Technical white paper

Update Self-Signed SSL Certificate in HP DMA

HP Database and Middleware Automation version 10.2x

This technical white paper is intended for HP DMA users who need to know how to generate and use a new Self-Signed SSL Certificate in HP DMA.

Update Self-Signed SSL Certificate

This paper provides information on how to generate a new Self-Signed SSL Certificate and to automate the distribution of your certificate to your managed servers. This information is particularly helpful when you need to update your certificate when it expires. This paper includes:

Update Self-Signed SSL Certificate on the HP DMA Server

Perform these steps to update the Self-Signed SSL Certificate on the HP DMA Server:

1. Stop HP DMA:

   ```
   # service dma stop
   ```

2. To list the certificates, execute the following command (all on one line—key in to avoid unwanted cut-and-paste characters):

   ```
   # /opt/hp/dma/server/jre/bin/keytool -list -keystore <keystore location>
   ```

   For example (with the default HP DMA keystore location):

   ```
   # /opt/hp/dma/server/jre/bin/keytool -list -keystore
   /opt/hp/dma/server/.keystore
   ```

   Specify the keystore password (the default is `changeit`).

   The results will be similar to this:

   ```
   [root@IWFVM01939 bin]# keytool -list -keystore /opt/hp/dma/server/.keysto
   re
   Enter keystore password:

   Keystore type: JKS
   Keystore provider: SUN

   Your keystore contains 1 entry

   tomcat, Oct 31, 2014, PrivateKeyEntry,
   ```

```
Certificate fingerprint (MD5): 99:35:B5:68:08:18:85:DB:51:96:FA:A4:41:A2:
F3:AB
[root@IWFVM01939 bin:#
```

3. To delete the existing certificate, execute the following command (all on one line):

   ```
   # /opt/hp/dma/server/jre/bin/keytool -delete -keystore <keystore location>
   -alias tomcat
   ```

   For example (with the default HP DMA keystore location):

   ```
   # /opt/hp/dma/server/jre/bin/keytool -delete -keystore
   /opt/hp/dma/server/.keystore -alias tomcat
   ```

   Specify the keystore password (the default is `changeit`).

   The results will be similar to this:

   ```
   [root@IWFVM01939 bin]# keytool -list -delete -keystore /opt/hp/dma/server
   /.keystore -alias tomcat
   Enter keystore password:


   [root@IWFVM01939 bin:#
   ```

4. To verify that there are now no certificates, execute the following command (all on one line):

   ```
   # /opt/hp/dma/server/jre/bin/keytool -list -keystore <keystore location>
   ```

   For example (with the default HP DMA keystore location):

   ```
   # /opt/hp/dma/server/jre/bin/keytool -list -keystore
   /opt/hp/dma/server/.keystore
   ```

   Specify the keystore password (the default is `changeit`).

   The results will be similar to this:

   ```
   [root@IWFVM01939 bin]# keytool -list -keystore /opt/hp/dma/server/.keysto
   re
   Enter keystore password:

   Keystore type: JKS
   Keystore provider: SUN
   ```

```
Your keystore contains 0 entries

[root@IWFVM01939 bin:#
```

5. To generate the new Self-Signed SSL Certificate, execute the following command (all on one line):

```
# /opt/hp/dma/server/jre/bin/keytool -genkeypair -validity <numberdays>
-keyalg RSA -dname "CN=<DMAserver>,OU=<orgunit>,O=<org>,L=<location>,
S=<state>,C=<country>" -alias <keyalias> -storepass <password>
-keypass <password> -keystore <storefile>
```

Caution: If you are using an SA gateway infrastructure as a proxy network, append `-ext SAN=ip:xx.xx.xxx.xxx` to the `keytool` command, replacing `xx.xx.xxx.xxx` with the desired IP address. For additional information, see "Use a Proxy Server with HP DMA" in the *HP DMA Installation Guide*.

The variables used here refer to the following information:

Variable	Description
<numberdays>	The number of days that the key will be valid.
<DMAserver>	Fully qualified host name of the server hosting the HP DMA 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.
<keyalias>	Unique alias for the server's private key. This will be used to associate the server certificate with its private key. The default is `tomcat`.
<password>	The password for both the keystore and this private key.
<storefile>	Keystore file name. For example: /opt/hp/dma/server/.mykeystore

For example:

```
# /opt/hp/dma/server/jre/bin/keytool -genkeypair -validity 365 -keyalg RSA
-dname "CN=someserver.domain.com, OU=DMA, O=My Company Name,
L=Fort Collins, ST=CO, C=US" -alias tomcat -storepass changeit -keypass
changeit -keystore  /opt/hp/dma/server/.keystore
```

Note: You must use the same password for the –keypass and –storepass settings.

6. To list the keystore contents to verify that the new certificate is available, execute the following command (all on one line):

   ```
   # /opt/hp/dma/server/jre/bin/keytool -list -keystore <keystore location>
   ```

   For example (with the default HP DMA keystore location):

   ```
   # /opt/hp/dma/server/jre/bin/keytool -list -keystore
   /opt/hp/dma/server/.keystore
   ```

   Specify the keystore password (the default is `changeit`).

   The results will be similar to this:

   ```
   [root@IWFVM05191 bin]# keytool -list -keystore /opt/hp/dma/server/.keysto
   re
   Enter keystore password:

   Keystore type: JKS
   Keystore provider: SUN

   Your keystore contains 1 entry

   tomcat, Nov 3, 2014, PrivateKeyEntry,
   Certificate fingerprint (SHA1): 0A:B5:E8:21:DC:38:A1:C4:6A:15:BD:09:3D:BC
   :90:50:7F:D0:86:32
   [root@IWFVM05191 bin:#
   ```

7. Start HP DMA:

   ```
   # service dma start
   ```

8. Using the browser, log in to HP DMA, as usual.

Update Self-Signed SSL Certificate on the HP DMA Client

The steps to update the Self-Signed SSL Certificate on the HP DMA Client differ depending on whether or not HP DMA is set up to trust all certificates.

To determine whether your HP DMA Server trusts all certificates:

1. Open the `dma.xml` file—located here on the HP DMA server:

   `/opt/hp/dma/server/tomcat/conf/Catalina/localhost/dma.xml`

   > **Note:** You do not need to stop and restart the HP DMA Server unless you change the value of `trustAllCertificates` in the file.

2. Search for `trustAllCertificates`:

   `<Parameter name="com.hp.dma.conn.trustAllCertificates" value="<value>" />`

3. Follow the appropriate instructions based on <*value*>:

Value of trustAllCertificates	Instructions
true	When trusting all certificates
false	When not trusting all certificates

When trusting all certificates

The HP DMA Clients can be set to trust any certificate coming from the HP DMA Server. This is the default setting.

> When trusting all SSL Certificates, there is no need to import the certificates to the HP DMA Client. Updating the SSL Certificate on the HP DMA Server is enough for the Clients to work. No changes are required on the HP DMA Clients.

When not trusting all certificates

The HP DMA Clients can be set NOT to trust all certificates coming from the HP DMA Server. When this is the case, the certificate sent from the HP DMA Server to the HP DMA Client needs to be validated against the certificates that are trusted.

To enable HP DMA to use a Self-Signed SSL Certificate for WEST to communicate with the HP DMA Server, the certificate needs to be added to the client as a trusted certificate. To do this for all clients, create an SA policy following the instructions in Add the certificate to Unix targets and Add the certificate to Windows targets.

Add the certificate to Unix targets

Add the certificate to the Unix targets **after** the new certificate is applied to the HP DMA Server (see Update Self-Signed SSL Certificate on the HP DMA Server).

1. Open a browser and export this certificate to <*download location*>. The steps required depends on your browser.

   Example for the Firefox browser:

   - Go to **Open menu** ( ) → **Options** → **Certificates** (tab) → **View Certificates**→ **Servers** (tab)
   - Scroll down to <*company_name*> and <*dma_server_name*>
   - Click **Export**
   - Save the certificate to <*download location*> with file extension CRT.

2. Zip up the certificate file into a file named `cert_file_unix.zip`.
3. Launch the HP SA Client from the Windows Start Menu.

   By default, the HP SA Client is located in Start → All Programs → HP Business Service Automation → HP Server Automation Client

   Note: For additional information, see About the SA Client. If the HP SA Client is not installed locally, follow the instructions under "Installing the SA Client Launcher" in the *User Guide: Server Automation*, available on the HP Software Support web site: https://softwaresupport.hp.com/

4. Upload the ZIP file as a package to SA:

   a. In the navigation pane in the HP SA Client, select **Library** → **By Folder**.

   b. Select (or create) the folder where you want to store the file.

   c. From the Actions menu, select **Import Software** and then browse to the certificate ZIP file.

d. Click **Import**.

e. Click **Close** after the import is completed.

5. Create a new software policy that is applicable to Unix:

a. Right-click on the certificate that you just uploaded, and then select **New** → **Software Policy**.

b. Add `cert_file_unix.zip` as the package.

c. Select Unix as the applicable OS for the ZIP file.

d. Specify `/opt/hp/dma/client/java_certs` as the default install path.

e. Under Install Scripts for the package, add the following lines as Post-Install Scripts (all on single lines):

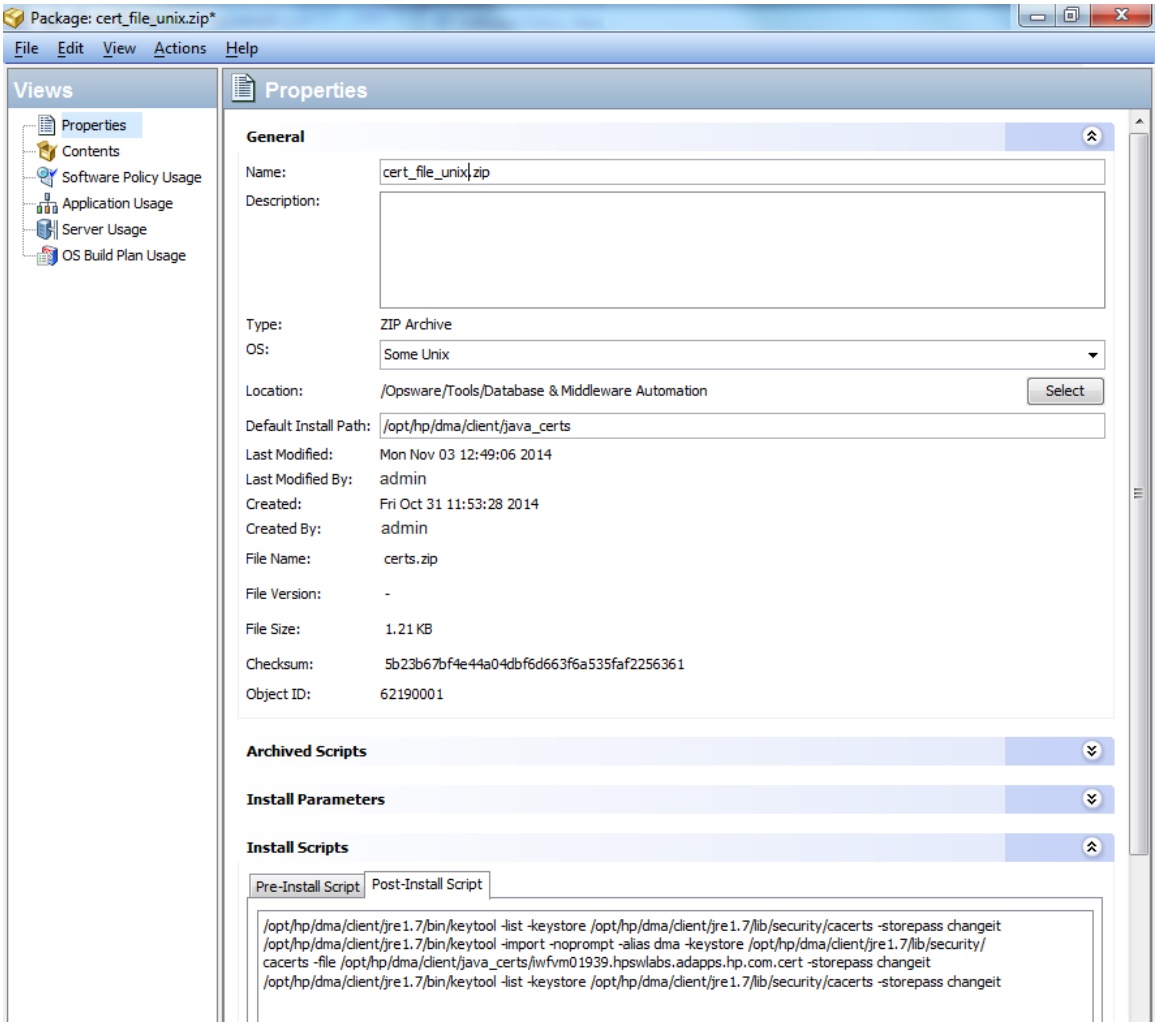
```
/opt/hp/dma/client/jre1.7/bin/keytool -list -keystore /opt/hp/dma/client/
jre1.7/lib/security/cacerts -storepass <password>
```

```
/opt/hp/dma/client/jre1.7/bin/keytool -import -noprompt -alias dma
-keystore /opt/hp/dma/client/jre1.7/lib/security/cacerts -file /opt/hp/
dma/client/java_certs/<certificate file name> -storepass <password>
```

```
/opt/hp/dma/client/jre1.7/bin/keytool -list -keystore /opt/hp/dma/client/
jre1.7/lib/security/cacerts -storepass <password>
```

Note: Here, <*certificate file name*> is the name of the certificate file inside the ZIP file and not the ZIP file itself and <*password*> is the appropriate password (the default is `changeit`).

For example:



6. Apply this software policy on the Unix devices.
7. Verify that this job has no failures. The post install message should say: Certificate was added to keystore.
8. Run the HP DMA workflows as usual.

Add the certificate to Windows targets

Add the certificate to the Windows targets **after** the new certificate is applied to the HP DMA Server (see Update Self-Signed SSL Certificate on the HP DMA Server).

1. Open a browser and export this certificate to <*download location*>. The steps required depends on your browser.

   Example for the Firefox browser:

   - Go to **Open menu** () → **Options** → **Certificates** (tab) → **View Certificates**→ **Servers** (tab)
   - Scroll down to <*company_name*> and <*dma_server_name*>
   - Click **Export**
   - Save the certificate to <*download location*> with file extension CRT.

2. Zip up the certificate file into a file named `cert_file_win.zip`.
3. Launch the HP SA Client from the Windows Start Menu.

   By default, the HP SA Client is located in Start → All Programs → HP Business Service Automation → HP Server Automation Client

   Note: For additional information, see About the SA Client. If the HP SA Client is not installed locally, follow the instructions under "Installing the SA Client Launcher" in the *User Guide: Server Automation*, available on the HP Software Support web site: https://softwaresupport.hp.com/

4. Upload the ZIP file as a package to SA:
   a. In the navigation pane in the HP SA Client, select **Library** → **By Folder**.
   b. Select (or create) the folder where you want to store the file.
   c. From the Actions menu, select **Import Software** and then browse to the certificate ZIP file.
   d. Click **Import**.
   e. Click **Close** after the import is completed.
5. Create a new software policy that is applicable to Windows:
   a. Right-click on the certificate that you just uploaded, and then select **New** → **Software Policy**.
   b. Add `cert_file_win.zip` as the package.

c. Select Windows as the applicable OS for the ZIP file.

d. Specify `%SystemDrive%\Program Files\HP\DMA\Client\java_certs` as the default install path.

e. Under Install Scripts for the package, add the following lines as Post-Install Scripts (all on single lines):

```
cd "%SystemDrive%\Program Files\HP\DMA\Client\jre1_7\bin"
```

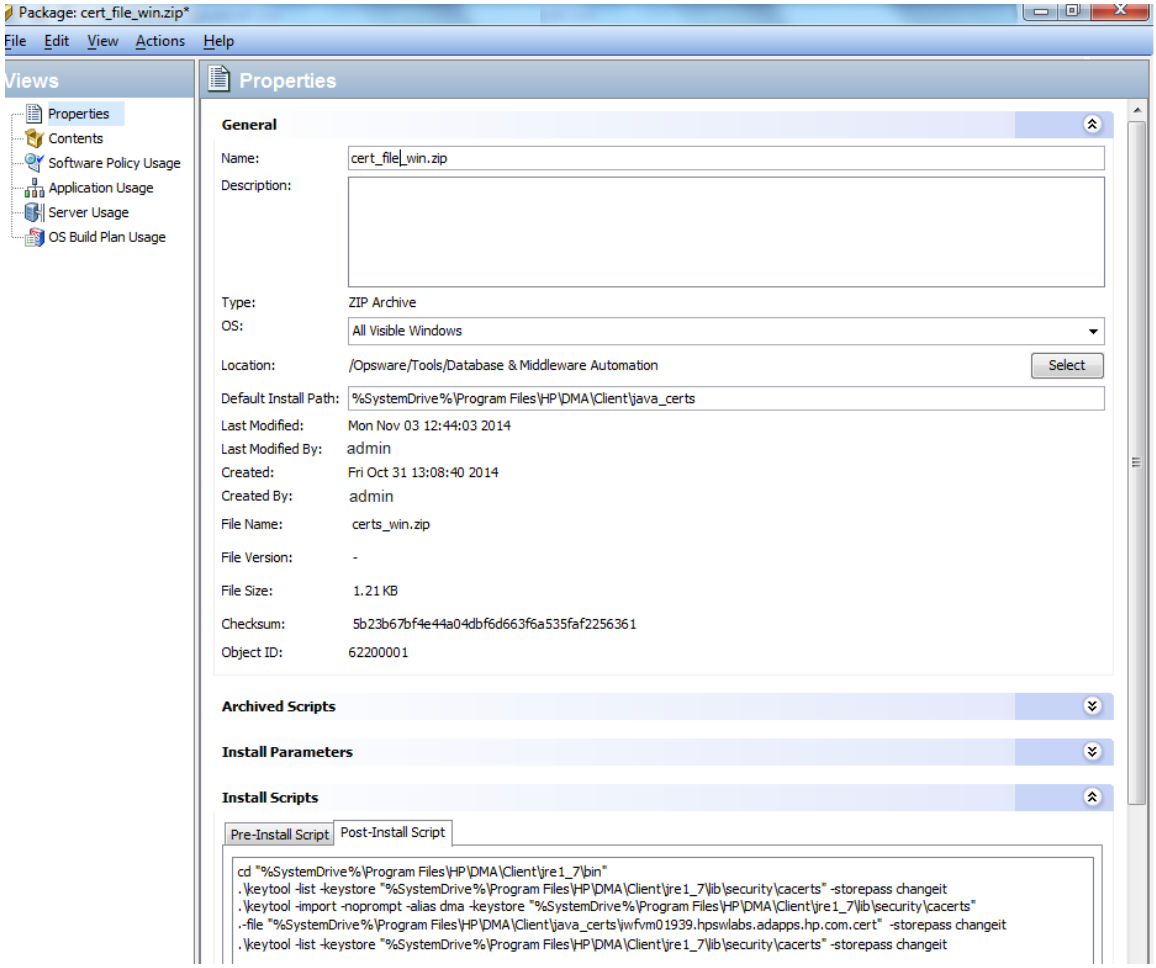
```
.\keytool -list -keystore "%SystemDrive%\Program Files\HP\DMA\Client\jre1_7\lib\security\cacerts" -storepass <password>
```

```
.\keytool -import -noprompt -alias tomcat -keystore "%SystemDrive%\Program Files\HP\DMA\Client\jre1_7\lib\security\cacerts" -file "%SystemDrive%\Program Files\HP\DMA\Client\java_certs\<certificate file name>"  -storepass <password>
```

```
.\keytool -list -keystore "%SystemDrive%\Program Files\HP\DMA\Client\jre1_7\lib\security\cacerts" -storepass <password>
```

Note: Here, *<certificate file name>* is the name of the certificate file inside the ZIP file and not the ZIP file itself and *<password>* is the appropriate password (the default is `changeit`).

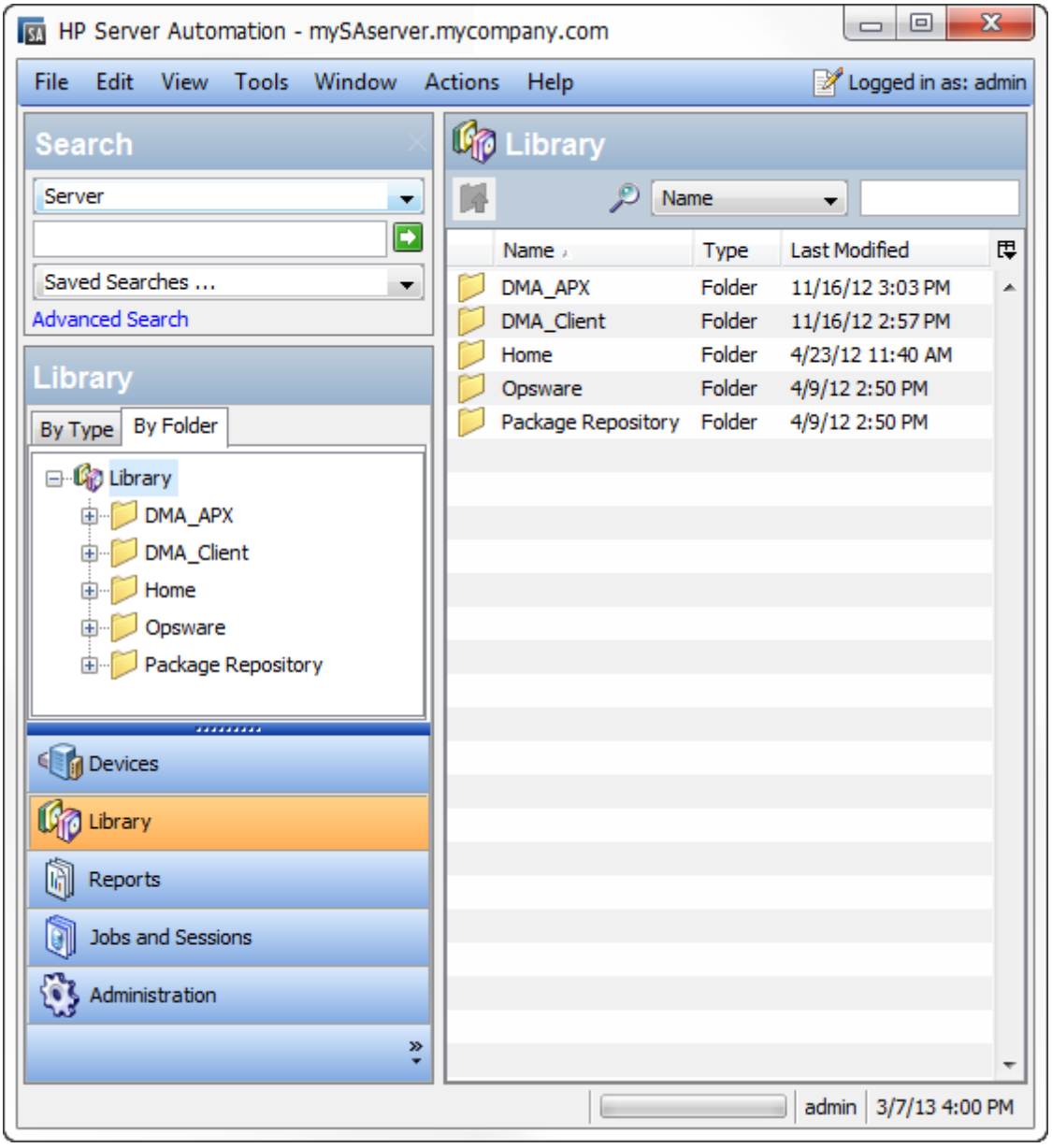
For example:



6. Apply this software policy on the Windows devices.
7. Verify that this job has no failures. The post install message should say: Certificate was added to keystore.
8. Run the HP DMA workflows as usual.

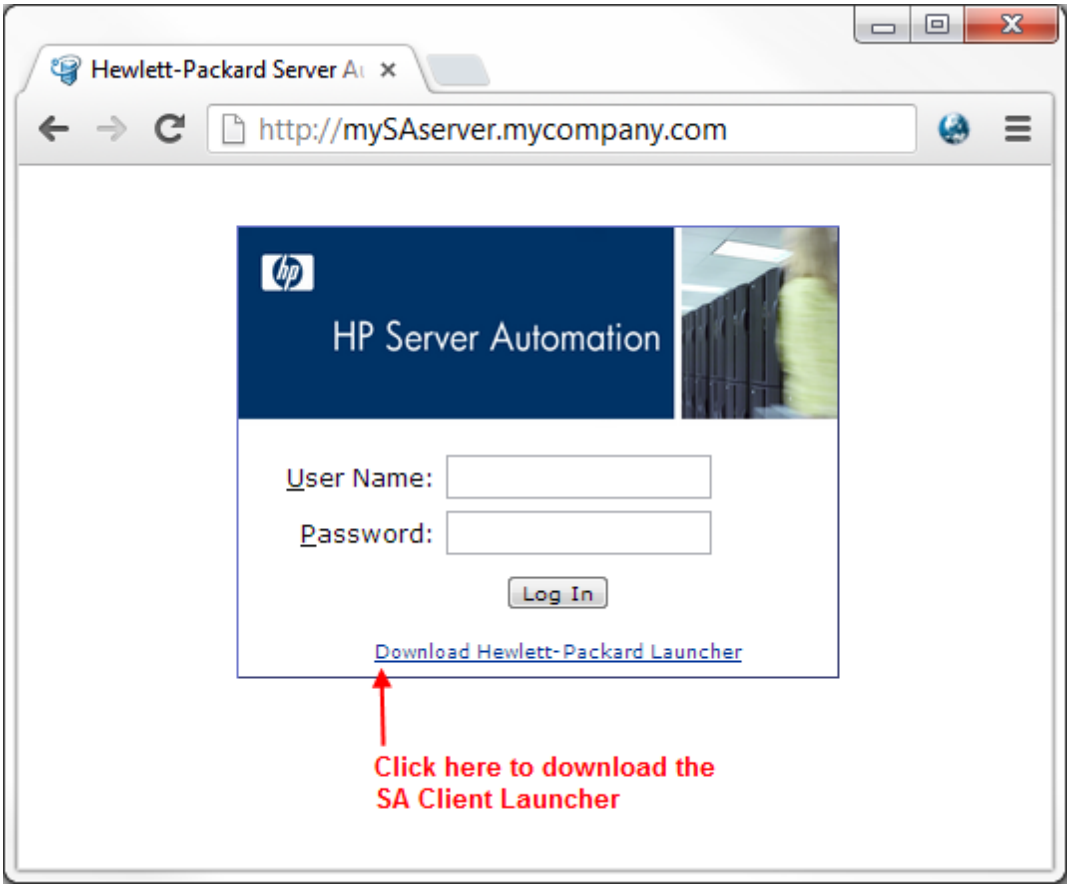
About the SA Client

The SA Client is a powerful Java client for the HP Server Automation System. It provides the look-and-feel of a Microsoft Windows desktop application with the cross-platform flexibility of Java.



If you installed your SA Core on multiple servers, you can access the SA Client from any Core Server hosting a Component Slice bundle.

To access the SA Client for the first time, you must invoke the SA Client Launcher from the SA Web Client Main Page:



Clicking on this link will install the SA Client and the required Java Runtime Environment (JRE) on your local machine. Once it is installed, you can invoke the SA Client from the local machine rather than from the SA Web Client.

Note: The SA Client is a Java application that installs and runs with its own Java Runtime Environment (JRE). The SA Client will not interfere with any other versions of JRE you may have installed on your system. The JDK will not be used (and is not usable) by any other Java application on the target computer, and it will not set itself as the default JDK on the target computer.

For more information about the SA Client, see the HP Server Automation documentation library available on the HP Software Support web site:

https://softwaresupport.hp.com/