# HP Database and Middleware Automation

for the HP-UX, IBM AIX, Red Hat Enterprise Linux, Solaris, and Windows®
operating systems

Software Version: 1.00

(Stratavia Data Palette version 6.0.11)

# SSL Configuration Guide

Manufacturing Part Number: none

Document Release Date: September 2011

Software Release Date: November 2010

# Legal Notices

## Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

## Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

## Copyright Notices

## Trademark Notices

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Java is a registered trademark of Oracle and/or its affiliates.

Windows is a U.S. registered trademark of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

# Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

*http://h20230.www2.hp.com/selfsolve/manuals*

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

*http://h20229.www2.hp.com/passport-registration.html*

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

# Support

Visit the HP Software Support Online web site at:

*www.hp.com/go/hpsoftwaresupport*

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport user ID, go to:

*http://h20229.www2.hp.com/passport-registration.html*

To find more information about access levels, go to:

*http://h20230.www2.hp.com/new_access_levels.jsp*

# Contents

# 1 About this Guide

## Introduction

This document provides instructions for configuring the Secure Sockets Layer (SSL) encryption protocol for communication between the HP Database and Middleware Automation (HP DMA) Nerve Center/Web Server and the HP DMA agent residing on each target server. This requires two steps:

- Configuring SSL on the HP DMA Server
- Configuring SSL on the Agent Servers

## Audience

This guide is primarily intended for the following IT professionals:

- Database administrators, who are responsible for installing and maintaining database software and assuring compliance with security standards.
- Application administrators, who are responsible for installing and maintaining application server software (middleware).
- Data center operators, who are responsible for executing automated data center tasks.

## Prerequisites

To perform the procedures include in this guide, you must be able to log in to both the server hosting the HP DMA Nerve Center/Web Server and the agent servers as the datapal OS user and as root.

You should be familiar with the operation of HP DMA and understand how SSL works.

## Conventions Used

The following typographical conventions are used in this guide:

| Font | Meaning |
|---|---|
| `Courier` | Information that you type on the command line or output from a command. For example:<br>`cd /opt/datapalette` |
| *`<italics>`* | A placeholder for a value that you specify. For example *`<password>`* represents the keystore password. |

# Related Documents

For additional information about HP DMA, see the following documents:

- *HP Database and Middleware Automation User Guide*
- *HP Database and Middleware Automation Installation Guide*

# 2 Configuring SSL on the HP DMA Server

To configure SSL on the HP DMA server, you must complete the following three steps:

1. Generate a private key for the server.
2. Obtain a signed server certificate.
3. Configure the HP DMA server to use that certificate for authentication.

For a production environment, you should have the server certificate signed by a trusted Certificate Authority (CA). For testing purposes, you may be able to use a self-signed server certificate (see Using a Self-Signed Server Certificate on page 17).

⚠ The process of producing a PDF file inserts line breaks in long lines of text, including commands that should be entered on a single line. When you execute the commands shown in this document, be sure to first remove any line breaks that might be present.

## About keytool

Many procedures in this document use the `keytool` utility, which is located in the following directory on the HP DMA server and the agent (target) servers:

`<installDir>/java/bin`

Here, *<installDir>* is the directory where HP DMA is installed (`/opt/datapalette` by default). To follow the procedures in this document as written, do one of the following things before executing the `keytool` command:

- `cd` to `<installDir>/java/bin`
- Add `<installDir>/java/bin` to your PATH

## Generate a Private Key for the Server

The first step in configuring SSL on the HP DMA server is to generate a private key for that server. You can do this by using the `keytool` utility provided with HP DMA.

If the keystore already exists on the server, you can add the key to it. If the keystore does not yet exist, `keytool` will create it.

### To generate a private key for the server:

1. Log in to the HP DMA server as the datapal user.
2. Execute the following command (all on one line):

```
keytool -genkey -alias <serveralias> -keyalg RSA -keysize 1024 -dname
"CN=<DMAserver>,OU=<orgunit>,O=<org>,L=<location>,S=<state>,C=<country>"
-keypass <password> -keystore <storefile> -storepass <password>
```

The placeholders used here refer to the following information:

*<serveralias>* Unique alias for the server's private key. This will be used to associate the server certificate with its private key.

*<DMAserver>* Fully qualified host name of the server hosting the HP DMA Nerve Center/Web Server.

*<orgunit>* The organizational unit (business unit) that owns this server.

*<org>* The organization (company) that owns this server.

*<location>* The city in which this server physically resides.

*<state>* The state or province in which this server physically resides.

*<country>* The country in which this server physically resides.

*<password>* The password for both the keystore and this private key.

*<storefile>* Keystore file name. For example: `/opt/datapalette/.keystore`

For example:

```
keytool -genkey -alias myserver -keyalg RSA -keysize 1024 -dname
"CN=myserver.mycompany.com,OU=IT,O=mycompany,L=Denver,S=Colorado,C=US"
-keypass mypassword -keystore /opt/datapalette/.keystore -storepass
mypassword
```

You must use the same password for the `-keypass` and `-storepass` settings.

3 To verify that the private key was created, execute the following command (all on one line):

```
keytool -list -v -keystore <storeFile> -storepass <password>
```

## Obtain a Signed Certificate

In a production environment, you should always use a server certificate signed by a trusted Certificate Authority (CA) in accordance with your security policy.

To obtain a signed certificate, you must generate a certificate signing request and submit it to your CA. The CA will send you a digitally signed certificate via email. You can then import the signed certificate into the keystore.

Before you can import your certificate, however, you must import your CA's root certificate. This will enable you to properly chain your server certificate to the root certificate. Your CA provides the root certificate.

In addition to the root certificate, your CA may provide one or more intermediate certificates. The root and intermediate certificates may be bundled in a single file, or they may be delivered as separate files. Your CA will provide instructions for importing the root and any intermediate certificates into the keystore.

The order of operations is important – you must import the root certificate (and any intermediate certificates required) before you import your signed server certificate.

### To generate the certificate signing request:

1. Log in to the HP DMA server as the datapal user.
2. Execute the following command (all on one line):

   ```
   keytool -certreq -v -alias <serveralias> -keypass <password> -keystore
   <storefile> -storepass <password>
   ```

   For example:

   ```
   keytool -certreq -v -alias myserver -keypass mypassword -keystore
   /opt/datapalette/.keystore -storepass mypassword
   ```

   Your certificate request will appear on `stdout`.
3. Submit the certificate signing request (the output of the `keytool -certreq` command) to your CA. The CA will provide instructions for submitting this request.

   In response to your request, the CA will send you a signed server certificate. Your CA will also send you the root certificate and any intermediate certificates required.
4. If your certificate is delivered in the body of an email message (versus a file), copy the certificate into a file.

   For example: `myserver.mycompany.com.cer`

   You will import the contents of this file into the keystore.

### To import the certificates:

1. To import the root certificate, execute the following command (all on one line):

   ```
   keytool -import -v -noprompt -trustcacerts -alias <rootalias> -file
   <CArootcert> -keystore <storefile> -storepass <password>
   ```

   Here, *`<rootalias>`* is the keystore alias for the root certificate, and *`<CArootcert>`* is the file containing the contents of the root certificate (obtain this from your CA). For example:

   ```
   keytool -import -v -noprompt -trustcacerts -alias myrootcert -file CA-root-
   cert.cer -keystore /opt/datapalette/.keystore -storepass mypassword
   ```
2. If your CA provides an intermediate certificate in a separate file, import that certificate as well. Be sure to specify a unique alias and the correct file name for the intermediate certificate.
3. To import your signed server certificate, execute the following command (all on one line):

   ```
   keytool -import -v -noprompt -alias <keyalias> -file <my-cert> -keystore
   <storefile> -storepass <password>
   ```

   Here, *`<my-cert>`* is the file that contains your signed certificate. For example:

   ```
   keytool -import -v -noprompt -alias myserver -file myserver.mycompany.com.cer
   -keypass mypassword -keystore /opt/datapalette/.keystore -storepass
   mypassword
   ```
4. Run the following command to verify the contents of your keystore (all on one line):

   ```
   keytool -list -keystore <storeFile> -storepass <password>
   ```

   For example:

   ```
   keytool -list -keystore /opt/datapalette/.keystore -storepass mypassword
   ```

   You should see the following type of output:

```
Keystore type: JKS
Keystore provider: SUN

Your keystore contains 2 entries

myrootcert, Aug 15, 2011, trustedCertEntry,
Certificate fingerprint (MD5): B5:95:C3:7C:61:A2:60:48:43:84:D5:70:29:F1:AC:E9
myserver, Aug 15, 2011, PrivateKeyEntry,
Certificate fingerprint (MD5): A4:E5:D7:3D:10:12:11:C2:F8:8B:29:E4:9B:97:21:07
```

In this example, only the root certificate was used – there was no intermediate certificate. If a single intermediate certificate is used, your keystore will contain three entries.

TIP: To view more detailed information, you can use the `-v` option with this command:

```
keytool -list -v -keystore <storeFile> -storepass <password>
```

## Configure the HP DMA Server to Use Your Certificate

After you add your server certificate to the keystore, you must add a `<Connector>` element to the `server.xml` file for the HP DMA Web Server.

### To add a <Connector> element to the server.xml file:

1. Determine which OS user (datapal or root) is running the Nerve Center:

   ```
   ps -ef | grep datapal
   ```

2. As that OS user (datapal or root), stop the Nerve Center using the following command:

   ```
   <installDir>/bin/datapal -sr
   ```

   Here, *`<installDir>`* is the location where HP DMA is installed (`/opt/datapalette` by default). For example:

   ```
   /opt/datapalette/bin/datapal -sr
   ```

2. Open the following file in a text editor:

   ```
   /opt/datapalette/web/tomcat/conf/server.xml
   ```

3. Remove the comment delimiters (`<!--` and `-->`) around the SSL Connector element, and specify the following attributes:

   ```
   <Connector port="<SSLport>" protocol="HTTP/1.1" SSLEnabled="true"
        scheme="https" secure="true" sslProtocol="TLS"
        keystoreFile="<storefile>"
        keyAlias="<serveralias>" keystorePass="<password>"
        connectionTimeout="25000"
        keepAliveTimeout="25000"
        maxKeepAliveRequests="-1"
        maxThreads="150"
        compression="1024"
        compressableMimeType="text/html,text/xml,text/plain,text/css,text/javascript"/>
   ```

   The placeholders used here represent the following information:

   *`<serveralias>`* Unique alias for the server's private key (see Generate a Private Key for the Server on page 8).

   *`<SSLport>`* Port that will be used for SSL communication between the HP DMA

Nerve Center/Web Server and the HP DMA agents.

`<storefile>` Keystore file name. For example: `/opt/datapalette/.keystore`

`<password>` The password for both this keystore and the server's private key.

For example:

```
<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true"
     scheme="https" secure="true" sslProtocol="TLS"
     keystoreFile="/opt/datapalette/.keystore"
     keyAlias="myserver" keystorePass="mypassword"
     connectionTimeout="25000"
     keepAliveTimeout="25000"
     maxKeepAliveRequests="-1"
     maxThreads="150"
     compression="1024"
     compressableMimeType="text/html,text/xml,text/plain,text/css,text/javascript"/>
```

If you used the `datapal` script to generate a self-signed certificate in a test environment, `keyAlias` will be `"stratavia,"` and `"keystoreFile"` will be `"/opt/datapalette/.keystore"` (see Using a Self-Signed Server Certificate on page 17). Do not use a self-signed certificate in a production environment.

Comment out the non-SSL Connector element by adding `<!--` before and `-->` after the element, as shown here :

```
<!--
<Connector port="80" protocol="org.apache.coyote.http11.Http11NioProtocol"
     acceptorThreadCount="2"
     connectionTimeout="25000"
     keepAliveTimeout="25000"
     maxKeepAliveRequests="-1"
     maxThreads="250"
     redirectPort="443"
     compression="1024"
     compressableMimeType="text/html,text/xml,text/plain,text/css,text/javascript"/>
-->
```

4 Save the `server.xml` file.

5 As root, start the Nerve Center by using the following command:

```
<installDir>/bin/datapal -r
```

# 3 Configuring SSL on the Agent Servers

There are two methods that you can use to configure SSL on the agent (target) servers:

- Follow the instructions provided below to manually copy a certificate to each agent server and import the certificate into the keystore.
- Use a workflow provided by HP Software Support.

  To obtain this workflow, open a support case, and Support will email you the workflow. This workflow can be used only when the agent is already installed, is configured to use a non-SSL Port, and is communicating with the HP DMA Web Server.

Before configuring SSL on the agent servers, follow the instructions for Configuring SSL on the HP DMA Server on page 8.

## Install the Certificate to the Agent Servers

The first step in configuring SSL on the agent servers is to copy the certificate that you obtained from your certificate authority (or generated yourself by using the `datapal` script, as per the instructions in Appendix A: Using a Self-Signed Server Certificate on page 17) to each agent server and import it into the keystore there.

### To copy the certificate file to an agent server:

1. Copy the certificate file (for example: `myserver.mydomain.com.cer`) from the server hosting the HP DMA Nerve Center/Web Server to the `/tmp` directory on the agent server.
2. On the agent server, change the permissions on the `cacerts` file:

   ```
   chmod u+w /opt/datapalette/java/lib/security/cacerts
   ```

3. Import the server certificate into the keystore by using the following command (all on one line):

   ```
   keytool -import -alias <keyalias> -keystore
   /opt/datapalette/java/lib/security/cacerts -trustcacerts -file
   /tmp/<DMAserver>.cer -storepass <agentstorepwd> -noprompt
   ```

   Here, *`<DMAserver>`* is the fully qualified host name of the server hosting the HP DMA Nerve Center/Web Server, *`<keyalias>`* is the alias that you specified when you generated the private key for that server (see Generate a Private Key for the Server on page 8), and *`<agentstorepwd>`* is the password for the `cacaerts` keystore on the agent server.

   For example:

   ```
   keytool -import -alias myserver -keystore
   /opt/datapalette/java/lib/security/cacerts -trustcacerts -file
   /tmp/myserver.mycompany.com.cer -storepass changeit -noprompt
   ```

   The certificate will be appended to any existing certificates in the keystore.

➤ By default, the keystore password is `changeit`. You can change this password by using the `keytool -storepasswd` command. For more information, see: *http://download.oracle.com/javase/1,5.0/docs/tooldocs/windows/keytool.html*

# Modify the startup.properties File

After you copy the certificate to the agent server and import it into the keystore, you must modify the `startup.properties` file on that server to use SSL.

### To modify the startup.properties file:

1. On the agent server, open the following file in a text editor:

   ```
   /opt/datapalette/collect/conf/startup.properties
   ```

2. Locate the following lines (assuming that the Web Server is running on port 8080):

   ```
   expertEngineHost=<webServer>
   port=8080
   ssl=false
   ```

   Here, *<webServer>* is the host name of the server hosting the HP DMA Nerve Center/Web Server.

3. Modify this information to use the SSL port specified in the `<Connector>` element in the `server.xml` file on the server hosting the HP DMA Nerve Center/Web Server (see page 11):

   ```
   expertEngineHost=<DMAserver>
   port=<SSLPort>
   ssl=true
   ```

   Here, *<DMAserver>* is the fully qualified host name of the server hosting the HP DMA Nerve Center/Web Server, and *<SSLPort>* is the port that will be used for SSL communication between the HP DMA Nerve Center/Web Server and the HP DMA agent.

   For example:

   ```
   expertEngineHost=myserver.mycompany.com
   port=443
   ssl=true
   ```

# Stop and Start the HP DMA Agent

After you modify the `startup.properties` file, you must restart the HP DMA agent so that your changes can take effect.

### To stop and start the agent:

1. Stop the agent by using the following command:

   ```
   <installDir>/bin/datapal -sc
   ```

   Here, *<installDir>* is the location where HP DMA is installed (`/opt/datapalette` by default). For example:

   ```
   /opt/datapalette/bin/datapal -sc
   ```

2. Make sure that the agent process is not running:

   ```
   ps -ef | grep datapal
   ```

3. Start the agent again:

   ```
   <installDir>/bin/datapal -c
   ```

# 4 Verifying the SSL Connection

By examining entries in the `collector.log` file, you can confirm that the HP DMA server is communicating with a specific agent (target) server using SSL.

### To verify the SSL connection:

1 On the HP DMA server, tail the following log file (or examine it in a text editor):

```
tail <installDir>/collect/log/collector.log
```

Here, *<installDir>* is the directory where HP DMA is installed. For example:

```
tail /opt/datapalette/collect/log/collector.log
```

2 Look for the following types of entries:

```
PUT https://<DMAserver>/api/agent/stats/dns/<agentHost>/ip/<agentIP> 200 OK
2011-09-06 12:57:35,260 DEBUG [CommandChecker] AgentApi.logRequest:276
GET https://<DMAserver>/api/agent/commands/dns/<agentHost>/ip/<agentIP> 200 OK
2011-09-06 12:57:55,277 DEBUG [CommandChecker] AgentApi.logRequest:276
PUT https://<DMAserver>/api/agent/stats/dns/<agentHost>/ip/<agentIP> 200 OK
2011-09-06 12:57:55,290 DEBUG [CommandChecker] AgentApi.logRequest:276
GET https://<DMAserver>/api/agent/commands/dns/<agentHost>/ip/<agentIP> 200 OK
```

In this case, the placeholders represent the following information:

*<DMAserver>* Host name of the HP DMA server.

*<agentHost>* Host name of the agent (target) server for this operation.

*<agentIP>* IP address of the agent (target) server.

HTTPS protocol indicates that the HP DMA server is communicating with the agent (target) server using SSL.

# 5 Deleting a Certificate

You may find it necessary at some point to delete a certificate from the keystore – for example, if the certificate expires or is revoked by the Certificate Authority (CA).

A certificate should be revoked under any of the following circumstances:

- The private key is lost.
- The private key is compromised.
- The certificate contains incorrect or outdated information.

A revoked certificate immediately becomes invalid. It cannot be renewed, re-keyed, or reissued.

If your HP DMA server certificate expires, is revoked, or otherwise becomes invalid, you must remove it from the keystore and replace it with a valid certificate.

You can delete a certificate from the HP DMA server keystore by using the `keytool` utility.

### To delete the server certificate from the HP DMA server keystore:

1 Log in to the HP DMA server as the datapal user.

2 Execute the following command (all on one line):

```
keytool -delete -alias <keyalias> -keystore <storeFile> -keypass <password>
```

Here, *<keyalias>* is the alias associated with the HP DMA server's private key, *<storeFile>* is the file that contains the keystore, and *<password>* is the keystore password.

For example:

```
keytool -delete -alias myserver -keystore /opt/datapalette/.keystore -
storepass mypassword
```

3 Repeat step 2 for each agent (target) server where this certificate was installed (see Configuring SSL on the Agent Servers on page 13). In this case, specify the agent server keystore file and password. For example:

```
keytool -delete -alias myserver -keystore
/opt/datapalette/java/lib/security/cacerts -storepass changeit
```

4 Install a valid server certificate on the HP DMA server and all agent servers.

# A Using a Self-Signed Server Certificate

Depending on your security policy, you may be permitted to use a self-signed certificate for development and testing purposes in a lab environment.

The `datapal` script provided with HP DMA enables you to generate a self-signed certificate, store it in your keystore, and export it into a file.

Do not use a self-signed server certificate in a production environment. Always use a certificate signed by a trusted certificate authority (see page 8).

### To generate a self-signed certificate using the `datapal` script:

1 Log in to the server hosting HP DMA Nerve Center/Web Server as the datapal user.

2 Execute the following command to generate the certificate:

```
/opt/datapalette/bin/datapal -t CertificateGen <password> <DMAserver>
```

Here, *`<DMAserver>`* represents the fully qualified host name of the server hosting the HP DMA Nerve Center/Web Server, and *`<password>`* represents the keystore password.

For example:

```
/opt/datapalette/bin/datapal -t CertificateGen mypassword myserver.mydomain.com
```

Note that the *`<DMAserver>`* must match the host name in the URL that HP DMA users will use to access the HP DMA Web Server in their web browsers.

3 Export the self-signed certificate from the keystore to a file:

```
keytool -exportcert -alias stratavia -file <DMAserver>.cer
```

This will enable you to copy the certificate to the agent servers (see Configuring SSL on the Agent Servers on page 13).

For example:

```
keytool -exportcert -alias stratavia -file myserver.mycompany.com.cer
```

To proceed, see Configure the HP DMA Server to Use Your Certificate on page 11.