxsb24ubmV0c2NhcGUuY29tMIGfMA0GCSqGSI
b3DQEBAQUAA4GNADCBiQKBgQCwAbskGh6SKYOgHy+UCSLnm3ok3X3u83Us7
ug0EfgSLR0f+K41eNqqRftGR83emqPLDOf0ZLTLjVGJaH4Jn4l1gG+JDf/n
/zMyahxtV7+mT8GOFFigFfuxaxMjr2j7IvELlxQ4IfZgWwqCm4qQecv3G+N
9YdbjveMVXW0v4XwIDAQABoAAwDQYK
------END NEW CERTIFICATE REQUEST-----
```

4. Wait for the CA to respond with the server certificate; this can be as short as a few hours for an internal CA or as long as several weeks for a third-party CA.
5. Save the issued certificate to a file.

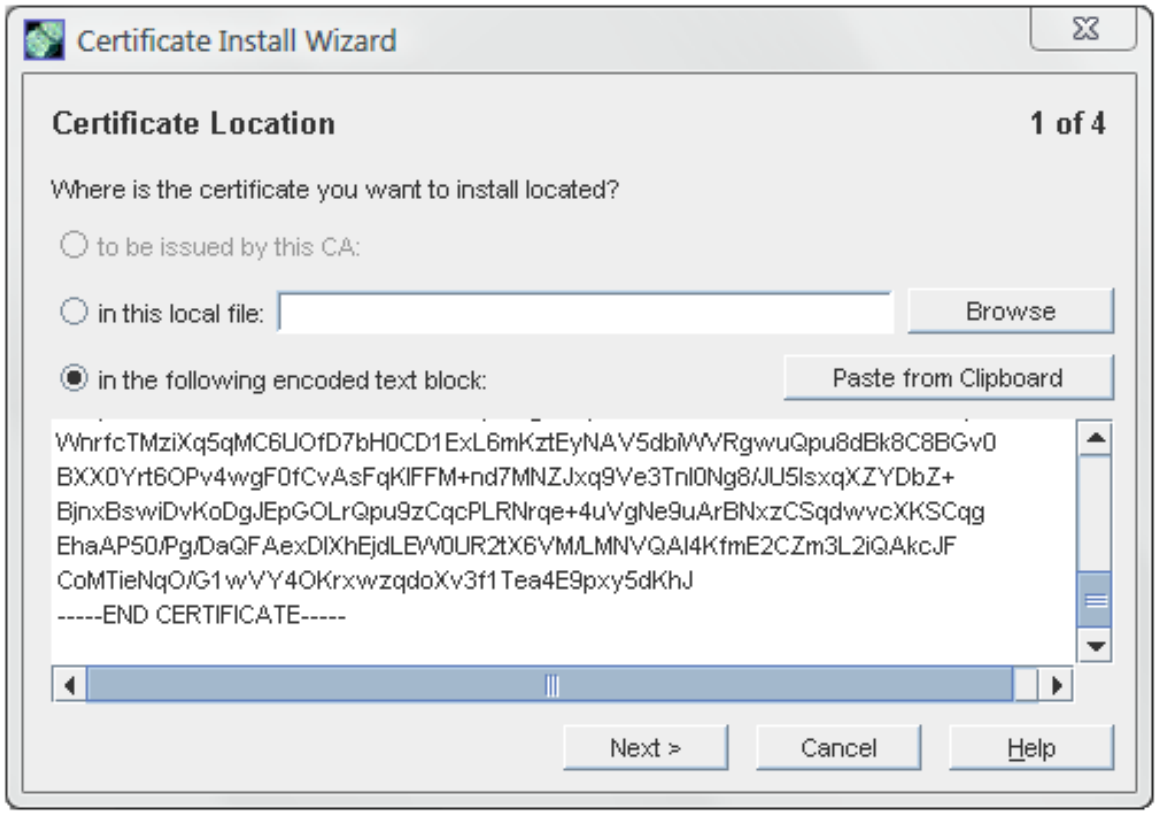
NOTE:

Keep a backup of the certificate data in a safe location. If the system ever loses the certificate data, the certificate can be reinstalled using the backup file.

6. Install the certificate.
   a. Select the **Tasks** tab, and click **Manage Certificates**.



   b. Select the **Server Certs** tab, and click **Install**.
   c. Give the absolute path to the certificate (**In this local file** radio button) or paste the certificate text in the text box (**In the following encoded text block** radio button), then click **Next**.



d. Check that the certificate information displayed is correct, and click **Next**.

e. Name the certificate, and click **Next**.

f. Provide the password that protects the private key. This password is the same as the one provided in step c.

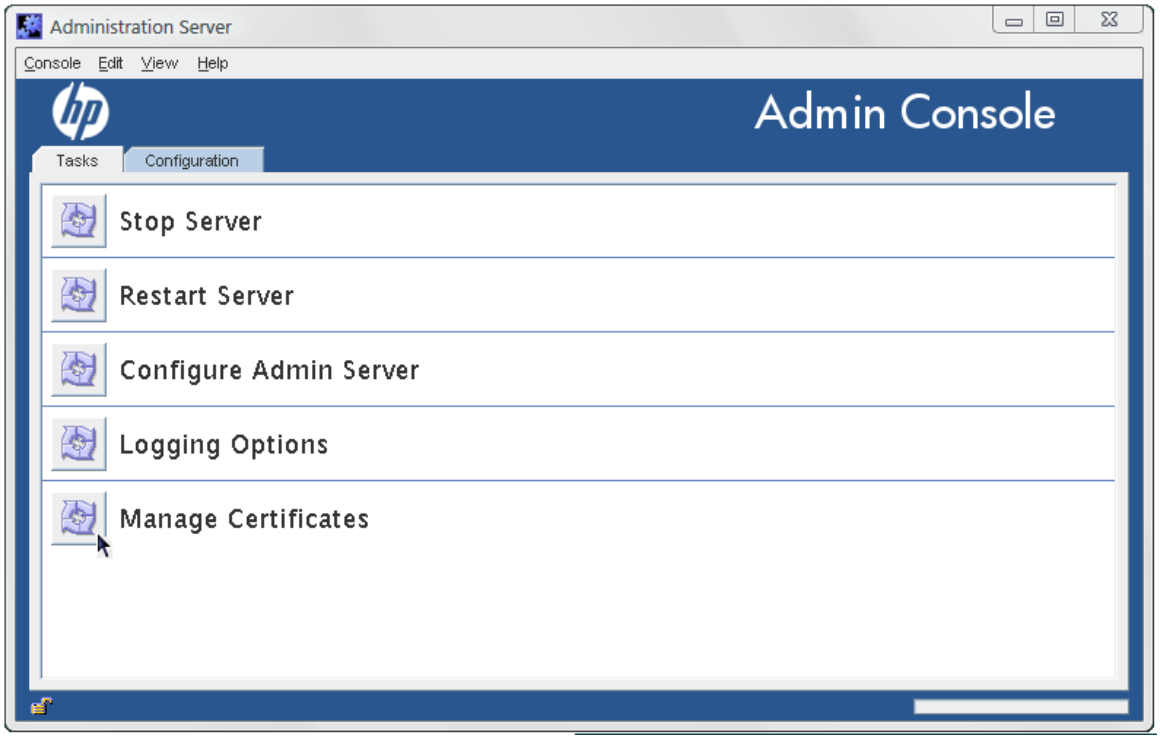
After installing the server certificate, configure the Admin Server to trust the CA which issued the server's certificate.

2.8.2 Installing a CA certificate

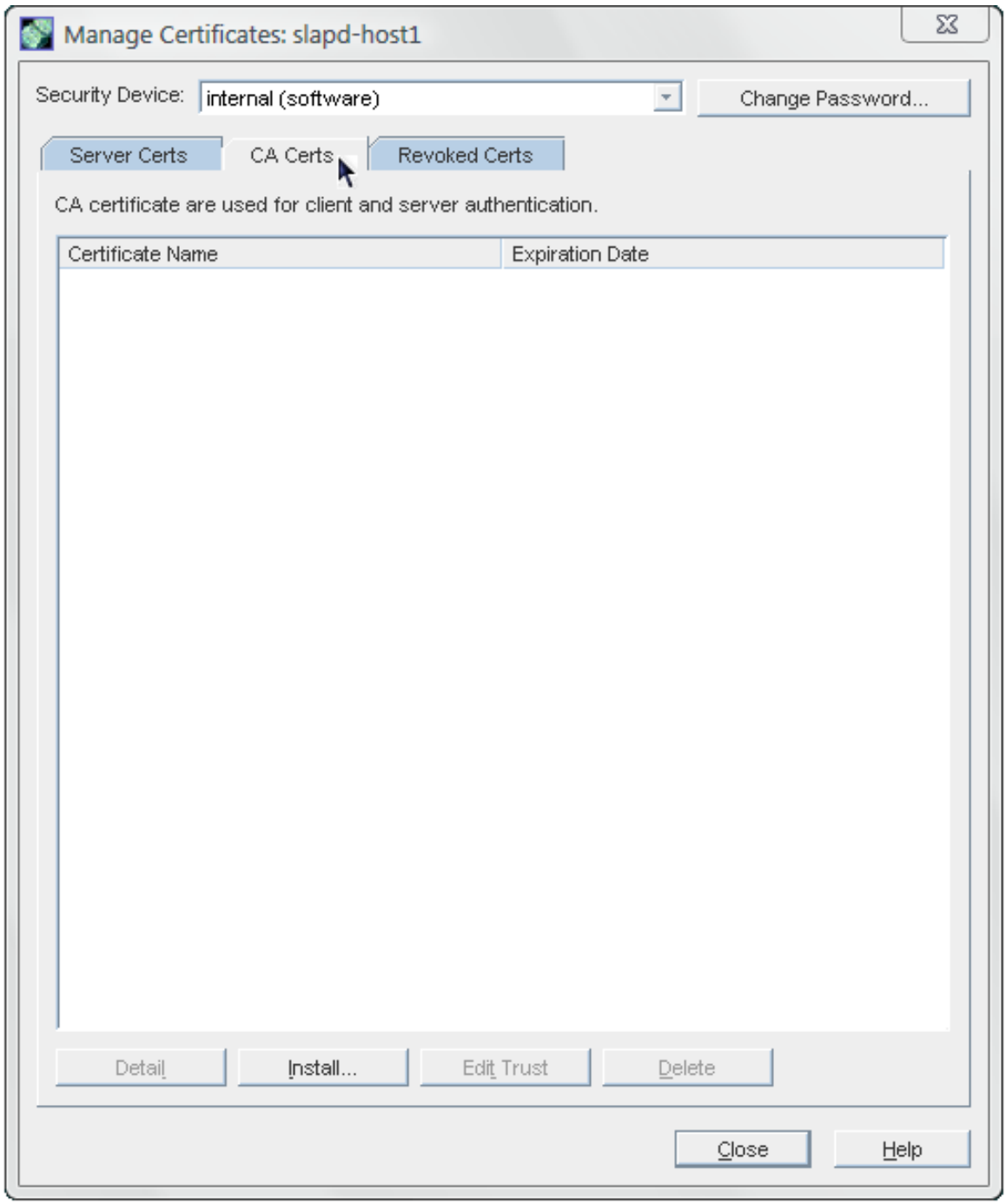
To configure the Admin Server to trust the CA, obtain the CA's certificate and install it into the server's certificate database. Some commercial CAs provide a web site that allow users to automatically download the certificate, while others will email it back to users.

After receiving the CA certificate, use the **Certificate Install Wizard** to configure the Admin Server to trust the CA.

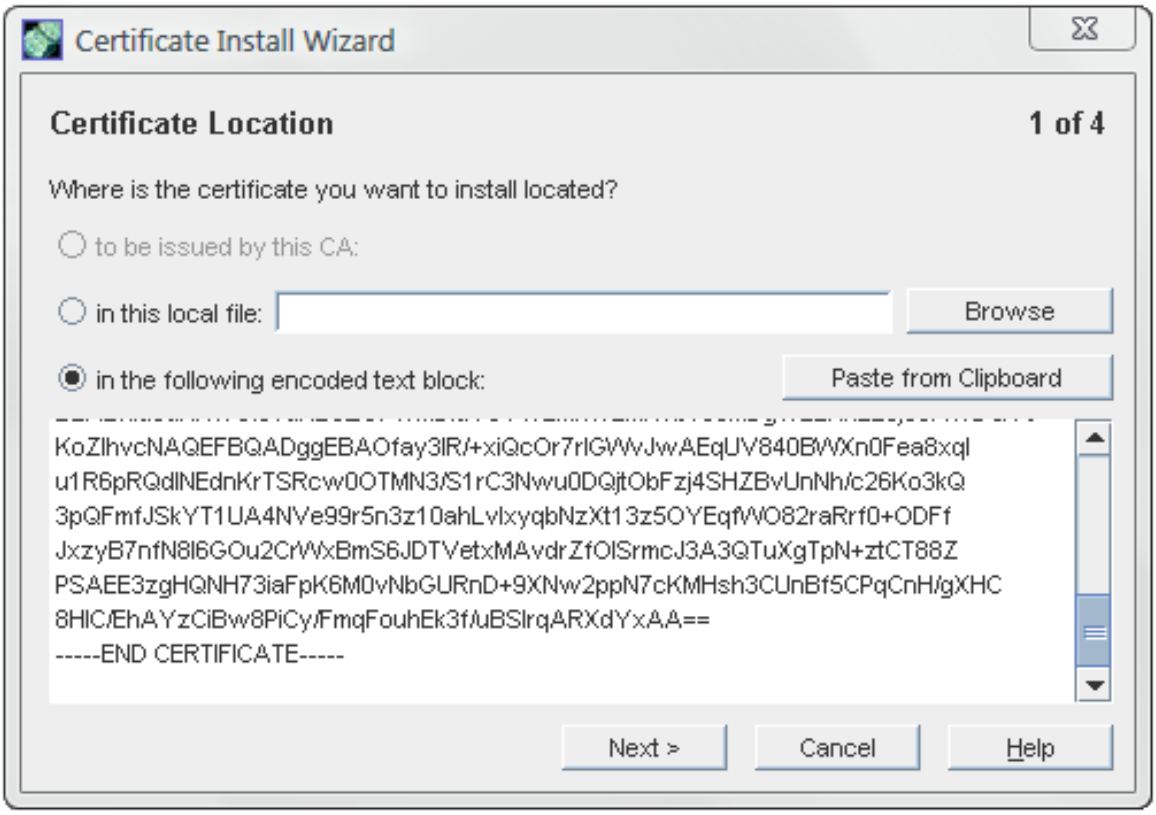
1. In the Admin Server Console, select the **Tasks** tab, and click **Manage Certificates**.



2. Go to the **CA Certs** tab, and click **Install**.



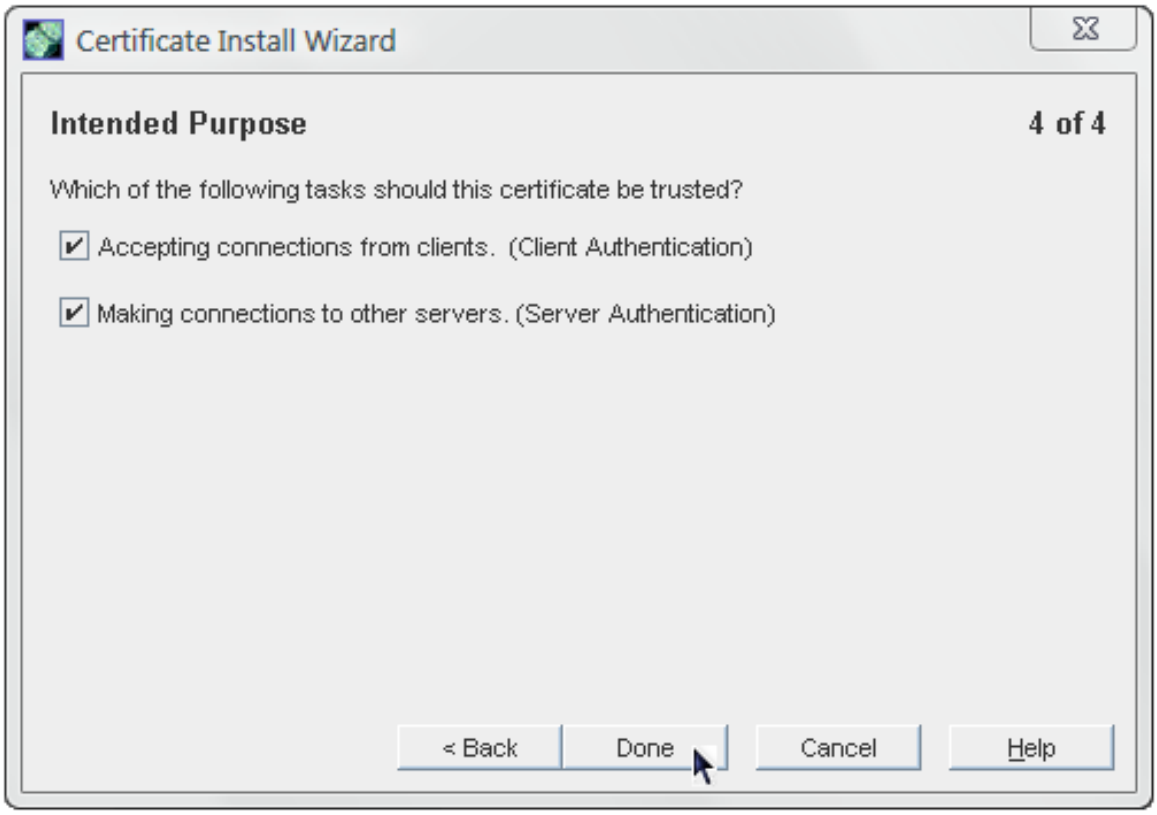
3. If the CA's certificate is saved to a file, enter the path in the field provided. Alternatively, copy and paste the certificate, including the headers, into the text box. Click **Next**.



4. Click **Next** to move through the panels that show the CA certificate information and the certificate name.
5. Select the purpose of trusting this certificate authority; it is possible to select both options:
   - **Accepting connections from clients (Client Authentication).**

     The server checks that the client's certificate has been issued by a trusted certificate authority.
   - **Accepting connections to other servers (Server Authentication).**

     This server checks that the directory to which it is making a connection (for replication updates, for example) has a certificate that has been issued by a trusted certificate authority.



6. Click **Done**.

After installing the CA certificate, it is listed in the **CA Certificates** tab in the Console.

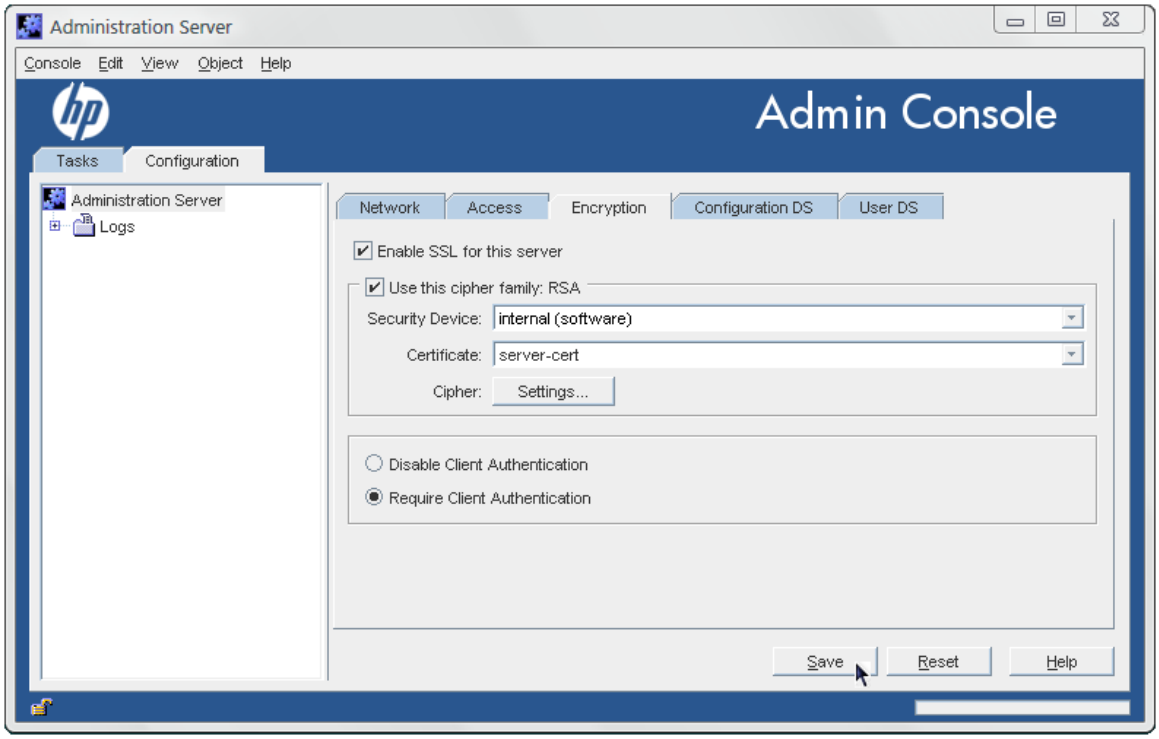
NOTE:

If a CA certificate is incorrectly generated, it is listed in the **Server Certificates** tab in the Console rather than the **CA Certificates** tab. The certificate still works as a CA certificate, even though it is listed in the wrong tab.

Still, request certificates from a real certificate authority to minimize the risk of using an incorrectly generated certificate and breaking SSL/TLS in the Admin Server.

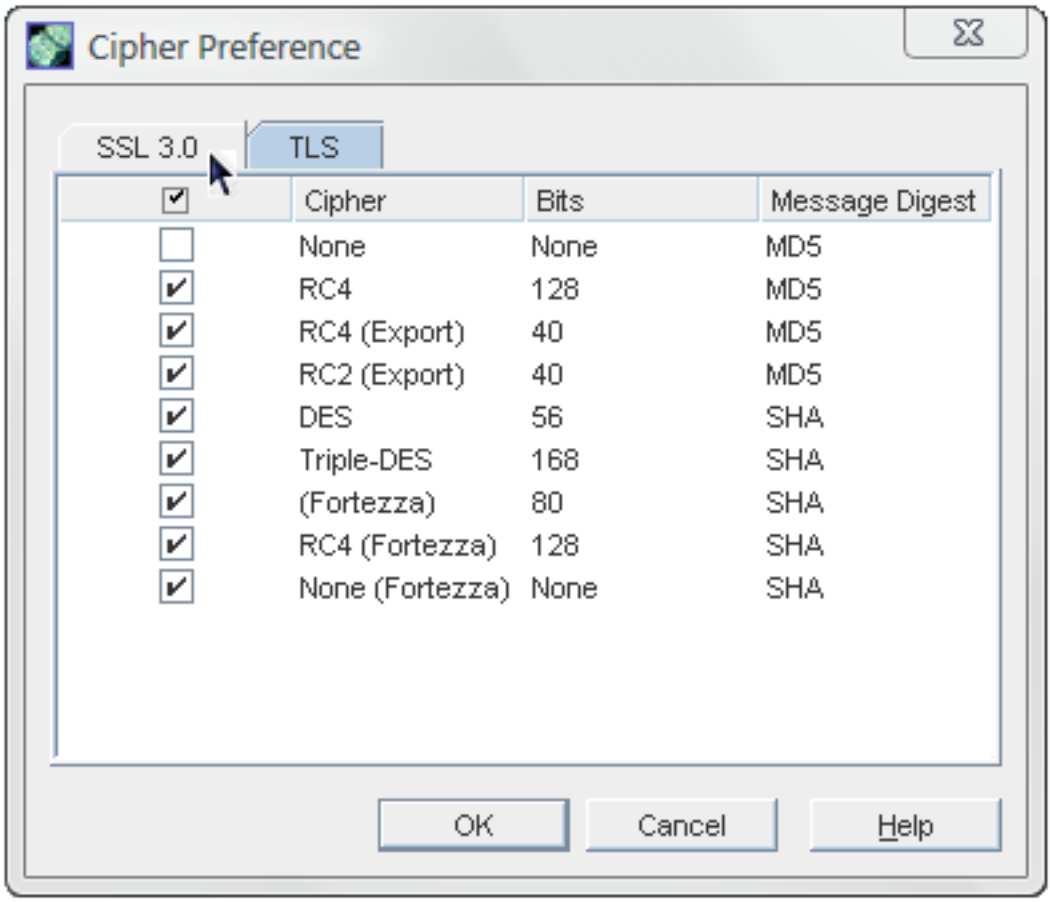
2.8.3 Enabling SSL

1. Open the Admin Server management window.
2. Click the **Configuration** tab.
3. Click the **Encryption** tab.



4. Select the **Enable SSL for this server** checkbox.
5. Select the **Use this cipher family: RSA** checkbox.
6. Choose the security device where the key is stored. By default, the key is stored in the local key database, **Internal (Software-based)**. If the key is stored on an external device (such as a smart card), select that device from the menu.
7. Choose the server certificate to use with SSL.

   The certificates available in the token certificate database are listed in the drop-down menu.
8. Click the **Settings** button to set the ciphers that the Admin Server accepts for SSL/TLS connections.



9. Set whether to require client **authentication** to the Admin Server. Client authentication means that the server checks that the client's certificate has been issued by a trusted CA.
10. Click **Save**.

2.8.4 Creating a password file for the Admin Server

Normally, if SSL is enabled, the server prompts for a security password when the Admin Server is restarted:

```
Starting dirsrv-admin
Please enter password for "internal" token:
```

The Admin Server can use a password file when TLS/SSL is enabled so that the server restarts silently, without prompting for the security password.

WARNING!

This password is stored in clear text within the password file, so its use represents a significant security risk. Do not use a password file if the server is running in an unsecured environment.

1. Open the Admin Server configuration directory.

   ```
   cd /etc/opt/dirsrv/admin-serv
   ```

2. Create a password file named `password.conf`. The file should include a line with the token name and password, in the form *`token:password`*. For example:

   ```
   internal:secret
   ```

   For the NSS software crypto module (the default software database), the token is always called `internal`.

   The password file should be owned by the Admin Server user and set to read-only by the Admin Server user, with no access to any other user (mode `0400`).

NOTE:

To find out what the Admin Server user ID is, run `grep` in the Admin Server configuration directory:

```
cd /etc/opt/dirsrv/admin-serv
grep \^User console.conf
```

3. In the `/etc/opt/dirsrv/admin-serv` directory, edit the `nss.conf` file to point to the location of the new password file.

```
#   Pass Phrase Dialog:
#   Configure the pass phrase gathering process.
#   The filtering dialog program (`builtin' is a internal
#   terminal dialog) has to provide the pass phrase on stdout.
NSSPassPhraseDialog  file:/etc/opt/dirsrv/admin-serv/password.conf
```

4. Restart the Admin Server. For example:

```
/opt/dirsrv/sbin/restart-ds-admin
```

After TLS/SSL is enabled, then the Admin Server can only be connected to using HTTPS. All the previous HTTP (standard) URLs for connecting to the Admin Server and its services no longer work. This is true whether connecting to the Admin Server using the Console or using a web browser.

2.9 Changing Directory Server settings

The Admin Server stored information about the Directory Server *`Configuration Directory`* (which stores the instance configuration information) and the Directory Server *`User Directory`* (which stores the actual directory entries). These can be the same directory instance, but they do not have to be. The settings for both of those databases can be edited in the Admin Server configuration so that it communicates with a different Directory Server instance.

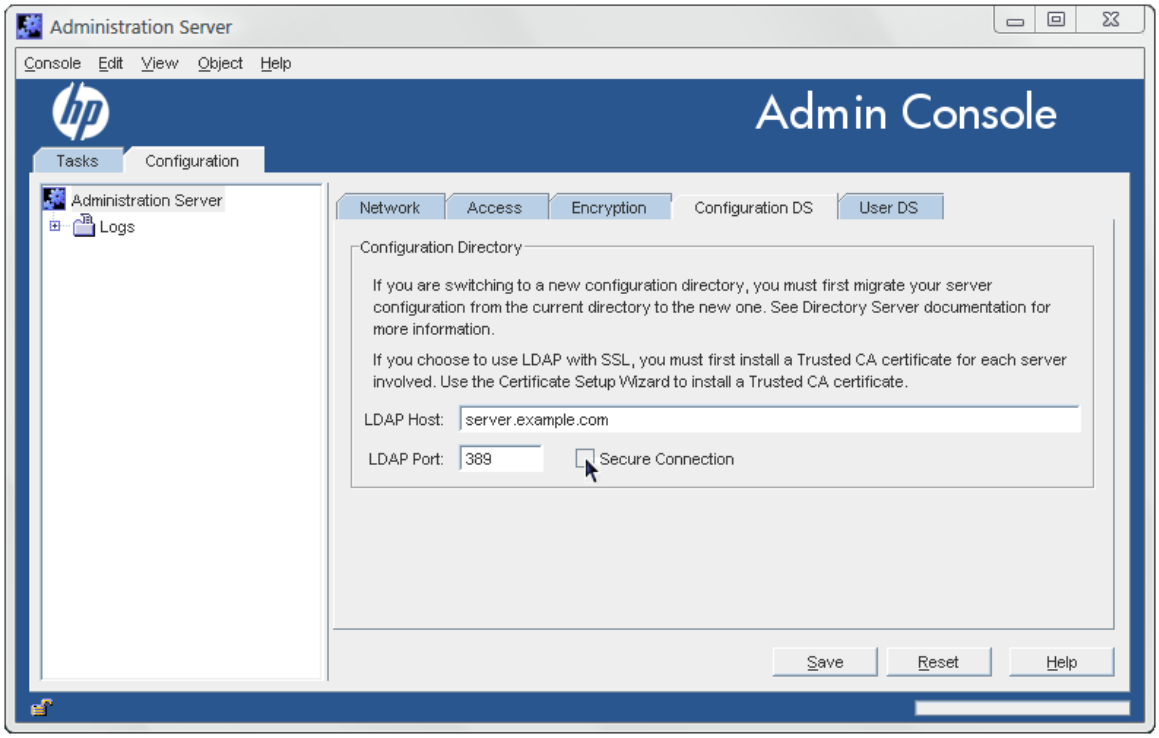
2.9.1 Changing the configuration directory host or port

Configuration data are stored under `o=NetscapeRoot` in the Configuration Directory. The configuration database contains server settings such as network topology information and server instance entries. When server configuration changes are stored in the configuration directory subtree.

WARNING!

Changing the Directory Server host name or port number impacts the rest of the servers in the server group. Changing a setting here means the same change must be made for every server in the server group.

1. Open the Admin Server management window.
2. Click the **Configuration** tab.
3. Click the **Configuration DS** tab.
4. Set the Configuration Directory Server connection information.



- The **LDAP Host** is the host name of the Configuration Directory Server machine.
- The **LDAP Port** is the port number to use for the Directory Server instance. The regular LDAP port is `389`; the default LDAPS (secure) port number is `636`.
- Check the **Secure Connection** checkbox to use the secure port. Before checking this box, make sure that the Configuration Directory Server has enabled SSL.

5. Click **Save**.

2.9.2 Changing the user directory host or port

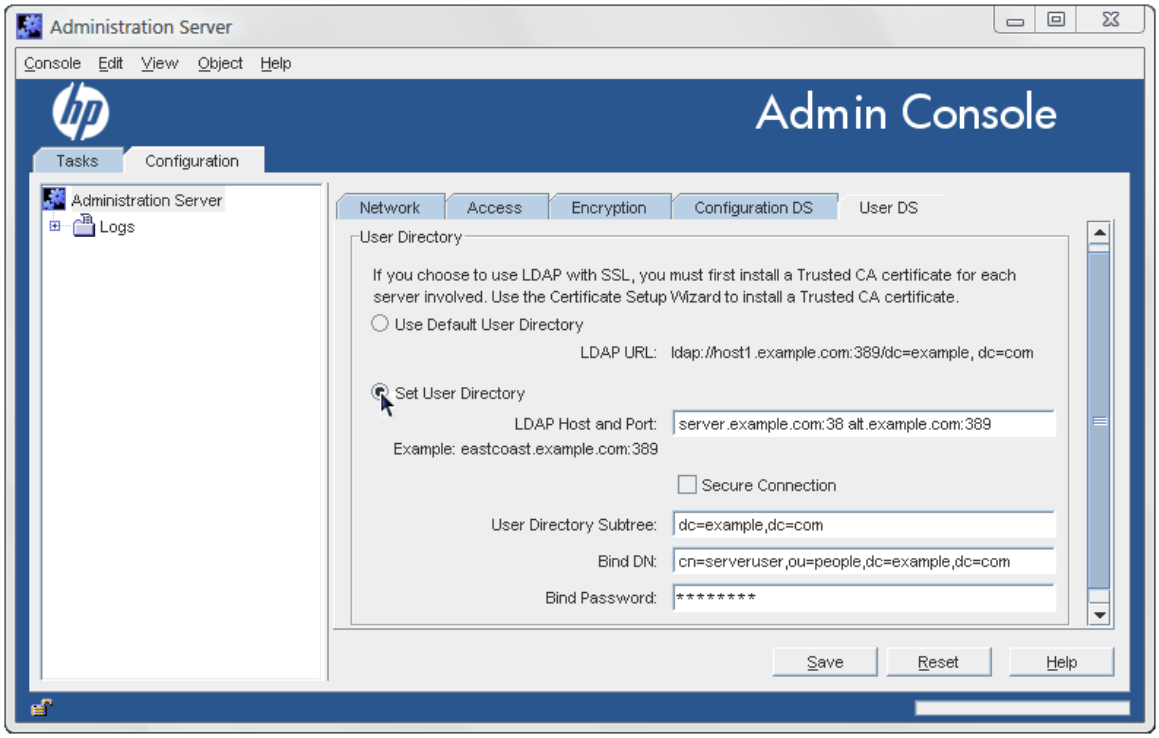
The user directory is used for authentication, user management, and access control. It stores all user and group data, account data, group lists, and access control instructions (**ACI**s).

There can be multiple user directories in a single deployment because using multiple user directories enhances overall performance for organizations which are geographically spread out, which have high usage, or have discrete divisions which benefit from individual directories.

Admin Server can be configured to authenticate users against multiple user directories.

To change the information for the user directory:

1. Open the Admin Server management window.
2. Click the **Configuration** tab.
3. Click the **User DS** tab.
4. Set the User Directory Server connection information.
5. Edit the user directory information.



The **Use Default User Directory** radio button uses the default user directory associated with the domain. To use multiple Directory Server instances or to use a different instance, select the **Set User Directory** radio button and set the required information:

- The **LDAP Host and Port** field specifies the location of the user directory instance.

  It is possible to configure multiple locations for the user directory for authentication and other directory functions; separate each location with a space. For example:

  ```
  server.example.com:389 alt.example.com:389
  ```

NOTE:

If more than one location is given in the **LDAP Host and Port** field, the settings for the remaining fields will apply to all those instances.

- Check the **Secure Connection** box to use SSL to connect to the user directory. Only select this if the Directory Server is already configured to use SSL.
- Give the **User Directory Subtree**. For example:

  ```
  dc=example,dc=com
  ```

  Every location listed in the **LDAP Host and Port** field must contain that subtree and the subtree must contain the user information.

- Optionally, enter the **Bind DN** and **Bind Password** for the user which connects to the user directory.

6. Click **Save**.

3 Admin express

3.1 Managing servers in Admin Express

Admin Express provides a quick, simple web-based gateway to do basic management of servers. There are three tasks that can be performed through Admin Express:

- Stopping and starting the server
- Checking the server access, error, and audit logs
- Monitoring the progress and information for replication betweehn Directory Servers

3.1.1 Opening Admin Express

The Admin Server services pages URL is the Admin Server host and port. For example:

```
http://ldap.example.com:9830/
```

The Admin Express page is always available at that URL.

NOTE:

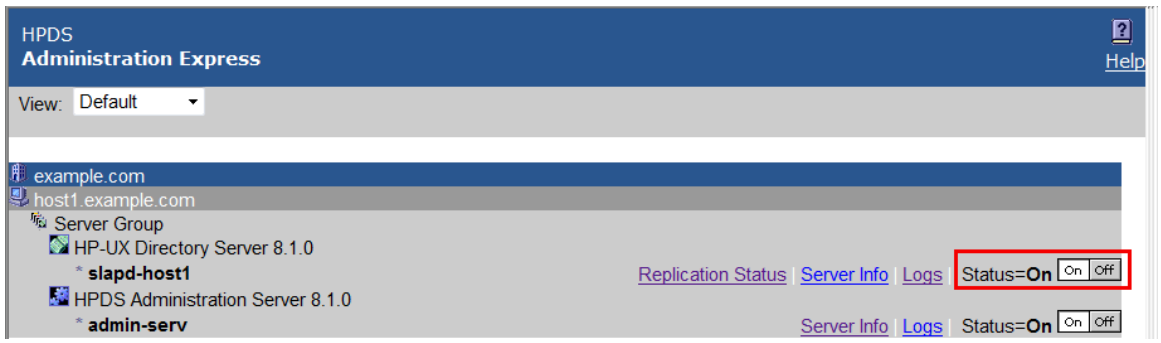
If SSL/TLS is enabled on the Admin Server, then the URL must use the prefix `https:` with the same port number. The standard HTTP URLs will not work.

```
https://ldap.example.com:9830/
```

3.1.2 Starting and stopping servers

On the main Admin Express page, there are buttons to turn servers off and on.

Figure 3-1 Stopping and stopping servers



IMPORTANT:

If either the Admin Server or the Configuration Directory Server is turned off through the Admin Express page, then it must be restarted through the command line, not through the Admin Express **On/Off** buttons because Admin Express requires access to both the Admin Server and Configuration Directory Server in order to function.

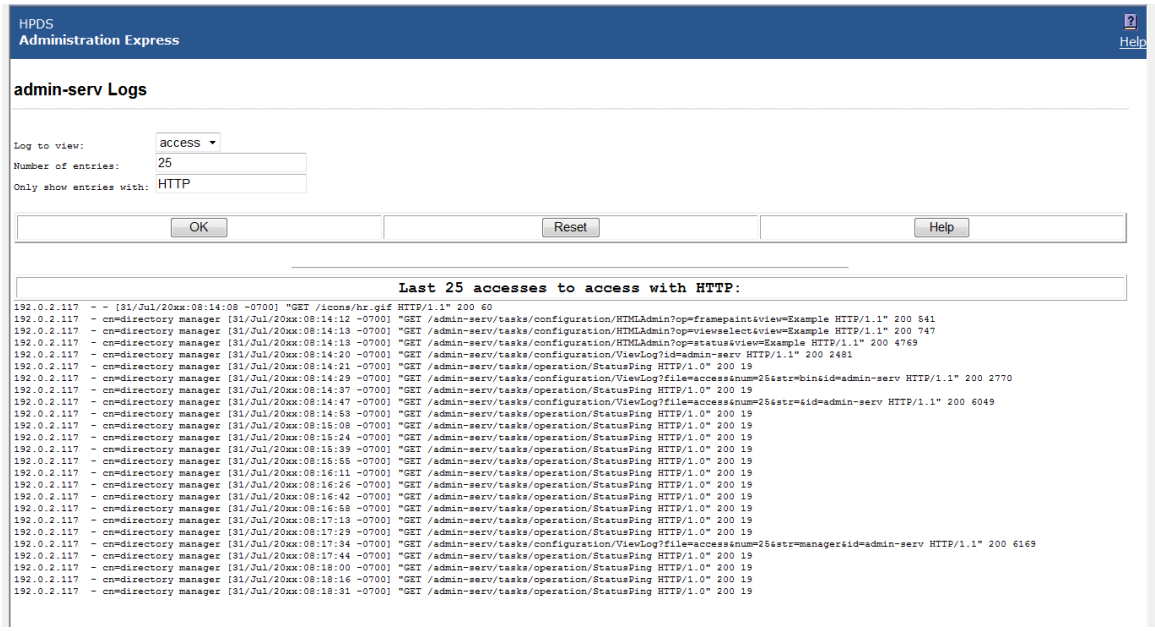
Other Directory Server instances can be safely stopped and restarted through Admin Express.

3.1.3 Viewing server logs

Admin Express can show and search the access and error logs for Directory Server and Admin Server and the audit logs for the Directory Server.

1. In the Admin Express page, click the **Logs** link by the server name.
2. Select which log type to view, how many lines to return, and any string to search for, and click **OK**.

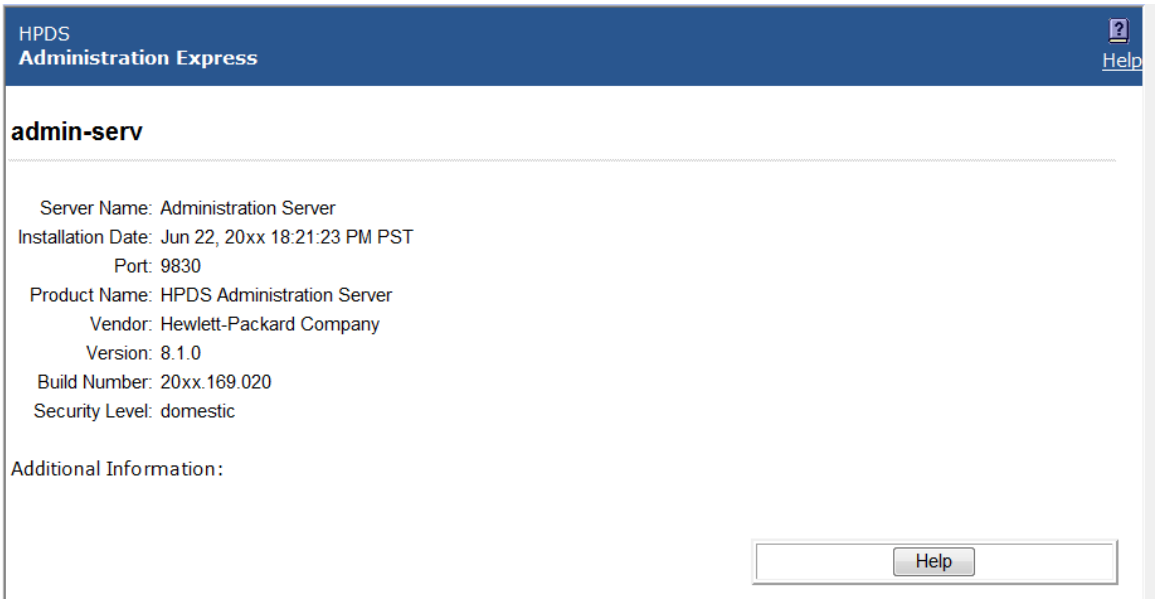
Figure 3-2 Checking logs



3.1.4 Viewing server information

The **Server Info** link on the Admin Express page opens a page with the basic description of the server instance, such as the build number, installation date, and server port number. This is the same information displayed in the Console when an instance is selected.

Figure 3-3 Checking server information



The Directory Server information is located in the `/etc/opt/dirsrv/slapd-`*`instance_name`*`/dse.ldif` file; the Admin Server information is located in `.conf` files in the `/etc/opt/dirsrv/admin-serv` directory.

3.1.5 Monitoring replication from Admin Express

Admin Express has an option to monitor replication status in real-time, meaning that it shows the number of updates, times the most recent updates were sent, error and success messages, replication schedule, the replicated directory suffix, and other information. Unlike other ways of checking replication status, the Admin Express **Replication Status** page shows the real-time

status of replication, including updates in progress, current changes sequence numbers, and the lag between when a change is made on the **supplier** and when that change is sent to the **consumer**.

Monitoring replication is set up using a simple configuration file which specifies which server to monitor and what supplier and consumer replicas to include in the status page.

When trying to monitor replication status through Admin Express, remember two things:

- The **Replication Status** page is only available for supplier servers. (It can be opened for other types of replicas; there's just no information available and has the message `The server is not a master or it has no replication agreement.`)
- The configuration file must be in a directory that is accessible to Admin Server, and the file must be readable by the Admin Server user. By default, the user is `nobody`.

  The user is set in the `console.conf` file. To check the user, use the `grep` command to return the value:

  ```
  grep \^User /etc/opt/dirsrv/admin-serv/console.conf
  ```

  The configuration file should be readable by the Admin Server user and no other users, so consider resetting the permissions on the file:

  ```
  chmod 0400 filename
  ```

To view in-progress status of replication in Admin Express:

1. Create a configuration file. The configuration file lists all the servers to monitor for replication, giving their host name, port, the bind credentials to use, and optional settings for aliases and time lag colors.

   ```
   #Configuration File for Monitoring Replication Via Admin Express
   [connection] Required. Gives the server host, port, supplier bind DN, and password.
   host1.example.com:389:cn=replication manager:mypassword
   host2.example.com:3891:cn=replication manager:altpassword
   [alias] Optional. Gives a friendly-name alias to the servers and consumers.
   M1 = host1.example.com:389
   M2 = host2.example.com:3891
   C1 = host3.example.com:3892
   C2 = host4.example.com:3890

   [color] Optional. Sets the color for the time lag boxes.
   0 = #ccffcc
   5 = #FFFFCC
   60 = #FFCCCC
   ```

   The configuration file must be in a directory that is accessible to the Admin Server, and the file must be readable by the Admin Server user. By default, the user is `nobody`.

   The user is set in the `console.conf` file. To check the user, use the `grep` command to return the value:

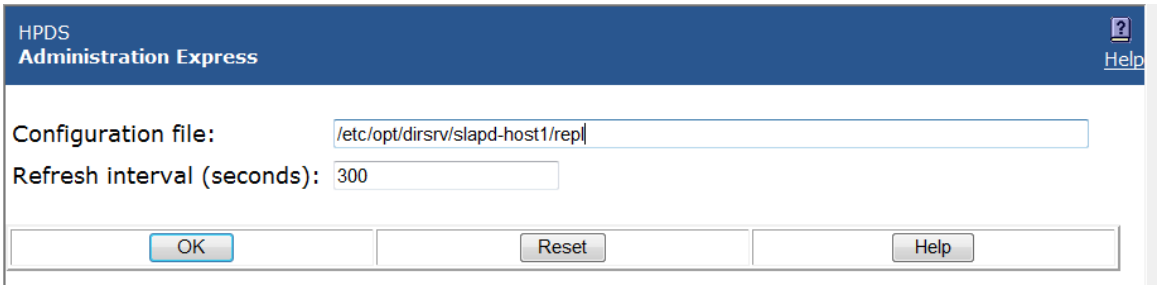
   ```
   grep \^User /etc/opt/dirsrv/admin-serv/console.conf
   ```

   The configuration file should be readable by the Admin Server user and no other users, so consider resetting the permissions on the file:

   ```
   chmod 0400 filename
   ```

2. In the Admin Server web page, click the **Admin Express** link, and log in.
3. Click the **Replication Status** link by the supplier server name.
4. Type the path to the configuration file in the **Configuration file** field. Also, set the refresh rate, which is how frequently the replication status page updates; the default is 300 seconds.

Figure 3-4 Viewing replication status



5. Click **OK**.

The **Replication Status** page shows the status for sending updates to every consumer listed in the configuration file.

Figure 3-5 Viewing replication status

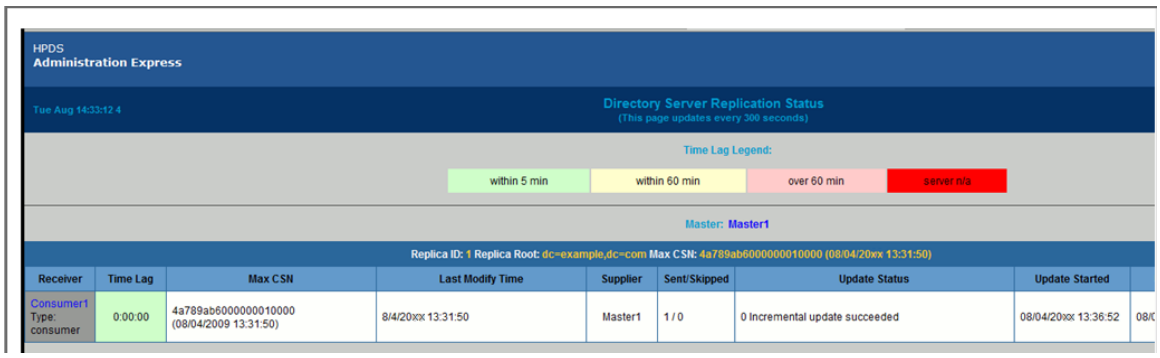


Table	Description
Table header	The table header shows the replica ID of the supplier **replica**, the replicated suffix root (such as `dc=example,dc=com`), and the maximum change state number (CSN) on the supplier. (The CSN is the ID of the latest change on the supplier, while the max CSN for the supplier shows the last update it received.)
Max CSN	The ID number of the most recent CSN the consumer has received that originated from the supplier.
Time lag	How long it takes for the consumer to receive updates from the supplier; this is the time difference between the supplier and the consumer's max CSNs. When a consumer is in sync with its supplier, the time lag is `0`.
Last Modify Time	Gives the time of the last update for the consumer (the time the last CSN entry was sent).
Supplier	Gives the name of the supplier sending updates to that consumer; this can be useful if a consumer receives updates from multiple suppliers or there are multiple suppliers being monitored on the **Replication Status** page.
Sent/Skipped	The number of changes that were sent from the supplier and the number skipped in the replication update. The numbers are kept in suppliers' memory only and are cleared if the supplier is restarted.
Update Status	The status code (and meaning) for the last update. This column can indicate a possible deadlock if all the suppliers complain that they cannot acquire a busy replica. It is normal for there to be a busy message if one of the suppliers is doing an update.
Update Start and End	The timestamps for when the most recent update process started and ended.
Schedule	The configured replication schedule. `0::` means that the consumer is continually updated by the supplier.
SSL?	Indicates whether the supplier connects to the consumer over SSL.

3.2 Configuring Admin Express

Admin Express can be edited for the page appearance, but most functionality is controlled through the web server or the Admin Server configuration and should be edited through those servers, not by editing the configuration files directly.

3.2.1 Admin Express file locations

The directories for all the Admin Express configuration files are listed in Table 3-1 "Admin Express file directories"; the specific files are described in each section describing the different Admin Express page configurations.

Table 3-1 Admin Express file directories

File or directory	Description
`/etc/opt/dirsrv/admin-serv`	Contains the `local.conf`, `httpd.conf`, and other configuration files which define the Admin Server and configure the web server.
`/opt/dirsrv/share/html`	Contains the HTML files and graphics used for the Admin Express appearance.

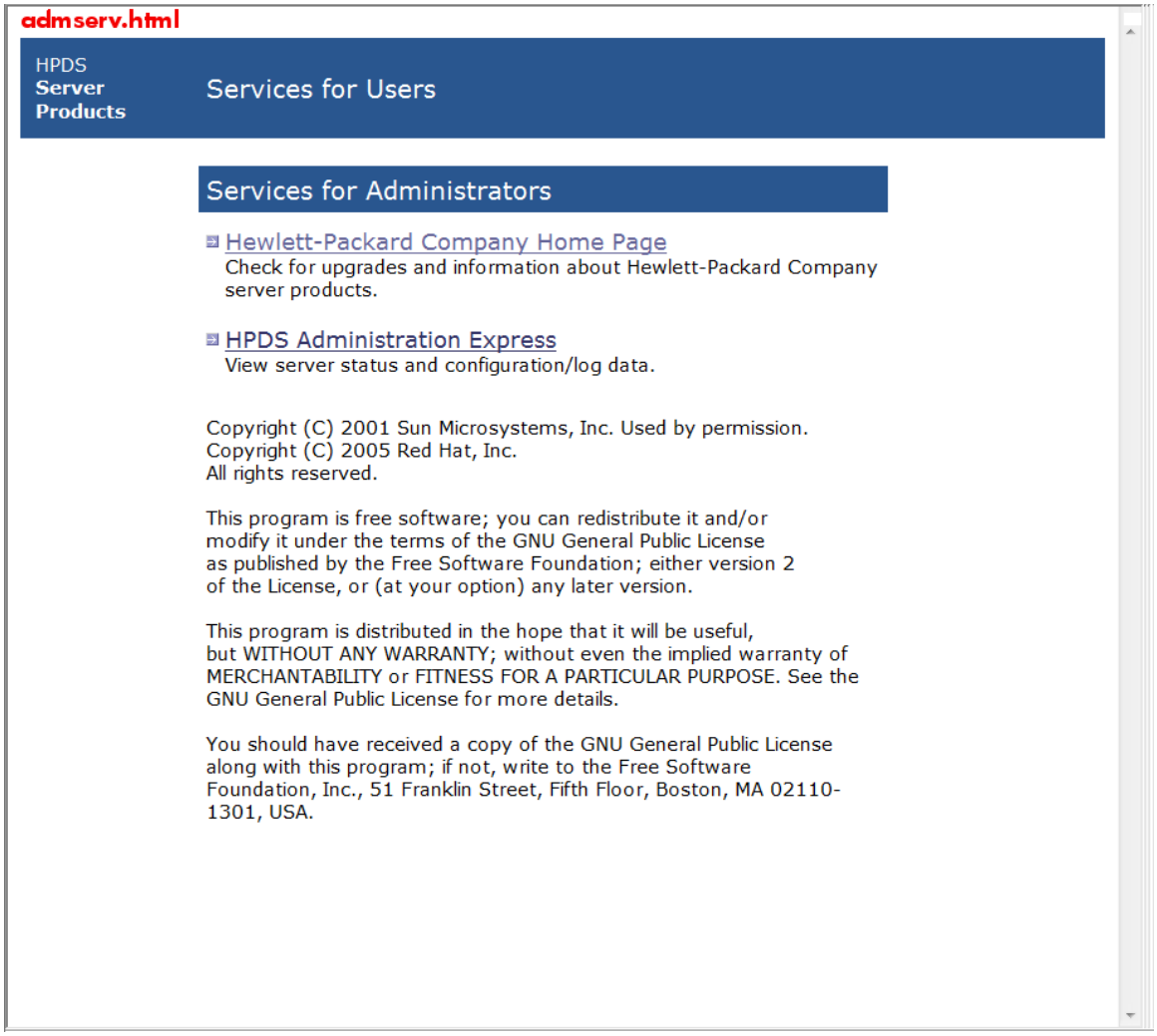
3.2.2 Admin Express configuration files

The behavior for Admin Express is mostly set through the web server configuration and should not be edited. The other Admin Express configuration is set through directives which insert data or form fields.

3.2.2.1 Files for the Admin Server welcome page

The configuration files for the introductory page for the web applications are located in the Admin Express directory, `/opt/dirsrv/share/html`. The main file is `admserv.html`.

Figure 3-6 Intro page elements



All the formatting for the page is set inline. The text files are inserted using the `INCLUDEIFEXISTS` directive.

```
  <tr valign="TOP">
    <td> </td>
    <td bgcolor="#9999cc" colspan="4"> <font color="white"
size="+1"><font face="Verdana, sans-serif">Services
      for Administrators</font></font></td>
    <td> </td>
  </tr>
  <tr valign="TOP">
    <td> </td>
    <td colspan="4">
      <table border="0" cellspacing="0" cellpadding="0">
        <tr valign="TOP">
          <td><img src="/icons/spacer.gif" width="6" height="6"></td>
          <td></td>
        </tr>
<!-- INCLUDEIFEXISTS admserv_dsgw.html -->
```

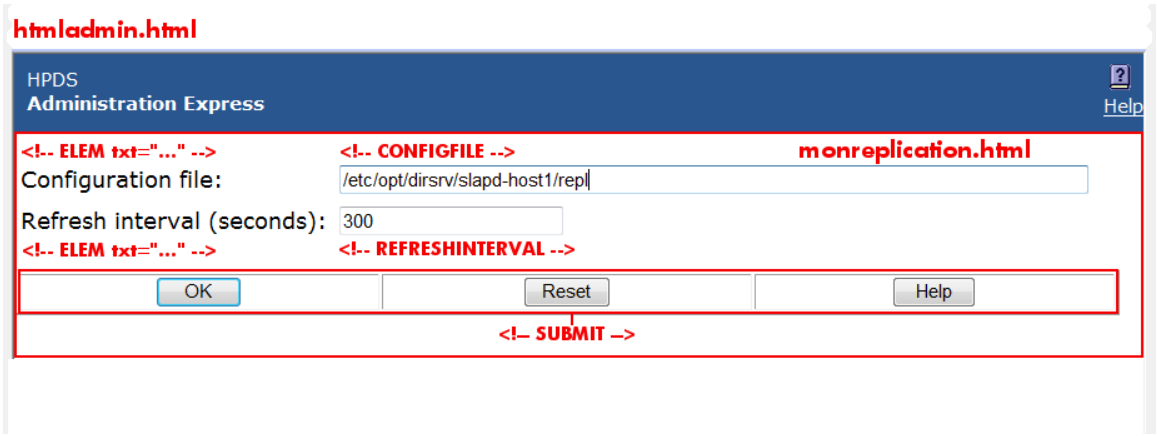
The text files themselves have inline formatting for the inserted table rows.

3.2.2.2 Files for the replication status appearance

There are two pages for monitoring the replication status. The first is for the configuration page, which requires two files:

- The body of the page, `/opt/dirsrv/share/html/monreplication.html`
- The heading of the page, `/opt/dirsrv/share/html/htmladmin.html`

Figure 3-7 Monitoring replication setup page elements



The **Replication Status** page uses two script-related configuration files:

- The body of the page, which is configured in the replication monitoring script, `/opt/dirsrv/bin/repl-monitor.pl`
- Optionally, the configuration file for the replication monitoring, which can configure the time lag colors with the `[colors]` section
- The heading of the page, `/opt/dirsrv/share/html/htmladmin.html`

Figure 3-8 Monitoring replication view page elements

The text for the table headings, labels, and page sections are set in the Perl script. For example:

```
#Print the header of consumer
   print "\n<tr class=bgColor16>\n";
   print "<th nowrap>Receiver</th>\n";
   print "<th nowrap>Time Lag</th>\n";
   print "<th nowrap>Max CSN</th>\n";
....
   print "</tr>\n";
```

The styles for the **Replication Status** page are printed in the Perl script in the `<style>` tag in the HTML header. Many of the classes are the same as those in the `style.css` for the other

web applications. These can be edited in the Perl script or by uncommenting the stylesheet reference and supplying a CSS file. For example:

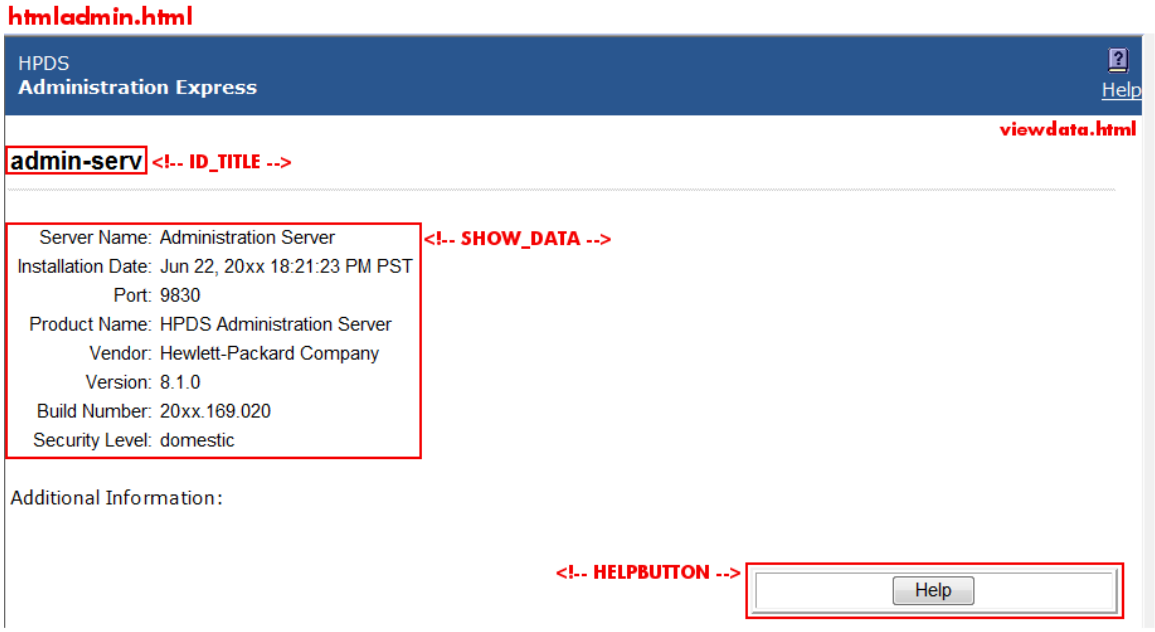
```
# print the HTML header

  print "Content-type: text/html\n\n";
  print "<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 3.2//EN\"><html>\n";
  print "<head><title>Replication Status</title>\n";
  # print "<link type=text/css rel=stylesheet href=\"master-style.css\">\n";
  print "<style text/css>\n";
  print "Body, p, table, td, ul, li {color: #000000; font-family: Arial,
Helvetica, sans-serif; font-size: 12px;}\n";
  print "A {color:blue; text-decoration: none;}\n";
  print "BODY {font-family: arial, helvetica, sans-serif}\n";
  print "P {font-family: arial, helvetica, sans-serif}\n";
  print "TH {font-weight: bold; font-family: arial, helvetica, sans-serif}\n";
  print "TD {font-family: arial, helvetica, sans-serif}\n";
  print ".bgColor1  {background-color: #003366;}\n";
  print ".bgColor4  {background-color: #cccccc;}\n";
  print ".bgColor5  {background-color: #999999;}\n";
  print ".bgColor9  {background-color: #336699;}\n";
  print ".bgColor13 {background-color: #ffffff;}\n";
  print ".bgColor16 {background-color: #6699cc;}\n";
  print ".text8  {color: #0099cc; font-size: 11px; font-weight:
bold;}\n";
  print ".text28 {color: #ffcc33; font-size: 12px; font-weight:
bold;}\n";
  print ".areatitle {font-weight: bold; color: #ffffff; font-family:
arial, helvetica, sans-serif}\n";
  print ".page-title {font-weight: bold; font-size: larger; font-family:
arial, helvetica, sans-serif}\n";
  print ".page-subtitle {font-weight: bold; font-family: arial, hel\
vetica, sans-serif}\n";
  print "</style></head>\n<body class=bgColor4>\n";
```

3.2.2.3 Files for the server information page

There are two files formatting the server information page:

- The body of the page, `/opt/dirsrv/share/html/viewdata.html`
- The heading of the page, `/opt/dirsrv/share/html/htmladmin.html`

Figure 3-9 Server information page elements



The `viewdata.html` file is very simple, using only the two directives to insert the server data, plsut other directives to insert other information. For the Admin Server, the `SHOW_DATA` directive takes the information from the `/etc/opt/dirsrv/admin-serv/local.conf` file. For the Directory Server, it takes the data from the `/etc/opt/dirsrv/slapd-`*`instance_name`*`/dse.ldif` file. The `ID_TITLE` is the name of the server instance.

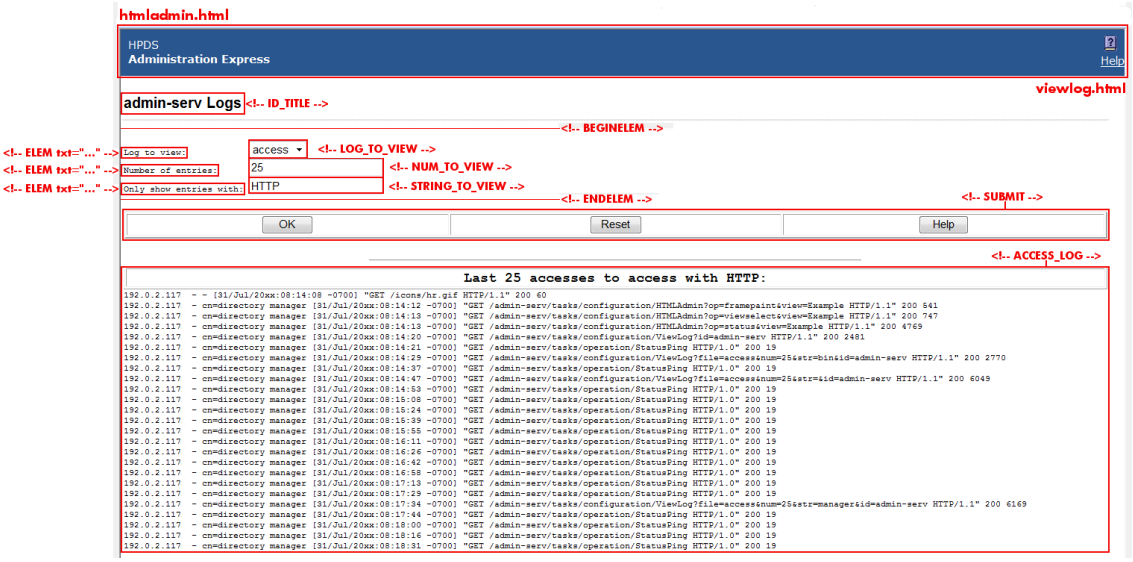
```
<body text="#000000" bgcolor="#FFFFFF" link="#666699" vlink="#666699"
alink="#333366">

<br>
<table BORDER=0 CELLSPACING=2 CELLPADDING=2 WIDTH="100%">
<!-- ID_TITLE -->
<p>
<!-- SHOW_DATA -->
<p>
<font face="PrimaSans BT, Verdana, sans-serif"><font size=-1>Additional
Information:</font></font>
<p>
<!-- CHECK_UPGRADE -->
<p>
<!-- SHOW_URL -->
</table>

<!-- HELPBUTTON -->

</body>
```

3.2.2.4 Files for the server logs page

There are two files formatting the server logs page:

- The body of the page, `/opt/dirsrv/share/html/viewlog.html`
- The heading of the page, `/opt/dirsrv/share/html/htmladmin.html`

Figure 3-10 Log view page elements



The page information is set through the inserted directives. The server instance name is set in the `ID_TITLE` directive. The log is displayed through the `ACCESS_LOG` directives. The form at the top is formatted with directive pairs, one which sets the descriptive text and the other inserting the field type. For example, this sets the log type menu:

```
<form method=GET action=ViewLog>
<font face="PrimaSans BT, Verdana, sans-serif"><font size=-1>
```

```
<!-- BEGINELEM -->
<!-- ELEM txt="Log to view:              " -->
<!-- LOG_TO_VIEW -->
....
<!-- SUBMIT -->
</font></font>
</form>
```

3.2.3 Admin Express directives

The Admin Express directives are HTML comments that are interpreted by the CGI scripts; these directives are used to set form fields and to pull data from the server configuration and log files.

Table 3-2 Admin Express directives

Directive	Description	Example
ACCESS_LOG	Inserts the server log file.	<!-- ACCESS_LOG -->
ADMURL		<!-- ADMURL -->
BEGINELEM	Marks the opening of form input elements. This is always paired with ENDELEM.	<!-- BEGINELEM -->
CHECK_UPGRADE		<!-- CHECK_UPGRADE -->
ELEM	Inserts a text element. This has one argument, txt=, which defines the text to use.	<!-- ELEM txt="Field name here: " -->
ELEMADD	Inserts a text element. This has one argument, txt=, which defines the text to use.	<!-- ELEMADD txt="Field name here: " -->
ENDELEM	Marks the ending of form input elements. This is always paired with BEGINELEM.	<!-- ENDELEM -->
HELP_BUTTON	Inserts a button to open context-specific help.	<!-- HELP_BUTTON -->
HELPLINK	Inserts a link to the general Admin Express help file.	<!-- HELPLINK -->
HIDDEN_ID		<!-- HIDDEN_ID -->
ID_TITLE	Inserts the name of the server instance, such as admin-serv or example (if the Directory Server instance name is slapd-example)	<!-- ID_TITLE -->
INCLUDEIFEXISTS	Inserts the contents of the HTML file. The inserted file should include both the text and any HTML markup.	<!-- INCLUDEIFEXISTS "file.html" -->
LOG_TO_VIEW	Inserts a drop-down menu with the types of logs available to view.	<!-- LOG_TO_VIEW -->
NUM_TO_VIEW	Inserts a form field to set the number of lines to return.	<!-- NUM_TO_VIEW -->
REFRESHINTERVAL	Inserts a form field to set the refresh interval (in seconds) for replication monitoring.	<!-- REFRESHINTERVAL -->
SERVHOST		<!-- SERVHOST -->
SERVPORT		<!-- SERVPORT -->
SHOW_DATA	Inserts the server data from the configuration file, including the port number, installation date, and build number.	<!-- SHOW_DATA -->
SHOW_URL		<!-- SHOW_URL -->
SITEROOT		<!-- SITEROOT -->

Table 3-2 Admin Express directives *(continued)*

Directive	Description	Example
`STRING_TO_VIEW`	Inserts a form field to use to set the search string for the logs.	`<!-- STRING_TO_VIEW -->`
`SUBMIT`	Inserts a three-button set: to save or submit the form; to reset the form; and to open a help topic.	`<!-- SUBMIT -->`

4 Admin Server command-line tools

The Admin Server has command-line utilities which make it easier to manage the Admin Server without having to launch the Admin Console.

This chapter explains where to find and how to use the Admin Server tools.

4.1 sec-activate

The `sec-activate` tool activates and deactivates SSL for the Admin Server.

- "Location"
- "Syntax"

Location The `sec-activate` tool is located in the `/opt/dirsrv/lib/cgi-bin` directory.

Syntax

```
sec-activate serverRoot SSLEnabled
```

Argument	Description
`serverRoot`	The location of the Admin Server configuration directory. The default location is `/etc/opt/dirsrv/admin-serv`.
`SSLEnabled`	Sets whether to turn SSL `on` or `off` for the Admin Server.

For example:

```
sec-activate /etc/opt/dirsrv/admin-serv on
```

4.2 modutil

The `modutil` tool is a command-line utility for managing PKCS #11 module information stored in `secmod.db` files or hardware tokens. `modutil` can perform a variety of security database operations:

- Adding and deleting PKCS #11 modules
- Changing passwords
- Setting defaults
- Listing module contents
- Enabling or disabling slots
- Enabling or disabling FIPS-140-1 compliance
- Assigning default providers for cryptographic operations
- Creating `key3.db`, `cert8.db`, and `secmod.db` security databases.

Security module database management is part of a process that typically involves managing key databases (`key3.db` files) and certificate databases (`cert8.db` files). The key, certificate, and PKCS #11 module management process generally begins with creating the keys and key database necessary to generate and manage certificates and the certificate database.

- "Location"
- "Syntax"
- "Tasks and options"
- "JAR information file"
- "Examples of using modutil"

Location The `modutil` tool is located in the `/opt/dirsrv/bin` folder.

Syntax

```
modutil task [option]
```

Where *task* is one of the commands listed in Table 4-1 "Task commands for modutil" and *option* is from Table 4-2 "Options for modutil". Each `modutil` command can take one task and one option.

Tasks and options You can use the `modutil` tool to perform a number of different tasks. These tasks are specified through the use of commands and options. Commands specify the task to perform. Options modify a task command.

NOTE:

Each `modutil` command can take one task and one option.

Table 4-1 "Task commands for modutil" describes what the `modutil` commands do and what options are available for each. Table 4-2 "Options for modutil" defines what the options do.

Table 4-1 Task commands for modutil

Tasks	Description	Allowed options
-add *moduleName*	Adds the named PKCS #11 module to the database.	-libfile *libraryFile* -mechanisms *mechanismList*
-changepw *token*	Changes the password for the named token. If the token has not been initialized, this option initializes it with the supplied password. In this context, the term *password* is equivalent to a personal identification number (PIN).	-pwfile *passwordFile* -newpwfile *newPasswordFile*
-create	Creates new `secmod.db`, `key3.db`, and `cert8.db` files. If any of these security databases already exist in a specified directory, the `modutil` tool displays an error message.	-dbdir *dbFolder*
-default *moduleName*	Sets the security mechanisms for which the named module is a default provider.	-mechanisms *mechanismList*
-delete *moduleName*	Deletes the named module. You cannot delete the internal PKCS #11 module.	
-disable *moduleName*	Disables all slots on the named module. To disable a specific slot, use the `-slot` option.	-slot *slotName*
-enable *moduleName*	Enables all slots on the named module. To enable a specific slot, use the `-slot` option.	-slot *slotName*
-fips `true` | `false`	Enables or disables FIPS-140-1 compliance for the internal module. `true` enabled FIPS compliance, and `false` disable FIPS compliance.	
-force	Disables the `modutil` tool's interactive prompts so it can be run from a script. Use this command only after manually testing each planned operation to check for warnings and to ensure that bypassing the prompts will cause no security lapses or loss of database integrity.	

Table 4-1 Task commands for modutil *(continued)*

Tasks	Description	Allowed options
-jar *JARfile*	Adds a new PKCS #11 module to the database. The module must be contained in the named JAR file. The JAR file identifies all files to install, the module name, and mechanism flags. It should also contain any files to be installed on the target machine, including the PKCS #11 module library and other files, such as documentation. The JAR file uses the Netscape Server PKCS #11 JAR format. See "JAR information file" for more information on creating JAR files.	-installdir *installation_directory* -tempdir *temporaryFolder*
-list *[moduleName]*	Shows basic information about the contents of the `secmod.db` file. To display detailed information about a particular module, including its slots and tokens, specify a value for *moduleName*.	
-undefault *moduleName*	Specifies the security mechanisms for which the named module will not be a default provider.	-mechanisms *mechanismList*

Table 4-2 "Options for modutil" describes the different options for the `modutil` task commands.

Table 4-2 Options for modutil

Option	Description
-dbdir *dbFolder*	Specifies a folder in which to access or create security module database files. This argument is required for every command. This should point to the Admin Server configuration directory. For example: `-dbdir /etc/opt/dirsrv/admin-serv`
-installdir *installation_directory*	Specifies the root installation folder for the files supplied with the `-jar`*JAR-file* task. The *installation_directory* folder should be one in which it is appropriate to store dynamic library files.
-libfile *libraryFile*	Specifies the library file which contains the PKCS #11 module that is being added to the database. Use the full path to identify the file.

Table 4-2 Options for modutil *(continued)*

Option	Description
-mechanisms *mechanismList*	Specifies the security mechanisms for which a particular module is the default provider. The *mechanismList* is a colon-separated list of mechanism names. Enclose this list in quotation marks if it contains spaces. The module becomes a default provider for the listed mechanisms when those mechanisms are enabled. If more than one module is assigned as a mechanism's default provider, the mechanism's default provider is listed as undefined. The following mechanisms are currently available: • RSA • DSA • RC2, RC4, and RC5 • AES • DES • DH • SHA1 and SHA256 • SSL and TLS • MD2 and MD5 • RANDOM (for random number generation) • FRIENDLY (for certificates that are publicly readable).
-newpwfile *newPasswordFile*	Specifies a text file containing a token's new password. This allows the password to be automatically updated when using the `-changepw` command.
-nocertdb	Instructs `modutil` not to open the certificate or key databases. This has several effects: • When used with the `-changepw` command, no one is able to set or change the password on the internal module, because the password is stored in `key3.db`. • When used with the `-create` command, only a `secmod.db` file will be created; `cert8.db` and `key3.db` will not be created. • When used with the `-jar` command, signatures on the JAR file will not be checked.
-pwfile *passwordFile*	Specifies a text file containing a token's current password. This allows automatic entry of the password when using the `-changepw` command.
-slot *slotName*	Specifies a particular slot to enable or disable when using the `-enable` or `-disable`options.
-tempdir *temporaryFolder*	Specifies a folder in which to store temporary files created by the `-jar` command. If a temporary folder is not specified, the current folder is used.

JAR information file JAR (Java Archive) is a platform-independent file format that aggregates many files into one. JAR files are used by `modutil` to install PKCS #11 modules. When `modutil` uses a JAR file, a special JAR information file must be included. This information file contains special scripting instructions and must be specified in the JAR file's `MANIFEST` file. Although the information file can have any name, it is specified using the `Pkcs11_install_script METAINFO` command.

For details on how to declare this `METAINFO` command in the `MANIFEST`, see http://docs.sun.com/source/816-6164-10/contents.htm.

If a PKCS #11 installer script is stored in the information file `pk11install`, the text file for the Signing Tool contains the following `METAINFO` tag:

```
+ Pkcs11_install_script: pk11install
```

Examples of using modutil

- "Creating database files"
- "Displaying module information"
- "Setting a default provider"

- “Enabling a slot”
- “Enabling FIPS compliance”
- “Adding a cryptographic module”
- “Changing the password on a token”

Creating database files To create a set of security management database files in a directory:

```
modutil -create -dbdir /etc/opt/dirsrv/admin-serv

WARNING: Performing this operation while the browser is running could cause
corruption of your security databases. If the browser is currently running,
you should exit browser before continuing this operation. Type
'q <enter>' to abort, or <enter> to continue:

Creating "/etc/opt/dirsrv/admin-serv/key3.db"...done.
Creating "/etc/opt/dirsrv/admin-serv/cert8.db"...done.
Creating "/etc/opt/dirsrv/admin-serv/secmod.db"...done.
```

Displaying module information To retrieve detailed information about a specific module:

```
modutil -list -dbdir /etc/opt/dirsrv/admin-serv

Using database directory /etc/opt/dirsrv/admin-serv...

Listing of PKCS #11 Modules
-----------------------------------------------------------
  1. NSS Internal PKCS #11 Module
         slots: 2 slots attached
        status: loaded

         slot: NSS Internal Cryptographic Services
        token: NSS Generic Crypto Services

         slot: NSS User Private Key and Certificate Services
        token: NSS Certificate DB
-----------------------------------------------------------
```

Setting a default provider To make a specific module the default provider for the RSA, DSA, and RC2 security mechanisms:

```
modutil -default "Cryptographic Module" -dbdir /etc/opt/dirsrv/admin-serv  \
-mechanisms RSA:DSA:RC2

WARNING: Performing this operation while the browser is running could cause
corruption of your security databases. If the browser is currently running,
you should exit browser before continuing this operation. Type 'q <enter>'
to abort, or <enter> to continue:

Using database directory /etc/opt/dirsrv/admin-serv...
Successfully changed defaults.
```

Enabling a slot To enable a particular slot in a module:

```
modutil -enable "Cryptographic Module" -slot "Cryptographic Reader" \
-dbdir /etc/opt/dirsrv/admin-serv

WARNING: Performing this operation while the browser is running could cause
corruption of your security databases. If the browser is currently running,
you should exit browser before continuing this operation. Type
'q <enter>' to abort, or <enter> to continue:

Using database directory /etc/opt/dirsrv/admin-serv...
Slot "Cryptographic Reader" enabled.
```

Enabling FIPS compliance To enable FIPS-140-1 compliance in the Admin Server's internal module:

```
modutil -fips true

WARNING: Performing this operation while the browser is running could cause
corruption of your security databases. If the browser is currently running,
you should exit browser before continuing this operation. Type
'q <enter>' to abort, or <enter> to continue:

FIPS mode enabled.
```

Adding a cryptographic module To add a new cryptographic module to the database:

```
modutil -dbdir "/etc/opt/dirsrv/admin-serv" -add "Cryptorific Module" \
-libfile "/crypto.so" -mechanisms RSA:DSA:RC2:RANDOM

WARNING: Performing this operation while the browser is running could cause
corruption of your security databases. If the browser is currently running,
you should exit browser before continuing this operation. Type 'q <enter>'
to abort, or <enter> to continue:

Using database directory /etc/opt/dirsrv/admin-serv...
Module "Cryptorific Module" added to database.
```

Changing the password on a token To change the password for a security device in use by a module.

```
modutil -dbdir "/etc/opt/dirsrv/admin-serv" -changepw "Admin Server Certificate DB"

WARNING: Performing this operation while the browser is running could cause
corruption of your security databases. If the browser is currently running,
you should exit browser before continuing this operation. Type 'q <enter>'
to abort, or <enter> to continue:

Using database directory /etc/opt/dirsrv/admin-serv...
Enter old password:
Enter new password:
Re-enter new password:

Token "Admin Server Certificate DB" password changed successfully.
```

5 Support and other resources

5.1 Contacting HP

5.1.1 Information to collect before contacting HP

Be sure to have the following information available before you call contact HP:

- Software product name
- Hardware product model number
- Operating system type and version
- Applicable error message
- Third-party hardware or software
- Technical support registration number (if applicable)

5.1.2 How to contact HP technical support

Use the following methods to contact HP technical support:

- In the United States, see the Customer Service / Contact HP United States website for contact options:

  http://welcome.hp.com/country/us/en/contact_us.html

- In other locations, see the Contact HP Worldwide website for contact options:

  http://welcome.hp.com/country/us/en/wwcontact.html

5.1.3 HP authorized resellers

For the name of the nearest HP authorized reseller, see the following sources:

- In the United States, see the HP U.S. service locator website at:

  http://www.hp.com/service_locator

- In other locations, see the Contact HP worldwide website at:

  http://welcome.hp.com/country/us/en/wwcontact.html

5.1.4 Documentation feedback

HP welcomes your feedback. To make comments and suggestions about product documentation, send a message to:

docsfeedback@hp.com

Include the document title and manufacturing part number in your message. All submissions become the property of HP.

5.2 Related information

5.2.1 HP-UX Directory Server documentation set

- *HP-UX Directory Server release notes*

  The release notes contain important information on new features, fixed bugs, known issues and workarounds, and other important information for this specific version of the HP-UX Directory Server.

- *HP-UX Directory Server administrator guide*

  This guide contains information and procedures you need to perform to maintain your Directory Server.

- *HP-UX Directory Server administration server guide*

  The Admin Server is a support server that drives access to the Directory Server Console , provides a web server for Directory Server web applications, and stores some Directory Server configuration. This guide covers how to manage the Admin Server through the Console, through the command line, and through the web services. It also covers basic Admin Server concepts.

- *HP-UX Directory Server configuration, command, and file reference*

  This document provides reference information on the command line scripts, configuration attributes, and log files shipped with the Directory Server.

- *HP-UX Directory Server console guide*

  This guide covers the basic structure of the Console for both the Directory Server and the Admin Server and provides an overview of how to use the main Console to manage users and access within the Console.

- *HP-UX Directory Server deployment guide*

  This guide covers the basic considerations that should be addressed before deploying the Directory Server. The decisions made during this phase can have a significant and lasting affect on the effectiveness, efficiency, and scalability of your Directory Server. You should have a good understanding of your Directory Server requirements before moving on to the installation phase.

- *HP-UX Directory Server installation guide*

  This manual contains information and procedures for installing your Directory Serveras well as procedures for migrating from Netscape Directory Server 6.21 or Red Hat Directory Server 7.1.

- *HP-UX Directory Server plug-in reference*

  This reference document describes server plug-ins, as well as how to write server plug-ins in order to customize and to extend the capabilities of the HP-UX Directory Server.

- *HP-UX Directory Server schema reference*

  This reference provides an overview of some of the basic concepts of the directory schema, including lists and descriptions of default schema files, and descriptions of object classes, attributes, object identifiers (OIDs), schema checking, and extending server schema.

For the latest information about HP-UX Directory Server, including current release notes, complete product documentation, technical notes, and white papers, as well as other HP Internet and Security products, see the HP-UX Directory Server documentation site at:

http://docs.hp.com/en/internet.html.

5.2.2 HP-UX documentation set

For the latest information about the HP-UX operating system, including current release notes, complete product documentation, technical notes, and white papers, see the HP-UX Operating Environments documentation sites for the version of HP-UX you use:

- HP-UX 11i v3 Operating Environments: http://docs.hp.com/en/oshpux11iv3.html
- HP-UX 11i v2 Operating Environments: http://docs.hp.com/en/oshpux11iv2.html

5.2.3 Troubleshooting resources

- You can search a technical knowledge database available on the HP IT Resource Center (ITRC) website at:

  http://itrc.hp.com/

- To seek solutions to problems, you can post messages on the ITRC Forums page at the following website (select the HP-UX area in the **Areas of peer problem solving** section):

  http://forums.itrc.hp.com/

5.3 Typographic conventions

This document uses the following typographical conventions:

Book title	The title of a book. On the web, this can be a hyperlink to the book itself.
`Command`	A command name or command phrase, for example `ls -a`.
`Computer output`	Information displayed by the computer.
Ctrl+x or **Ctrl-x**	A key sequence that indicates you must hold down the keyboard key labeled **Ctrl** while you press the letter `x`.
`ENVIRONMENT VARIABLE`	The name of an environment variable, for example, `PATH`.
Key	The name of a keyboard key. **Return** and **Enter** both refer to the same key.
Term	A term or phrase that is defined in the body text of the document, not in a glossary.
`User input`	Indicates commands and text that you type exactly as shown.
`Replaceable`	The name of a placeholder that you replace with an actual value.
[ ]	In command syntax statements, these characters enclose optional content.
{ }	In command syntax statements, these characters enclose required content.
|	The character that separates items in a linear list of choices.
...	Indicates that the preceding element can be repeated one or more times.
WARNING	An alert that calls attention to important information that, if not understood or followed, results in personal injury.
CAUTION	An alert that calls attention to important information that, if not understood or followed, results in data loss, data corruption, or damage to hardware or software.
IMPORTANT	An alert that calls attention to essential information.
NOTE	An alert that contains additional or supplementary information.
TIP	An alert that provides helpful information.

Glossary

A

access control instruction — *See* ACI.

access control list — *See* ACL.

access rights — In the context of access control, specify the level of access granted or denied. Access rights are related to the type of operation that can be performed on the directory. The following rights can be granted or denied: read, write, add, delete, search, compare, selfwrite, proxy and all.

account inactivation — Disables a user account, group of accounts, or an entire domain so that all authentication attempts are automatically rejected.

ACI — An instruction that grants or denies permissions to entries in the directory.
See also access control instruction.

ACL — The mechanism for controlling access to your directory.
See also access control list.

All IDs Threshold — *Replaced with the ID list scan limit in Directory Server version 7.1.* A size limit which is globally applied to every index key managed by the server. When the size of an individual ID list reaches this limit, the server replaces that ID list with an All IDs token.
See also ID list scan limit.

All IDs token — A mechanism which causes the server to assume that all directory entries match the index key. In effect, the All IDs token causes the server to behave as if no index was available for the search request.

anonymous access — When granted, allows anyone to access directory information without providing credentials, and regardless of the conditions of the bind.

approximate index — Allows for efficient approximate or "sounds-like" searches.

attribute — Holds descriptive information about an entry. Attributes have a label and a value. Each attribute also follows a standard syntax for the type of information that can be stored as the attribute value.

attribute list — A list of required and optional attributes for a given entry type or object class.

authenticating directory server — In pass-through authentication (PTA), the authenticating Directory Server is the Directory Server that contains the authentication credentials of the requesting client. The PTA-enabled host sends PTA requests it receives from clients to the host.

authentication — (1) Process of proving the identity of the client user to the Directory Server. Users must provide a bind DN and either the corresponding password or certificate in order to be granted access to the directory. Directory Server allows the user to perform functions or access files and directories based on the permissions granted to that user by the directory administrator.

(2) Allows a client to make sure they are connected to a secure server, preventing another computer from impersonating the server or attempting to appear secure when it is not.

authentication certificate — Digital file that is not transferable and not forgeable and is issued by a third party. Authentication certificates are sent from server to client or client to server in order to verify and authenticate the other party.

B

base distinguished name — *See* base DN.

base DN — Base distinguished name. A search operation is performed on the base DN, the DN of the entry and all entries below it in the directory tree.

bind distinguished name *See* bind DN.

bind DN Distinguished name used to authenticate to Directory Server when performing an operation.

bind rule In the context of access control, the bind rule specifies the credentials and conditions that a particular user or client must satisfy in order to get access to directory information.

branch entry An entry that represents the top of a subtree in the directory.

browser Software, such as Mozilla Firefox, used to request and view World Wide Web material stored as HTML files. The browser uses the HTTP protocol to communicate with the host server.

browsing index Speeds up the display of entries in the Directory Server Console. Browsing indexes can be created on any branch point in the directory tree to improve display performance.
See also virtual list view index .

C

CA *See* Certificate Authority.

cascading replication In a cascading replication scenario, one server, often called the hub supplier, acts both as a consumer and a supplier for a particular replica. It holds a read-only replica and maintains a changelog. It receives updates from the supplier server that holds the master copy of the data and in turn supplies those updates to the consumer.

certificate A collection of data that associates the public keys of a network user with their DN in the directory. The certificate is stored in the directory as user object attributes.

Certificate Authority Company or organization that sells and issues authentication certificates. You may purchase an authentication certificate from a Certification Authority that you trust. Also known as a CA.

CGI Common Gateway Interface. An interface for external programs to communicate with the HTTP server. Programs written to use CGI are called CGI programs or CGI scripts and can be written in many of the common programming languages. CGI programs handle forms or perform output parsing that is not done by the server itself.

chaining A method for relaying requests to another server. Results for the request are collected, compiled, then returned to the client.

changelog A changelog is a record that describes the modifications that have occurred on a replica. The supplier server then replays these modifications on the replicas stored on replica servers or on other masters, in the case of multi-master replication.

character type Distinguishes alphabetic characters from numeric or other characters and the mapping of upper-case to lower-case letters.

ciphertext Encrypted information that cannot be read by anyone without the proper key to decrypt the information.

class definition Specifies the information needed to create an instance of a particular object and determines how the object works in relation to other objects in the directory.

class of service *See* CoS.

classic CoS A classic CoS identifies the template entry by both its DN and the value of one of the target entry's attributes.

client *See* LDAP client.

code page An internal table used by a locale in the context of the internationalization plug-in that the operating system uses to relate keyboard keys to character font displays.

collation order Provides language and cultural-specific information about how the characters of a given language are to be sorted. This information might include the sequence of letters in the alphabet or how to compare letters with accents to letters without accents.

consumer Server containing replicated directory trees or subtrees from a supplier server.

consumer server In the context of replication, a server that holds a replica that is copied from a different server is called a consumer for that replica.

CoS A method for sharing attributes between entries in a way that is invisible to applications.

CoS definition entry Identifies the type of CoS you are using. It is stored as an LDAP subentry below the branch it affects.

CoS template entry Contains a list of the shared attribute values.
See also template entry.

D

daemon A background process on a Unix machine that is responsible for a particular system task. Daemon processes do not need human intervention to continue functioning.

DAP Directory Access Protocol. The ISO X.500 standard protocol that provides client access to the directory.

data master The server that is the master source of a particular piece of data.

database link An implementation of chaining. The database link behaves like a database but has no persistent storage. Instead, it points to data stored remotely.

default index One of a set of default indexes created per database instance. Default indexes can be modified, although care should be taken before removing them, as certain plug-ins may depend on them.

definition entry *See* CoS definition entry.

Directory Access Protocol *See* DAP.

Directory Manager The privileged database administrator, comparable to the root user in UNIX. Access control does not apply to the Directory Manager.

directory service A database application designed to manage descriptive, attribute-based information about people and resources within an organization.

directory tree The logical representation of the information stored in the directory. It mirrors the tree model used by most filesystems, with the tree's root point appearing at the top of the hierarchy. Also known as DIT.

distinguished name String representation of an entry's name and location in an LDAP directory.

DIT *See* directory tree.

DM *See* Directory Manager.

DN *See* distinguished name.

DNS Domain Name System. The system used by machines on a network to associate standard IP addresses (such as 198.93.93.10) with host names (such as `www.example.com`). Machines normally get the IP address for a host name from a DNS server, or they look it up in tables maintained on their systems.

DNS alias A DNS alias is a host name that the DNS server knows points to a different host—specifically a DNS CNAME record. Machines always have one real name, but they can have one or more aliases. For example, an alias such as `www.`*`yourdomain.domain`* might point to a real machine called `realthing.`*`yourdomain.domain`* where the server currently exists.

E

entry A group of lines in the LDIF file that contains information about an object.

entry distribution Method of distributing directory entries across more than one server in order to scale to support large numbers of entries.

entry ID list Each index that the directory uses is composed of a table of index keys and matching entry ID lists. The entry ID list is used by the directory to build a list of candidate entries that may match the client application's search request.

equality index Allows you to search efficiently for entries containing a specific attribute value.

F

file extension The section of a file name after the period or dot (.) that typically defines the type of file (for example, .GIF and .HTML). In the file name `index.html` the file extension is `html`.

file type The format of a given file. For example, graphics files are often saved in GIF format, while a text file is usually saved as ASCII text format. File types are usually identified by the file extension (for example, .GIF or .HTML).

filter A constraint applied to a directory query that restricts the information returned.

filtered role Allows you to assign entries to the role depending upon the attribute contained by each entry. You do this by specifying an LDAP filter. Entries that match the filter are said to possess the role.

G

general access When granted, indicates that all authenticated users can access directory information.

GSS-API Generic Security Services. The generic access protocol that is the native way for UNIX-based systems to access and authenticate Kerberos services; also supports session encryption.

H

host name A name for a machine in the form *machine.domain.dom*, which is translated into an IP address. For example, `www.example.com` is the machine `www` in the subdomain `example` and `com` domain.

HTML Hypertext Markup Language. The formatting language used for documents on the World Wide Web. HTML files are plain text files with formatting codes that tell browsers such as the Mozilla Firefox how to display text, position graphics, and form items and to display links to other pages.

HTTP Hypertext Transfer Protocol. The method for exchanging information between HTTP servers and clients.

HTTPD An abbreviation for the HTTP daemon or service, a program that serves information using the HTTP protocol. The daemon or service is often called an httpd.

HTTPS A secure version of HTTP, implemented using the Secure Sockets Layer, SSL.

hub In the context of replication, a server that holds a replica that is copied from a different server, and, in turn, replicates it to a third server.
See also cascading replication.

I

ID list scan limit A size limit which is globally applied to any indexed search operation. When the size of an individual ID list reaches this limit, the server replaces that ID list with an all IDs token.

index key Each index that the directory uses is composed of a table of index keys and matching entry ID lists.

indirect CoS An indirect CoS identifies the template entry using the value of one of the target entry's attributes.

international index Speeds up searches for information in international directories.

International Standards Organization *See* ISO.

IP address Internet Protocol address. A set of numbers, separated by dots, that specifies the actual location of a machine on the Internet (for example, 198.93.93.10).

ISO International Standards Organization.

K

knowledge reference Pointers to directory information stored in different databases.

L

LDAP Lightweight Directory Access Protocol. Directory service protocol designed to run over TCP/IP and across multiple platforms.

LDAP client Software used to request and view LDAP entries from an LDAP Directory Server. *See also* browser.

LDAP Data Interchange Format *See* LDAP Data Interchange Format.

LDAP URL Provides the means of locating Directory Servers using DNS, then completing the query through LDAP. A sample LDAP URL is `ldap://ldap.example.com`.

LDAPv3 Version 3 of the LDAP protocol, upon which Directory Server bases its schema format.

LDBM database A high-performance, disk-based database consisting of a set of large files that contain all the data assigned to it. The primary data store in Directory Server.

LDIF LDAP Data Interchange Format. Format used to represent Directory Server entries in text form.

leaf entry An entry under which there are no other entries. A leaf entry cannot be a branch point in a directory tree.

Lightweight Directory Access Protocol *See* LDAP.

locale Identifies the collation order, character type, monetary format and time / date format used to present data for users of a specific region, culture, and/or custom. This includes information on how data of a given language is interpreted, stored, or collated. The locale also indicates which code page should be used to represent a given language.

M

managed object A standard value which the SNMP agent can access and send to the NMS. Each managed object is identified with an official name and a numeric identifier expressed in dot-notation.

managed role Allows creation of an explicit enumerated list of members.

management information base *See* MIB.

mapping tree A data structure that associates the names of suffixes (subtrees) with databases.

master *See* supplier.

master agent *See* SNMP master agent.

matching rule Provides guidelines for how the server compares strings during a search operation. In an international search, the matching rule tells the server what collation order and operator to use.

MD5 A message digest algorithm by RSA Data Security, Inc., which can be used to produce a short digest of data that is unique with high probability and is mathematically extremely hard to produce; a piece of data that will produce the same message digest.

MD5 signature A message digest produced by the MD5 algorithm.

MIB Management Information Base. All data, or any portion thereof, associated with the SNMP network. We can think of the MIB as a database which contains the definitions of all SNMP managed objects. The MIB has a tree-like hierarchy, where the top level contains the most general information about the network and lower levels deal with specific, separate network areas.

MIB namespace Management Information Base namespace. The means for directory data to be named and referenced. Also called the directory tree.

monetary format Specifies the monetary symbol used by specific region, whether the symbol goes before or after its value, and how monetary units are represented.

multi-master replication An advanced replication scenario in which two servers each hold a copy of the same read-write replica. Each server maintains a changelog for the replica. Modifications made on one server

are automatically replicated to the other server. In case of conflict, a time stamp is used to determine which server holds the most recent version.

multiplexor The server containing the database link that communicates with the remote server.

N

n + 1 directory problem The problem of managing multiple instances of the same information in different directories, resulting in increased hardware and personnel costs.

name collisions Multiple entries with the same distinguished name.

nested role Allows the creation of roles that contain other roles.

network management application Network Management Station component that graphically displays information about SNMP managed devices, such as which device is up or down and which and how many error messages were received.

network management station *See* NMS.

NIS Network Information Service. A system of programs and data files that Unix machines use to collect, collate, and share specific information about machines, users, filesystems, and network parameters throughout a network of computers.

NMS Powerful workstation with one or more network management applications installed. Also network management station.

ns-slapd Red Hat's LDAP Directory Server daemon or service that is responsible for all actions of the Directory Server.
See also slapd.

O

object class Defines an entry type in the directory by defining which attributes are contained in the entry.

object identifier A string, usually of decimal numbers, that uniquely identifies a schema element, such as an object class or an attribute, in an object-oriented system. Object identifiers are assigned by ANSI, IETF or similar organizations.
See also OID.

OID *See* object identifier.

operational attribute Contains information used internally by the directory to keep track of modifications and subtree properties. Operational attributes are not returned in response to a search unless explicitly requested.

P

parent access When granted, indicates that users have access to entries below their own in the directory tree if the bind DN is the parent of the targeted entry.

pass-through authentication *See* PTA.

pass-through subtree In pass-through authentication, the PTA directory server will pass through bind requests to the authenticating directory server from all clients whose DN is contained in this subtree.

password file A file on Unix machines that stores Unix user login names, passwords, and user ID numbers. It is also known as `/etc/passwd` because of where it is kept.

password policy A set of rules that governs how passwords are used in a given directory.

PDU Encoded messages which form the basis of data exchanges between SNMP devices. Also protocol data unit.

permission In the context of access control, permission states whether access to the directory information is granted or denied and the level of access that is granted or denied.
See also access rights.

pointer CoS A pointer CoS identifies the template entry using the template DN only.

presence index Allows searches for entries that contain a specific indexed attribute.

protocol A set of rules that describes how devices on a network exchange information.

protocol data unit *See* PDU.

proxy authentication A special form of authentication where the user requesting access to the directory does not bind with its own DN but with a proxy DN.

proxy DN Used with proxied authorization. The proxy DN is the DN of an entry that has access permissions to the target on which the client-application is attempting to perform an operation.

PTA Mechanism by which one Directory Server consults another to check bind credentials. Also pass-through authentication.

PTA directory server In pass-through authentication (PTA), the PTA Directory Server is the server that sends (passes through) bind requests it receives to the authenticating directory server.

PTA LDAP URL In pass-through authentication, the URL that defines the authenticating directory server, pass-through subtree(s), and optional parameters.

R

RAM Random access memory. The physical semiconductor-based memory in a computer. Information stored in RAM is lost when the computer is shut down.

RDN The name of the actual entry itself, before the entry's ancestors have been appended to the string to form the full distinguished name. Also relative distinguished name.

read-only replica A replica that refers all update operations to read-write replicas. A server can hold any number of read-only replicas.

read-write replica A replica that contains a master copy of directory information and can be updated. A server can hold any number of read-write replicas.

referential integrity Mechanism that ensures that relationships between related entries are maintained within the directory.

referral (1) When a server receives a search or update request from an LDAP client that it cannot process, it usually sends back to the client a pointer to the LDAP sever that can process the request.

(2) In the context of replication, when a read-only replica receives an update request, it forwards it to the server that holds the corresponding read-write replica. This forwarding process is called a referral.

relative distinguished name *See* RDN.

replica A database that participates in replication.

replica-initiated replication Replication configuration where replica servers, either hub or consumer servers, pull directory data from supplier servers. This method is available only for legacy replication.

replication Act of copying directory trees or subtrees from supplier servers to replica servers.

replication agreement Set of configuration parameters that are stored on the supplier server and identify the databases to replicate, the replica servers to which the data is pushed, the times during which replication can occur, the DN and credentials used by the supplier to bind to the consumer, and how the connection is secured.

RFC Request for Comments. Procedures or standards documents submitted to the Internet community. People can send comments on the technologies before they become accepted standards.

role An entry grouping mechanism. Each role has members, which are the entries that possess the role.

role-based attributes Attributes that appear on an entry because it possesses a particular role within an associated CoS template.

root The most privileged user available on Unix machines. The root user has complete access privileges to all files on the machine.

root suffix The parent of one or more sub suffixes. A directory tree can contain more than one root suffix.

S

SASL An authentication framework for clients as they attempt to bind to a directory. Also Simple Authentication and Security Layer .

schema Definitions describing what types of information can be stored as entries in the directory. When information that does not match the schema is stored in the directory, clients attempting to access the directory may be unable to display the proper results.

schema checking Ensures that entries added or modified in the directory conform to the defined schema. Schema checking is on by default, and users will receive an error if they try to save an entry that does not conform to the schema.

Secure Sockets Layer *See* SSL.

self access When granted, indicates that users have access to their own entries if the bind DN matches the targeted entry.

Server Console Java-based application that allows you to perform administrative management of your Directory Server from a GUI.

server daemon The server daemon is a process that, once running, listens for and accepts requests from clients.

Server Selector Interface that allows you select and configure servers using a browser.

server service A process on Windows that, once running, listens for and accepts requests from clients. It is the SMB server on Windows NT.

service A background process on a Windows machine that is responsible for a particular system task. Service processes do not need human intervention to continue functioning.

SIE Server Instance Entry. The ID assigned to an instance of Directory Server during installation.

Simple Authentication and Security Layer *See* SASL.

Simple Network Management Protocol *See* SNMP.

single-master replication The most basic replication scenario in which multiple servers, up to four, each hold a copy of the same read-write replicas to replica servers. In a single-master replication scenario, the supplier server maintains a changelog.

SIR *See* supplier-initiated replication.

slapd LDAP Directory Server daemon or service that is responsible for most functions of a directory except replication.
See also ns-slapd.

SNMP Used to monitor and manage application processes running on the servers by exchanging data about network activity. Also Simple Network Management Protocol.

SNMP master agent Software that exchanges information between the various subagents and the NMS.

SNMP subagent Software that gathers information about the managed device and passes the information to the master agent. Also called a subagent.

SSL A software library establishing a secure connection between two parties (client and server) used to implement HTTPS, the secure version of HTTP. Also called Secure Sockets Layer.

standard index index maintained by default.

sub suffix A branch underneath a root suffix.

subagent *See* SNMP subagent.

substring index Allows for efficient searching against substrings within entries. Substring indexes are limited to a minimum of two characters for each entry.

suffix The name of the entry at the top of the directory tree, below which data is stored. Multiple suffixes are possible within the same directory. Each database only has one suffix.

superuser The most privileged user available on Unix machines. The superuser has complete access privileges to all files on the machine. Also called root.

supplier Server containing the master copy of directory trees or subtrees that are replicated to replica servers.

supplier server In the context of replication, a server that holds a replica that is copied to a different server is called a supplier for that replica.

supplier-initiated replication Replication configuration where supplier servers replicate directory data to any replica servers.

symmetric encryption Encryption that uses the same key for both encrypting and decrypting. DES is an example of a symmetric encryption algorithm.

system index Cannot be deleted or modified as it is essential to Directory Server operations.

T

target In the context of access control, the target identifies the directory information to which a particular ACI applies.

target entry The entries within the scope of a CoS.

TCP/IP Transmission Control Protocol/Internet Protocol. The main network protocol for the Internet and for enterprise (company) networks.

template entry *See* CoS template entry.

time/date format Indicates the customary formatting for times and dates in a specific region.

TLS The new standard for secure socket layers; a public key based protocol. Also Transport Layer Security.

topology The way a directory tree is divided among physical servers and how these servers link with one another.

Transport Layer Security *See* TLS.

U

uid A unique number associated with each user on a Unix system.

URL Uniform Resource Locater. The addressing system used by the server and the client to request documents. It is often called a location. The format of a URL is *protocol*`://`*machine*`:`*port*`/`*document*. The port number is necessary only on selected servers, and it is often assigned by the server, freeing the user of having to place it in the URL.

V

virtual list view index Speeds up the display of entries in the Directory Server Console. Virtual list view indexes can be created on any branch point in the directory tree to improve display performance. *See also* browsing index.

X

X.500 standard The set of ISO/ITU-T documents outlining the recommended information model, object classes and attributes used by directory server implementation.

Index