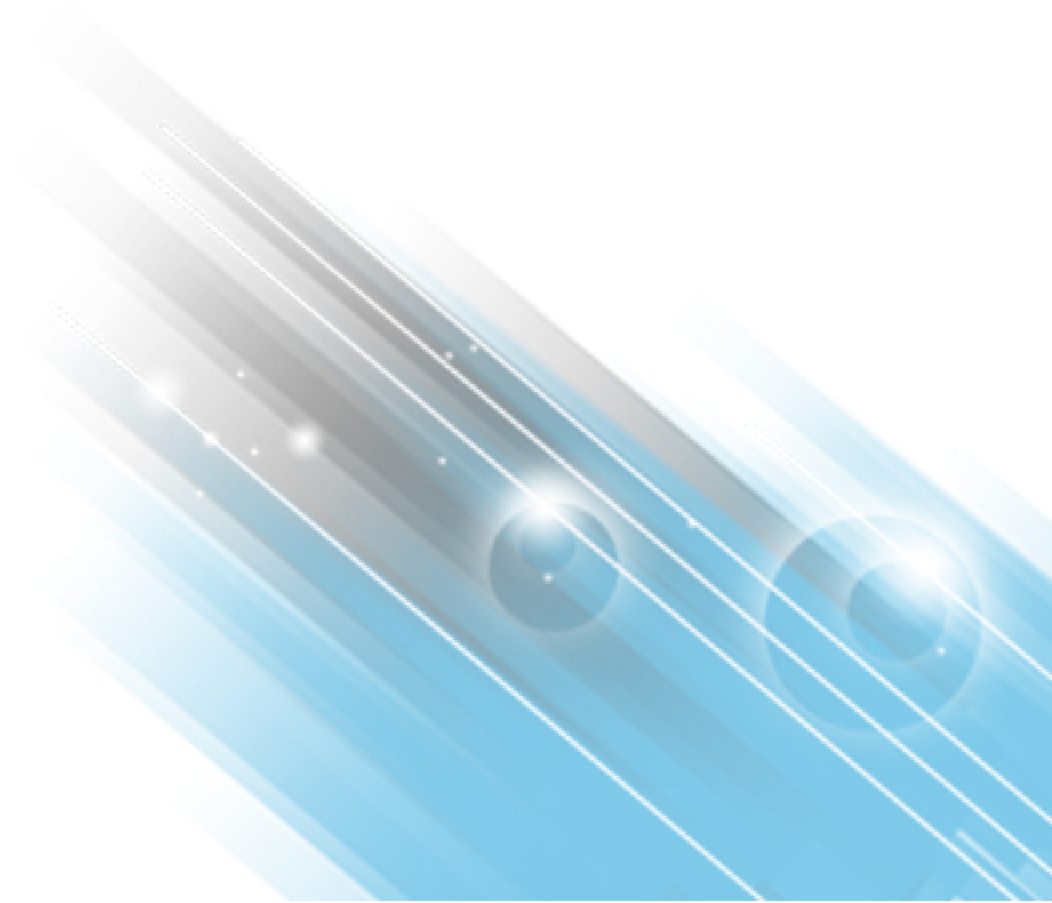
HP Database and Middleware Automation

Software Version: 10.30.000.000
Red Hat Enterprise Linux and SUSE Enterprise Linux

Troubleshooting Guide



Document Release Date: May 2015
Software Release Date: May 2015

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 Notice

Trademark Notices

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Java® and Oracle® are registered trademarks of Oracle and/or its affiliates.

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: **https://softwaresupport.hp.com**

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: **https://hpp12.passport.hp.com/hppcf/createuser.do**

Or click the **Register** link at the top of the HP Software Support 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.

The following table indicates changes made to this document since the last released major edition.

Document Changes

Chapter	Version	Changes
Title Page Legal Notices	10.20	Updated version number, software release date, document release date, and copyright date range. Added SUSE platform.

Document Changes, continued

Chapter	Version	Changes
Specify a Renamed Windows Administrator User HP Software Documentation	10.20	Added instructions to use the HP Live Network connector to update westAPX with the additional Update WestAPX for Windows User.
Common Baseline Errors	10.20	The TNS listener needs to be started after database creation. If the TNS listener is not running, an error in the Oracle Server or Oracle SID Name will occur.
DMA Client Files Policy Error	10.20	Added troubleshooting information if the `/DMA_Client` directory does not exist or is not writable.
Troubleshooting	10.20	Added information about turning on debug.
Troubleshooting	10.20.100	Added troubleshooting information for login errors: Oracle database password changed The HP DMA database is not accessible
Special Configurations Troubleshooting	10.20.100	Reduced instructions for advanced DMA users to create and configure Custom Fields.
Use a Proxy Server with HP DMA	10.20.100	Reorganized section.
Run as a Windows Domain User	10.20.100	Added new capability to configure a Windows domain user using runtime parameters.
Title Page Legal Notices Entire guide	10.21	Updated version number, software release date, document release date, and copyright date range. Updated document template. Updated screen shots.
Troubleshooting	10.21	Added new section Run Time Errors to describe Workflow Aborts Using an Internal SSL Certificate.
Troubleshooting	10.21	Added a new troubleshooting section "The SA Core was Updated" under Login Errors.
Troubleshooting	10.21	Added new "HP DMA is Switched to Different SA Core" section to Login Errors. Added new "Reset the HP DMA Initial Admin Password" section to Reset the HP DMA Initial Admin password.
Performance Issues	10.21	Added new Troubleshooting information for performance issues.
Title Page Legal Notices	10.22	Updated version number, software release date, document release date, and copyright date range.
Use a Proxy Server with HP DMA	10.22	Provided an example of how to use `keytool` to set up SAN.

Document Changes, continued

Chapter	Version	Changes
Change the Default Port and Security Level	10.22	Added additional information about changing the security level—port and protocol.
Troubleshooting	10.22	Added new troubleshooting information: The HP DMA Login Page Does Not Work with Internet Explorer Workflow Aborts After an HP DMA Upgrade Workflows "Stuck" in Perpetual Running State Deployments Are Skipped if Another Deployment of Same Workflow Is Running Update Self-Signed SSL Certificate
Title Page Legal Notices Entire guide	10.30	Updated version number, software release date, document release date, and copyright date range. Updated to new documentation template.
Installation Media Contents Import an HP DMA Solution Pack	10.30	Updated instructions for accessing patches, solution packs, and documentation on HPSoftware Support.
Supported Products and Platforms	10.30	PostgreSQL 9.3.5

Support

Visit the HP Software Support Online web site at: **https://softwaresupport.hp.com**

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 ID, go to:

https://hpp12.passport.hp.com/hppcf/createuser.do

To find more information about access levels, go to:

https://softwaresupport.hp.com/web/softwaresupport/access-levels

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contents

Introduction

This guide provides information that will help you troubleshoot problems that can arise during the installation and initial configuration of HP Database and Middleware Automation (HP DMA) version 10.30.

This guide also provides information about various Special Configurations that may be pertinent to your environment.

Audience

This guide is intended for HP DMA administrators who are responsible for installing or upgrading HP DMA.

Related Documents

This document refers to the *HP DMA Installation Guide*.

The following HP Server Automation (SA) documents may also be helpful:

- *HP SA Administration Guide*
- *HP SA Overview and Architecture Guide*
- *HP SA Single-Host Installation Guide*
- *HP SA Simple/Advanced Installation Guide*

All HP DMA and SA documentation is available on the HP Software Support web site (see HP Software Documentation on page 81).

Chapter 1: Troubleshooting

This guide provides information that will help you troubleshoot problems that can arise during the installation and initial configuration of HP Database and Middleware Automation (HP DMA) version 10.30.

Debugging Tools

HP DMA provides Custom Fields that can assist you in the debug process by providing additional output information:

- `DEBUG_LEVEL`: Controls the level of workflow output to the HP DMA Console Page. The following describes the values:

0	No debug
1	Error debug
2	Warning debug
3	Success, information, and notice debug
4	Debug debug
5	Verbose debug
99	Maximum debug

- `west_verbose`: Determines whether additional debug logging is written to the HP DMA Client log. Valid values are TRUE and FALSE.

This output can be valuable if you need assistance from HP Support.

> **Tip:** See the "Custom Field" section in the *HP DMA Administrator Guide* for additional information on how to create and customize Custom Fields.

To create and configure the debug Custom Fields:

1. Decide whether you want debug at the organization level or the server level.

   > **Note:** You can specify Custom Fields for both organizations and individual servers. If both are specified, the server level information takes precedence over the organization level information.

   > **Note:** To debug what happens on a specific target when a specific workflow runs, create the Custom Fields at the server level.

2. Go to Environment > Custom Fields to create the new Custom Fields at either the Organization or Server level (alternatively, you can add Custom Fields when the organization or server is open in the Environment page):
   - `DEBUG_LEVEL` with type Text
   - `west_verbose` with type List and options TRUE or FALSE
3. Specify the Custom Field values at the organization level, the server level, or both:
   - Go to Environment > Dashboard > <*organization_name*> (*Optional:* > <*server_name*>).
   - Set `DEBUG_LEVEL` to 99—the highest level of debug.
   - Set `west_verbose` to TRUE.

   > **Note:** This must be performed by an HP DMA user who has a role with Write permission for the pertinent organizations (or Administrator capability).

   > **Tip:** If you do not see this Custom Field, be sure that **Show empty values** is selected.

To obtain debug information:

1. Run the pertinent workflow on the server that has the debug Custom Fields turned on.
2. After the workflow completes, the debug information will be available on the Console and History tabs for the workflow.
3. *Optional:* To save the history output as a CSV file, click CSV at the upper-right corner of the history page.

You can relay this information to HP Support for further troubleshooting.

To turn off debug:

When you are done debugging, you can modify the values of the Custom Fields to turn the debug off:

- Go to Environment > Dashboard > <*organization_name*> (*Optional:* > <*server_name*>)
- Set `DEBUG_LEVEL` to 0—no debug.
- Set `west_verbose` to FALSE.

> **Tip:** If you do not see this Custom Field, be sure that **Show empty values** is selected.

Optional: You can also delete the `DEBUG_LEVEL` and `west_verbose` Custom Fields since the default values turn off the debug.

Troubleshooting Issues

Each troubleshooting topic shows you how to diagnose and resolve a particular problem. The topics are grouped according to where in the HP DMA installation process each problem can occur. Pertinent log file snippets are included.

In the following table, the Installation Step column indicates where in the HP DMA installation process each type of problem becomes apparent. The Probable Cause column contains links to topics that show you how to diagnose and resolve a particular problem.

Problem	Installation Step	Probable Cause
Common Baseline Errors	Install the HP DMA Server	Oracle Database User Was Not Created
		Oracle Listener Is Not Running
		Oracle Database Is Not Running
		Error in the Oracle Server or Oracle SID Name
		HP DMA Client Fails to Contact HP DMA Server
		Did Not Run the Baseline Command as Root User
APX Tool Configuration Error	Import the HP DMA APX	Not Pointing to Correct APX Tool Directory
DMA Client Files Policy Error	Install the DMA Client Files Policy	DMA_Client Directory Does Not Exist or Is Not Writable
		Microsoft Patch Database Is Out of Date
Connector Errors	Configure the Connector	The SA Core Server Is Down
		The JAR Files Are Not at the Required Locations
		Connector Errors

Problem	Installation Step	Probable Cause
Login Errors	Start HP DMA	The SA Core Server Is Down
		The SA Group Does Not have Login Access
		HP DMA Started Before SA was Running
		Oracle Database/PostgreSQL Password Changed
		The HP DMA Database is Not Accessible
		The SA Core was Updated
		HP DMA is Switched to Different SA Core
		The HP DMA Login Page Does Not Work with Internet Explorer
No Servers Available to Add to HP DMA	Add Available Targets	The HP DMA Connector User Does Not Have Required Permissions
		The HP DMA Connector User Cannot Find Any Servers
		The Servers Are Already in Another HP DMA Organization
		The HP DMA User Does Not Have Correct Permissions
		The DMA Client Files Policy Is Not Attached and Remediated
Run Time Errors	These errors may show up when you run an HP DMA workflow.	Workflow Aborts Using an Internal SSL Certificate
		Workflow Aborts After an HP DMA Upgrade
		Workflows "Stuck" in Perpetual Running State
		Deployments Are Skipped if Another Deployment of Same Workflow Is Running
Performance Issues	Performance issues may show up when you run HP DMA workflows.	Intermittently Unable to Log In and System Freezes

Problem	Installation Step	Probable Cause
Customization	Use these instructions to customize the HP DMA.	Add New Logo to the HP DMA UI
Maintenance	Use these instructions for normal HP DMA maintenance.	Reset the HP DMA Initial Admin password
		Update Self-Signed SSL Certificate

Common Baseline Errors

Most errors that occur when running the `dmaBaselineData` command can be attributed to:

- Not setting up Oracle Database as specified in "Create and Configure the Oracle Database" in the *HP DMA Installation Guide*.
- The TNS listener is not running.
- Not specifying the correct values in the `dmaBaselineData` command.
- Not specifying the correct HP DMA server host name in the `dmaBaselineData` command.
- Not running the `dmaBaselineData` command with the correct permissions (root).

The following topics will help you identify and resolve baseline errors.

For additional information, see "Install the HP DMA Server" in the *HP DMA Installation Guide*.

Oracle Database User Was Not Created

To verify that your HP DMA Oracle Database user was created:

1. Log in to Oracle Database:

   ```
   sqlplus / as sysdba
   ```

2. Run the following query:

   ```
   select username from dba_users where username like '%DMA%'
   ```

   This command will list any usernames where DMA is part of the name.

If your HP DMA Oracle Database user name is not on the list, have your Oracle Database administrator (DBA) follow the instructions in "Create and Configure the Oracle Database" in the *HP DMA Installation Guide* to add the HP DMA Oracle Database user.

Oracle Listener Is Not Running

To verify that the Oracle Listener is running:

1. On the Oracle Database system, run the following commands:

   ```
   su - oracle
   ps –ef | grep tns
   ```

2. If the Oracle Listener is running, the output of the `ps` command will be similar to this:

   ```
   [oracle@oraserver ~]$ ps -ef|grep tns
   oracle    3924     1  0 10:51 ?        00:00:00
   /u01/app/oracle/product/11.2.0/db1/bin/tnslsnr DMALIST -inherit
   oracle    3921  3632  0 10:50 pts/1    00:00:00 grep tns
   ```

   If the Oracle Listener is not running , the output of the `ps` command will be similar to this:

   ```
   [oracle@oraserver ~]$ ps -ef|grep tns
   oracle    3921  3632  0 10:50 pts/1    00:00:00 grep tns
   ```

If the Oracle Listener is not running, have your Oracle DBA start it.

Oracle Database Is Not Running

To verify that Oracle Database is running:

1. On the Oracle Database system, run the following commands:

   ```
   su - oracle
   ps –ef | grep pmon
   ```

2. If Oracle Database is running, the output of the `ps` command will be similar to this:

   ```
   [oracle@oraserver ~]$ ps -ef | grep pmon
   oracle    4018     1  0 10:55 ?        00:00:00 ora_pmon_dmademo
   oracle    4109  3956  0 10:55 pts/1    00:00:00 grep pmon
   ```

   If Oracle Database is not running, the output of the `ps` command will be similar to this:

   ```
   [oracle@oraserver ~]$ ps -ef | grep pmon
   oracle    3982  3956  0 10:54 pts/1    00:00:00 grep pmon
   ```

If Oracle Database is not running, have your Oracle DBA start it.

Error in the Oracle Server or Oracle SID Name

If you specify an incorrect host name for the Oracle Database system, an incorrect Oracle SID name, or any other incorrect database connection parameters in the `dmaBaselineData` command, the command will fail.

For example:

```
$ sh ./dmaBaselineData.sh --create-tables
--create-context --database-username dma --database-password dma
--jdbc-connection-string jdbc:oracle:thin:@badorcl.mycompany.com:1521:badsid
--dma-hostname dma.mycompany.com
```

This incorrect `dmaBaselineData` command will produce error messages similar to the following:

```
30 Jan 2005 11:28:45,901 INFO  DMABaselineData - Saved context file:
/opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/../WEB-
INF/../../../conf/Catalina/localhost/dma.xml
30 Jan 2005 11:28:45,903 INFO  DMABaselineData - Context file has been created.
30 Jan 2005 11:28:48,016 INFO  DMABaselineData - Using specified context for
settings (command line overrides ignored) file:
/opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/../WEB-
INF/../../../conf/Catalina/localhost/dma.xml
30 Jan 2005 11:28:48,834 ERROR DMABaselineData - Initial SessionFactory creation
failed.
30 Jan 2005 11:28:48,834 ERROR DMABaselineData - Unable to establish connection
with database using provided connection info.
java.lang.RuntimeException: Connection cannot be null when 'hibernate.dialect'
not set
at com.hp.dma.cmdline.DMABaselineData.init(DMABaselineData.java:171)
at com.hp.dma.cmdline.DMABaselineData.main(DMABaselineData.java:848)

...
```

To solve this problem:

- Verify that the TNS listener is running.
- Specify the correct names for the `dmaBaselineData` command.

HP DMA Client Fails to Contact HP DMA Server

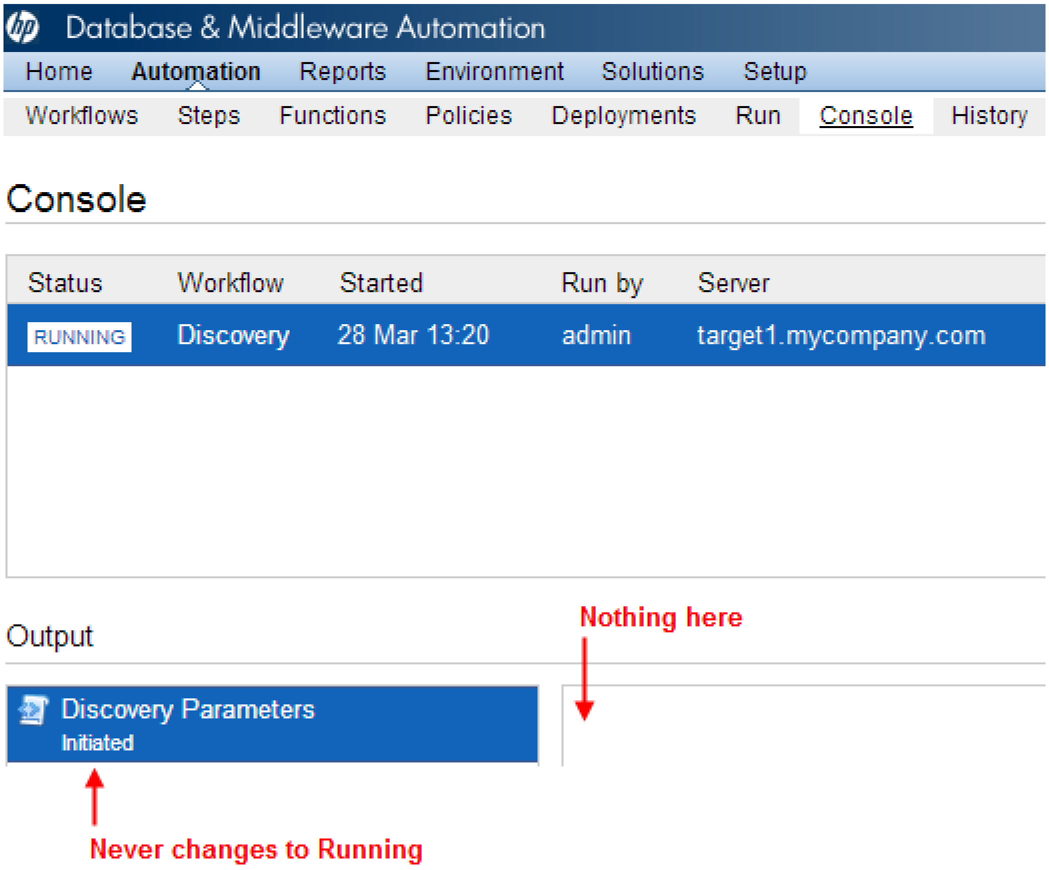
If the target server cannot communicate with the HP DMA server, a workflow will appear to be running when it really is not. There are several possible causes of this problem:

- The HP DMA server name is not resolvable on the target server.
- The HP DMA server is running a different port than the one specified in the `dma.xml` configuration file.

If the HP DMA server host name was not specified correctly when the `dmaBaselineData.sh` command was executed,

Symptoms

If this happens, the Console page looks like this—note that there are no messages in the step output box when you select the first step, and its status never changes from Initiated to Running.



Status	Workflow	Started	Run by	Server
RUNNING	Discovery	28 Mar 13:20	admin	target1.mycompany.com

Discovery Parameters
Initiated

Nothing here

Never changes to Running

The HP DMA log file on the target server will show that the target server cannot communicate with the HP DMA server:

```
2013-03-28 17:39:01,121 - INFO: Logging initiated for execution
'ff8080813db35c1e013db35e30e60000'
2013-03-28 17:39:01,312 - ERROR: Error with HTTP POST: "Failed to reach server:
error(111, 'Connection refused')"
2013-03-28 17:40:01,328 - ERROR: Error with HTTP POST: "Failed to reach server:
error(111, 'Connection refused')"
2013-03-28 17:41:01,345 - ERROR: Error with HTTP POST: "Failed to reach server:
error(111, 'Connection refused')"
```

This log file is located here on the target server:

- UNIX targets: `/var/tmp/DMA/<execution-id>/<execution-id>.log`
- Windows targets: `%TMPDIR%\dma\<execution-id>\<execution-id>.log`

  Note that that `%TMPDIR%` is evaluated based on the user running the workflow. If you log in as a different user, you may not see this file in your `%TMPDIR%`.

Note: You will see Connection Refused error messages (as shown above) if the specified `dma-hostname` is a valid and resolvable host name. If it is not a resolvable host name, you will see error messages like this one:

```
2013-03-28 17:48:07,026 - ERROR: Error with HTTP POST: "Failed to reach server:
gaierror(20001, 'getaddrinfo failed')"
```

Tip: This information is also displayed on the Connector Errors tab on the History page.

Solution

You can solve this problem by modifying the `webServiceUrl` parameter in the following file:

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

Perform these steps on the HP DMA server:

1. Stop the DMA service.

   ```
   $ service dma stop
   ```

2. In the `/opt/hp/dma/server/tomcat/conf/Catalina/localhost/dma.xml` file, check the highlighted value of webServiceUrl for the following:

   - The host name is correct
   - The host name is not `localhost`

- The host name is fully qualified
- The host name is spelled correctly

```
<?xml version="1.0" encoding="UTF-8"?>
<Context allowLinking="true" disableURLRewriting="true"
   path="/dma" privileged="true" swallowOutput="true"
   workDir="/var/opt/hp/dma/work/dma">
 <Valve className="org.apache.catalina.valves.AccessLogValve"
   directory="/var/log/hp/dma/" pattern="%h %l %u %t '%r' %s %b
   %S" prefix="localhost_access." suffix=".log"/>
 <Parameter name="com.hp.dma.core.webServiceUrl"
  value="https://dma1.mycompany.com:8443/dma"/>
 <Parameter name="com.hp.dma.conn.trustAllCertificates"
   value="false" />
 <Resource auth="container"
   driverClassName="oracle.jdbc.OracleDriver"
   factory="com.hp.dma.util.DmaTomcatContextHandler"
   maxActive="20" maxIdle="5" maxWait="2000" name="jdbc/dma"
   password="{AES}54dd1d97a915c4c3c8d0db986a1218db62008816fb924"
   type="javax.sql.DataSource"
   url="jdbc:oracle:thin:@dma1.mycompany.com:1521:DMA"
   username="dma"/>
</Context>
```

3. Start the DMA service.

   ```
   $ service dma start
   ```

Note: You must also terminate the HP DMA Client process on the target server (see Workflow Execution ScripT on page 88).

Did Not Run the Baseline Command as Root User

You must run the `dmaBaselineData` command as root. If you run `dmaBaselineData` as another user, it will fail.

For example:

```
$ sh ./dmaBaselineData.sh --create-tables --create-context
--database-username dma --database-password dma
--jdbc-connection-string jdbc:oracle:thin:@oraserver.mycompany.com:1521:dmademo
--dma-hostname dmaserver.mycompany.com
```

If you run this correct `dmaBaselineData` command as a user other than root, you will see error messages similar to the following:

```
log4j:ERROR setFile(null,true) call failed.
java.io.FileNotFoundException: /var/log/hp/dma/dma.log (Permission denied)
        at java.io.FileOutputStream.openAppend(Native Method)
        at java.io.FileOutputStream.<init>(Unknown Source)
        at java.io.FileOutputStream.<init>(Unknown Source)
        at org.apache.log4j.FileAppender.setFile(FileAppender.java:294)
        at org.apache.log4j.RollingFileAppender.setFile
(RollingFileAppender.java:207)
        at org.apache.log4j.FileAppender.activateOptions(FileAppender.java:165)

...

java.io.FileNotFoundException: /opt/hp/dma/server/tomcat/webapps/dma/WEB-
INF/../WEB-INF/../../../conf/Catalina/localhost/dma.xml (Permission denied)
        at java.io.FileOutputStream.open(Native Method)
        at java.io.FileOutputStream.<init>(Unknown Source)
        at java.io.FileOutputStream.<init>(Unknown Source)
        at com.hp.dma.cmdline.DMABaselineData.saveXMLFile
(DMABaselineData.java:713)
        at com.hp.dma.cmdline.DMABaselineData.main(DMABaselineData.java:837)
30 Jan 2005 10:43:43,463 ERROR CmdlineExceptionHandler - Exception
java.lang.Throwable: java.io.FileNotFoundException:
/opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/../WEB-
INF/../../../conf/Catalina/localhost/dma.xml (Permission denied

...
```

To solve this problem, run the `dmaBaselineData` command again as root.

APX Tool Configuration Error

You may receive an error that you do not have a valid APX file or directory when you perform the "Import the HP DMA APX" installation step.

Not Pointing to Correct APX Tool Directory

If you receive an error message similar to the following at the root command prompt, you are not pointing to the correct directory for the APX tool:

```
...

[root@dmaserver ~](4) $ apxtool import westapx.zip
Error: westapx.zip is not a valid APX file or directory.

...
```

If you have this problem, verify the location of the APX tool and rerun the `apxtool` command (see "Import the HP DMA APX" in the *HP DMA Installation Guide*).

DMA Client Files Policy Error

Possible errors that can occur when you install, attach, or remediate the DMA Client Files policy on the SA server are the following:

- The `/DMA_Client` directory does not exist or is not writable
- The Microsoft Patch Database is out of date

The following topics will help you identify and resolve DMA Client Files policy issues.

For additional information, see "Install the DMA Client Files Policy" in the *HP DMA Installation Guide*.

DMA_Client Directory Does Not Exist or Is Not Writable

Symptoms

If the `/DMA_Client` directory does not exist or is not writable you will receive error messages similar to the following when you run `dma_upload.sh`:

```
...

# sh ./dma_upload.sh -host sa2.mycompany.com -user myusername -password
mypassword -keyFile /opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/publicKey -
folderName /DMA_Client
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
Dload  Upload   Total   Spent    Left  Speed
100 2780k  100 2780k    0     0   120M      0 --:--:-- --:--:-- --:--:--  142M
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
Dload  Upload   Total   Spent    Left  Speed
100 1712k  100 1712k    0     0   127M      0 --:--:-- --:--:-- --:--:--  151M
CORBA BAD_PARAM 0 No; nested exception is:
org.omg.CORBA.BAD_PARAM:   vmcid: 0x0  minor code: 0  completed: No

...
```

Solution

Make sure that the `/DMA_Client` directory exists and you can write to it.

If the upload is successful, you will receive messages similar to the following:

```
...

# sh ./dma_upload.sh -host sa2.mycompany.com -user myusername -password
mypassword -keyFile /opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/publicKey -
folderName /DMA_Client
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
Dload  Upload   Total   Spent    Left  Speed
100 2780k  100 2780k    0     0   137M      0 --:--:-- --:--:-- --:--:--  150M
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
Dload  Upload   Total   Spent    Left  Speed
100 1712k  100 1712k    0     0   121M      0 --:--:-- --:--:-- --:--:--  139M
Policy associations for DMA completed.

...
```

Microsoft Patch Database Is Out of Date

It is important to have the latest Windows Patch Utilities on SA Core to support Windows 2012.

Symptoms

If your Windows 2012 servers are successfully managed by SA but failed to have the DMA Client Files policy installed, examine the contents of the Job Status log for Overall Server Status. If they are similar to the following, your Microsoft patch database is out of date.

```
The request to retrieve information from the Agent failed for an
unknown reason, please contact your HP Server Automation
Administrator.Execution error: Traceback (most recent call last):
File ".\base\wayfuncs.py",line 136, in evaluator
File "", line 3058, in ?

...

File ".\nt_hotfix_handler.py", line 539, in installedList
File ".\nt\nt_hotfix_handler.py", line 521, in
filterMbsa20ResultByInstalledOrRecommended
OpswareError:

...

params: {'handler':'nt_hotfix_handler','results':'AGENT_ERROR_PATCH_DATABASE_
CERTIFICATE_ERROR'}
request: UNKNOWN
tb_change: []

...
```

Solution

> **Tip:** The following steps must be performed by an SA administrator.
>
> You should verify that you are using the current Microsoft links and files. The ones listed here were correct as of the publication of this guide.

Perform the following steps to update the Microsoft Products and install the DMA Client Files policy on Windows 2012 servers:

1. Using the SA Client, navigate to the Administration > Patch Settings > Patch Products page.
2. Update the Windows Update Redistribution Catalog (`wuredist.cab`) with one of the following methods:
   a. Update Products from Vendor:

      Click the Update Products from Vendor button, set the URL to http://update.microsoft.com/redist/wuredist.cab, and then update.

   b. Update Product List from File:

      Download the `wuredist.cab` file manually at http://update.microsoft.com/redist/wuredist.cab and then click the Update Product List from File button to update the `wuredist.cab` file that you just downloaded.
3. Update the Security Update Catalog (`wsusscn2.cab`) with one of the following methods:
   a. Update Products from Vendor:

      Click the Update Products from Vendor button to update the available products list directly from Microsoft's web site (the default URL).

   b. Update Product List from File:

      Download the `wsusscn2.cab` file manually at http://go.microsoft.com/fwlink/?LinkId=76054 and then click the Update Product List from File button to update the `wsusscn2.cab` file that you just downloaded.

   This updates the catalog of available patches.
4. Navigate to the Administration > Patch Settings > Patch Database page.
5. Update the Windows Update Agent standalone installers with one of the following methods:
   a. Import from Vendor:

      From the Windows Patch Utilities pane—auto-populated from the Security Update Catalog—select `WindowsUpdateAgent30-x86.exe`, `WindowsUpdateAgent30-x64`, and `WindowsUpdateAgent30-ia64.exe`, and then click Import from Vendor.

   b. Import from File:

      Download the installer files manually from:

http://download.windowsupdate.com/windowsupdate/redist/standalone/7.4.7600.226/WindowsUpdateAgent30-x86.exe

http://download.windowsupdate.com/windowsupdate/redist/standalone/7.4.7600.226/WindowsUpdateAgent30-x64.exe

http://download.windowsupdate.com/windowsupdate/redist/standalone/7.4.7600.226/WindowsUpdateAgent30-ia64.exe

Click the Import from File button to update the installer files that you just downloaded.

6. Clean up any Windows 2012 servers that indicate that the DMA Client Files policy is installed but are actually in a corrupt state.
7. Install the DMA Client Files policy on the Windows 2012 servers and remediate. For more information, see "Install the DMA Client Files Policy" in the *HP DMA Installation Guide*.

   Examine the contents of the Job Status log for the ✓ Succeeded status.
8. To update your repository with the same patching tools, copy the files that were downloaded in steps 3 and 5 to the Windows patching utilities directory on your SA Core (for example: `/root/wintools` or `/root/winutils`).

For more information see the *White Paper: SA 9.14: SA Server Patching Update* and the *SA 9.10 User Guide: Server Patching* that are available on the HP Software Support web site:

https://softwaresupport.hp.com/

Connector Errors

The HP DMA connector enables HP DMA and SA to communicate. Possible errors that can occur when you configure the connector are:

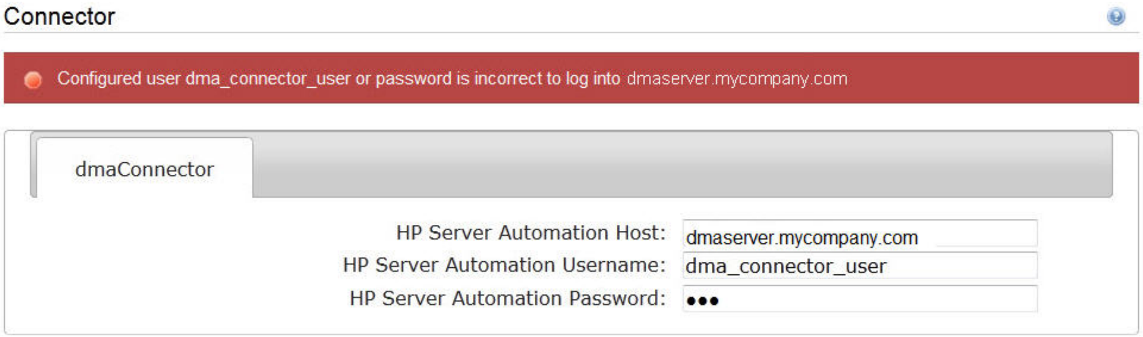
- The SA Core server is down.
- The JAR files are not at the required locations.

The following topics will help you identify and resolve connector errors.

For additional information, see "Configure the Connector" in the *HP DMA Installation Guide*.

The SA Core Server Is Down

You may see the following error when you try to add the connector:



Connector

Configured user dma_connector_user or password is incorrect to log into dmaserver.mycompany.com

HP Server Automation Host: dmaserver.mycompany.com
HP Server Automation Username: dma_connector_user
HP Server Automation Password: ●●●

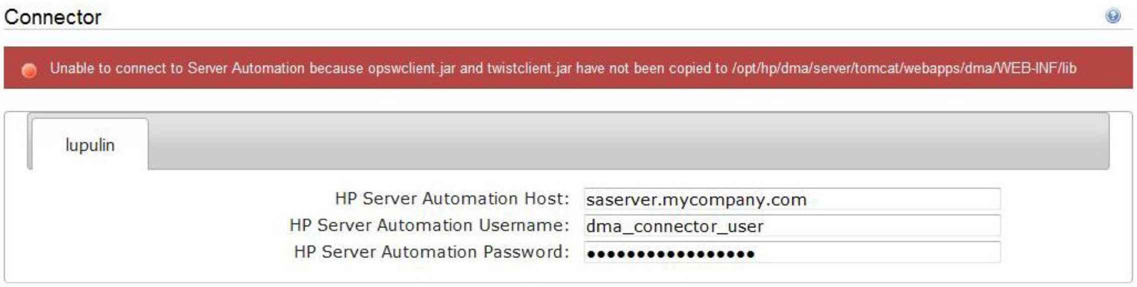
If you experience this error, examine the contents of the `/var/log/hp/dma/dma.log` file. If they are similar to the following, your SA server is down:

```
...

2013-03-14 08:46:47,720 INFO [main] SAConnector$StartExceptionHandler.handle:962
Can't connect to Host saserver.mycompany.com on port 443
2013-03-14 08:46:47,723 INFO [main]
BaseExceptionHandler.makeConnectorExceptionException:174
Can't connect to Host 'saserver.mycompany.com' on port 443. Ensure HP Server
Automation is currently running on 'saserver.mycompany.com' and firewall does
not block access to port 443.
org.omg.CORBA.COMM_FAILURE:   vmcid: SUN  minor code: 201  completed: No
at com.sun.corba.se.impl.logging.ORBUtilSystemException.connectFailure
(ORBUtilSystemException.java:2200)

...
```

If your SA server is down, have your SA administrator fix the problem.

The JAR Files Are Not at the Required Locations

You may receive the following message when you try to add the connector:



Connector

Unable to connect to Server Automation because opswclient.jar and twistclient.jar have not been copied to /opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/lib

lupulin

HP Server Automation Host: saserver.mycompany.com
HP Server Automation Username: dma_connector_user
HP Server Automation Password: •••••••••••••••••

If you receive this error message,examine the contents of the `/var/log/hp/dma/dma.log` file. If the file contents are similar to the following, the `opswclient.jar` and `twistclient.jar` files are not at the required locations:

```
2005-01-30 16:37:54,626  INFO [main] PersistenceService:137 - Setting
oracle.net.tns.admin
2005-01-30 16:37:57,037  INFO [main] WorkflowStarter:107 - abortIfNotStarted =
true
2005-01-30 16:37:57,489 ERROR [main] StartupListener:114 - Unable to connect to
Server Automation because opswclient.jar and twistclient.jar have not been
copied to /opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/lib
2005-01-30 16:37:57,489  INFO [main] StartupListener:115 - Failure:
java.lang.NoClassDefFoundError: com/opsware/client/TokenFinder

...

2005-01-30 16:37:57,491 ERROR [main] StartupListener:49 - Exception on startup
java.lang.RuntimeException: Unable to start DMA due to Connector failure
```

To fix this problem, run the script command to copy the required JAR files to the correct locations as described in "Install the HP DMA Server" in the *HP DMA Installation Guide*.

Login Errors

If you are unable to log in to HP DMA, you may receive the following messages on the login screen:

- Credentials are incorrect or do not allow login.

- Error: Failed to connect with the configured database.

  This can be caused by an invalid or locked out user, an incorrect password, or an unavailable database. Fix the problem with your database connection, restart DMA and try again.

Assuming that you have a valid username and password, the following cases may cause this problem:

- The SA server is down.
- Your role (SA group) does not have Login Access capability.
- HP DMA started before SA was running.
- The database password changed (or expired).
- The HP DMA database is not accessible.
- The SA core was updated.
- Your HP DMA server has been switched to a different SA core.
- The HP DMA login page does not work with the Internet Explorer.

Use the following information to help you identify and resolve the problem.

The SA Core Server Is Down

If your login fails, examine the contents of the `/var/log/hp/dma/dma.log` file. If they are similar to the following, the SA server is probably down:

```
2005-01-30 17:25:19,182  INFO [http-8443-1] SAConnector:176 - SA Exception
transformed into
com.hp.dma.conn.ConnectorException: Error calling HP Server Automation Twister
API on dmaserver.mycompany.com. HP Server Automation may be down or core
unreachable.

...

2005-01-30 17:25:19,186  INFO [http-8443-1] LoginAction:158 - User dmausername
failed to log in
```

If your SA server is down, have your SA administrator start it.

The SA Group Does Not have Login Access

If your login fails, examine the contents of the `/var/log/hp/dma/dma.log` file. If they are similar to the following, none of the user's roles (SA groups) have Login Access capability:

```
...

2013-03-21 15:58:48,145  INFO [http-8443-6] LoginAction:136 - User joe_user is
valid in connector ff8080813d69ac23013d69ac475a0000 but has no role allowing
login
2013-03-21 15:58:48,146  INFO [http-8443-6] LoginAction:158 - User joe_user
failed to log in

...
```

If an HP DMA user’s role (SA Group) does not have Login Access capability, add that user to a role (SA group) that does have Login Access capability – or register a different role, and grant that role Login Access capability.

See "Set Up the SA Groups and Users" in the *HP DMA Installation Guide* for more information.

HP DMA Started Before SA was Running

If all of the following conditions are true, and you still see the "Credentials are incorrect or do not allow login" error message, it is possible that HP DMA started running before SA was running:

- You are certain that your credentials are correct.
- You are certain that at least one of your HP DMA roles (SA groups) has Login Access capability.
- SA is now running.

The solution to this problem is to simply stop and restart HP DMA:

1. Stop the DMA service.

   ```
   $ service dma stop
   ```

2. Start the DMA service.

   ```
   $ service dma start
   ```

Oracle Database/PostgreSQL Password Changed

Periodically the password for the database may change (or expire). HP DMA provides a script to change the password that is stored in the `dma.xml` file.

If your login fails, examine the contents of the `/var/log/hp/dma/dma.log` file. Example: If they are similar to the following, the Oracle database password changed:

```
2014-03-03 12:18:14,436  INFO [localhost-startStop-1] PersistenceService:143 -
Setting oracle.net.tns.admin
2014-03-03 12:18:15,412 ERROR [localhost-startStop-1] StartupListener:63 -
Exception on startup
org.hibernate.HibernateException: Connection cannot be null when
'hibernate.dialect' not set
at
org.hibernate.service.jdbc.dialect.internal.DialectFactoryImpl.determineDialect
(DialectFactoryImpl.java:97)
at org.hibernate.service.jdbc.dialect.internal.DialectFactoryImpl.buildDialect
(DialectFactoryImpl.java:67)
at org.hibernate.engine.jdbc.internal.JdbcServicesImpl.configure
(JdbcServicesImpl.java:170)

...

at java.util.concurrent.Executors$RunnableAdapter.call(Unknown Source)
at java.util.concurrent.FutureTask.run(Unknown Source)
at java.util.concurrent.ThreadPoolExecutor.runWorker(Unknown Source)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(Unknown Source)
at java.lang.Thread.run(Unknown Source)
```

If your Oracle/PostgreSQL password changed, perform the following:

1. Run the following commands to execute the `changeDbPassword` script:

   ```
   $ cd /opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/
   ```

   Use either the short command:

   ```
   $ sh ./changeDbPassword.sh -dbpw <dbpw>
   ```

   Or the long command:

   ```
   $ sh ./changeDbPassword.sh --database-password <dbpw>
   ```

   Here, *<dbpw>* is the new password.

2. Restart the DMA service:

   ```
   $ service dma restart
   ```

The HP DMA Database is Not Accessible

If the previous troubleshooting cases do not solve your login issue, it is possible that the Oracle database/PostgreSQL is not accessible. To determine whether this is the case, perform the following:

1. Examine the contents of the `/opt/hp/dma/server/tomcat/conf/Catalina/localhost/dma.xml` file.
2. Locate the Resource entry. Example: If it looks similar to the following:

   ```
   <Resource name="jdbc/dma" auth="container" type="javax.sql.DataSource"
   maxActive="20" maxIdle="20" maxWait="20000" username="dma" password="{AES}
   9bd10ee0695c84daccec11d5dbbaaccd2045240810732fc005ad3c57f6d6bfee"
   driverClassName="oracle.jdbc.OracleDriver"
   url="jdbc:oracle:thin:@mydma.example.com:1521:dma"
   factory="com.hp.dma.util.DmaTomcatContextHandler" />
   ```

3. Verify the following:

   - You are pointing to the correct system—this might be incorrect in `/etc/hosts` or DNS.

   - You have the correct database user.

   - You have the correct Oracle SID.

   - You have the correct port number.

   If you find any incorrect values continue with steps 4 to 6.

4. Stop the DMA service:

   ```
   $ service dma stop
   ```

5. Edit the incorrect values in the `dma.xml` file and save.
6. Restart the DMA service:

   ```
   $ service dma restart
   ```

The SA Core was Updated

If you cannot log in to HP DMA (or can only log in as `dma_initial_admin`), it is possible that the SA core was updated but the JAR files were not updated. This is most likely to occur if you have different individuals administering SA and HP DMA.

To solve this problem perform the following steps:

1. On your HP DMA server, run the following script command to copy the required JAR files from the SA server to the HP DMA server. For example (enter as a single line):

   ```
   $ sh /opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/copyJars.sh
   <SA_Server>
   ```

   > **Note:** Whenever the SA Core is upgraded you need to rerun this command.

2. Restart the DMA service:

   ```
   $ service dma restart
   ```

HP DMA is Switched to Different SA Core

If you switch to a different SA core, you may not be able to log in to HP DMA.

> **Caution:** It is NOT recommended to switch the HP DMA Server to an SA Core that is NOT part of the same SA mesh. The recommended solution is to install a new HP DMA Server. Follow the instructions in "How to Install HP DMA" in the *HP DMA Installation Guide*. To move your workflows from the old HP DMA Server to the new server, use the Promote workflows that are described in the *HP DMA Promote User Guide.*

If your login fails, examine the contents of the `/var/log/hp/dma/dma.log` file. If they are similar to the following, the HP DMA server has been switched to a different SA core:

```
2014-04-03 15:12:25,887  INFO [http-bio-8443-exec-3] LoginAction:187 - User fred
is valid in connector 90cefcae43bffe650143c00c2b140001 but has no role allowing
login
2014-04-03 15:12:25,888  INFO [http-bio-8443-exec-3] LoginAction:209 - User fred
failed to log in
```

The problem is that HP DMA is remembering the SA IDs from the original SA core—which do not apply to the new SA core.

To solve this problem perform the following steps while logged in to the HP DMA server as the default initial HP DMA administrator (`dma_initial_admin`):

1. Go to the **Setup** tab.
2. To update HP DMA to recognize the new SA roles:
   a. Go to the **Roles** tab.
   b. Use the < or << button to remove the all of the currently registered roles.
   c. Click **Save**.
   d. Then use the > or >> button to replace the same SA roles (that now contain the updated SA IDs).
   e. Click **Save**.
3. To force the HP DMA capabilities to associate with the new roles:
   a. Go to the **Capabilites** tab.
   b. Open the window to view assigned roles by clicking any of the Capabilities (Administrator, Login Access, Workflow Create).

c. Remove any of the capabilities and then click **Save**.

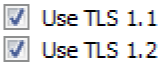
d. Add the capability that you removed and then click **Save** again.

The HP DMA Login Page Does Not Work with Internet Explorer

If you cannot log in to HP DMA with the Internet Explorer (IE) browser but can log in with other browsers, you will need to configure IE's security settings to work with the HP DMA Server.

To solve this problem, each person who wants to use HP DMA with IE needs to perform the following steps:

1. Open the IE browser
2. Go to **Tools** (⚙) > **Internet options** > **Advanced** (tab)
3. Scroll down to 🔒 **Security**
4. Enable **Use TLS 1.1** and **Use TLS 1.2**:

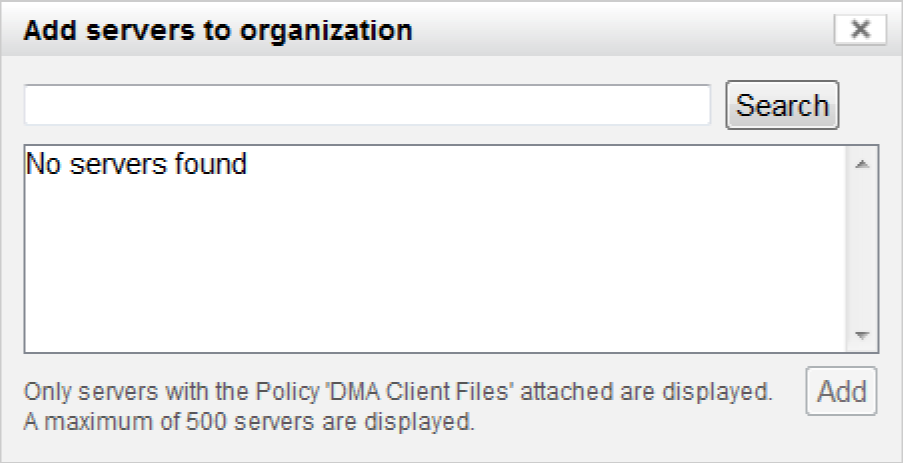
   

   ☑ Use TLS 1.1
   ☑ Use TLS 1.2

5. Click **OK**
6. Close and reopen IE

No Servers Available to Add to HP DMA

If no servers are available in the "Add Available Targets" installation step, you will see the following error when you try to add servers to an organization:



Add servers to organization

No servers found

Only servers with the Policy 'DMA Client Files' attached are displayed.
A maximum of 500 servers are displayed.

There are several situations that may cause this problem:

- The HP DMA connector user does not have the proper permissions.
- The HP DMA connector user cannot find any servers.
- The servers are already included in another HP DMA organization.
- The HP DMA user who is logged in does not have the correct permissions.
- The DMA Client Files policy is not attached and remediated on any managed servers.

Use the following information to help you identify and resolve the problem.

The HP DMA Connector User Does Not Have Required Permissions

If you experience a "No servers found" error, examine the contents of the `/var/log/hp/dma/dma.log` file. If they are similar to the following, your HP DMA connector user (dma_connector_user) does not have the required permissions:

```
...

2013-03-15 14:43:43,301 ERROR [http-8080-1] DmaPolicyCacher.update:183
DMA Client Files does not exist
2013-03-15 14:43:43,301 INFO [http-8080-1] DmaPolicyCacher.findServers:94
No DMA Client Files

...
```

If you have this problem, have your SA administrator grant the dma_connector_user the following permissions:

- Manage Software Policy (Read)
- List, Read, and Execute permission on the folder containing the DMA Client Files policy (for example: `/DMA_Client`)

For more information, see "Set Up the SA Groups and Users" in the *HP DMA Installation Guide*.

The HP DMA Connector User Cannot Find Any Servers

If you experience a "No servers found" error when the HP DMA connector user (dma_connector_user) has the required permissions on the folder containing the DMA Client Files policy (for example: `/DMA_Client`), examine the contents of the `/var/log/hp/dma/dma.log` file. If they are similar to the following, either there are no servers with the DMA Client Files policy attached, or the HP DMA connector user does not have Read permission for the servers:

```
...

2013-03-15 14:59:57,377 INFO [http-8080-1]
DmaPolicyCacher.getDMASoftwarePolicyRef:306
DMA Software Policy ref is DMA Client Files (SoftwarePolicyRef:1230001)

...
```

```
2013-03-15 14:59:57,634 INFO [http-8080-1] DmaPolicyCacher.findServers:107
User can't read any servers or no servers have policy DMA Client Files
```

If you have this problem, have your SA administrator check two possible solutions:

- Attach and remediate the DMA Client Files policy to the servers.
- Grant the dma_connector_user Read permission for the servers.

For more information, see "Install the DMA Client Files Policy" and "Set Up the SA Groups and Users" in the *HP DMA Installation Guide*.

The Servers Are Already in Another HP DMA Organization

Servers can only be in one HP DMA organization. If they are already included in another organization, they will not be available for you to add.

If you experience a "No servers found" error, examine the contents of the `/var/log/hp/dma/dma.log` file. If they are similar to the following, all servers that you are able to add are already included in another organization:

```
...

2013-03-15 15:08:13,655 INFO [http-8080-1] DmaPolicyCacher.findServers:126
Returning 2

...
```

If you have this problem, contact your HP DMA administrator to determine which organization the servers should belong to.

The HP DMA User Does Not Have Correct Permissions

Another possible cause of a "No servers found" error is that the HP DMA user who is currently logged in does not have the correct permissions.

To determine whether this is the case:

1. Log in to HP DMA as a different user, preferably one with Administrator capability.
2. Have this user try to add targets (see "Add Available Targets" in the *HP DMA Installation Guide*).

If the HP DMA administrator can see the servers in the Add Servers to Organization dialog, have your SA administrator grant the following permissions to the SA group to which your HP DMA user belongs:

- List, Read, and Execute permission for the `/DMA_APX` folder
- Managed Servers and Groups
- Read access to all managed servers that will be added to HP DMA

For more information, see "Set Up the SA Groups and Users" in the *HP DMA Installation Guide*.

The DMA Client Files Policy Is Not Attached and Remediated

Another possible cause of a "No servers found" error is that the DMA Client Files policy has not been attached and remediated on the servers.

To determine whether this is the case, have your SA administrator check that the DMA Client Files policy is attached and remediated on all servers that need to be available to HP DMA, as described in "Install the DMA Client Files Policy" in the *HP DMA Installation Guide*.

Run Time Errors

Possible errors that may occur when you run HP DMA workflows are the following:

- HP DMA workflows may abort because you are using an internal SSL certificate.
- HP DMA workflows may abort shortly after doing an HP DMA upgrade.
- HP DMA workflows may appear to be "stuck" in a perpetual running state.
- HP DMA deployments may be skipped if another deployment of the same workflow is already running.

Use the following information to help you identify and resolve the problem.

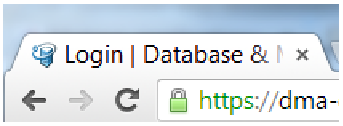
Workflow Aborts Using an Internal SSL Certificate

If you obtained an internal SSL certificate from your company's internal certification authority, your HP DMA workflows may abort.

Symptoms

If you have this problem you will observe the following:

1. When you log in to the HP DMA server you correctly observe the lock icon:

2. Go to Automation > History. You see that your workflow status is ABORTED.
3. Select your workflow.
4. Go to the Connector Output tab. Verify that the HP DMA connector output does NOT contain the following:

   ```
   Warning: DMA Client is trusting all HTTPS Certificates
   ```

   If you do not have this message, HP DMA is using an SSL certificate—such as an internal SSL certificate—for the connection.

5. Go to the Connector Errors tab. See whether the stacktrace contains messages similar to the following:

   ```
   ...

   WestHttpClientException: com.hp.dma.client.WestHttpClientException: Invalid
   SSL Certificate returned from https://dma-
   mycompany.com:8443/dma/api/execute/workflow/90cefce442b538650142b53912b60000
   /server/90cefce4429544990142954a915c000b : peer not authenticated
   The West APX execution was not successful

   ...
   ```

   If so, the problem is that the target server’s JRE could not authenticate the SSL certificate from your company’s internal certification organization. Only certificates which are traceable back to a trusted Certification Authority (CA) can be authenticated.

Solution

The solution is to add your company’s Certification Authority certificate to all target JREs.

Consult with your company’s security team to determine the proper procedure for adding your company’s Certification Authority to the list of trusted certificates.

Workflow Aborts After an HP DMA Upgrade

After upgrading HP DMA to version 10.22 (or later), HP DMA may stop working. This may be caused if the HP DMA clients do not have the increased security settings specified in the upgraded `server.xml` file.

Symptoms

If you have this problem you will observe the following:

1. Go to Automation > History. You see that your workflow status is ABORTED.
2. Select your workflow.
3. Go to the Connector Errors tab. See whether the stacktrace contains messages similar to the following:

   ```
   *sys-package-mgr*: processing modified jar,
   '/opt/hp/dma/client/lib/westhttpclient.jar'
   Invalid SSL Certificate returned from
   https://dmaserver.mycompany.com:8443/dma/api/execute/workflow/ff8080813cfda9
   fa013cfdaa7aa9113f
   2014-11-21 11:48:42 - Error occurred during WEST execution
   ```

```
Traceback (most recent call last):
 File "/opt/hp/dma/client/bin/west.py", line 59, in main
   encoded, headers, count = run_workflow(options, encoded, headers,
storage_dir)
 File "/opt/hp/dma/client/bin/west.py", line 126, in run_workflow
   code, response = wh.get_http_post_response(options, headers)
  File "/opt/hp/dma/client/jython/Lib/westhttp.py", line 400, in _execute_
post
    return _try_to_execute_post(options, url, headers)
  File "/opt/hp/dma/client/jython/Lib/westhttp.py", line 412, in _try_to_
execute_post
    raise rsp_exc
WestHttpClientException: com.hp.dma.client.WestHttpClientException: Invalid
SSL Certificate returned from https://dmaserver.mycompany.com

The West APX execution was not successful
```

If so, the HP DMA RPMs have been upgraded but the DMA Client Files policy was not remediated, so that HP DMA refuses to communicate with the managed servers.

Solution

You can solve this problem by reinstalling the DMA Client Files policy on the SA core and remediating the policy on all managed servers that use that policy. Follow the instructions in "How to Upgrade HP DMA" steps 10, 11, and 12 in the *HP DMA Installation Guide*.

Workflows "Stuck" in Perpetual Running State

If you have workflow deployments that seem to be "stuck" in a perpetual running state, HP DMA provides a script to cancel the deployments.

Symptoms

Workflow deployments may become "stuck" in a perpetual running state when deployments started at the same time that the HP DMA Server restarted. The deployments remain in the "Initiated" state but never proceed to the "Finished" state.

Solution

You can solve this problem by running the `cancelWorkflow` script. It will cancel ALL workflows that are in the "Initiated" and "Running" states.

1. Stop the DMA service:

   ```
   $ service dma stop
   ```

2. Run the following commands to execute the `cancelWorkflow.sh` script:

```
$ cd /opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/
```

```
$ sh ./cancelWorkflow.sh
```

3. After the script completes, restart the DMA service:

```
$ service dma restart
```

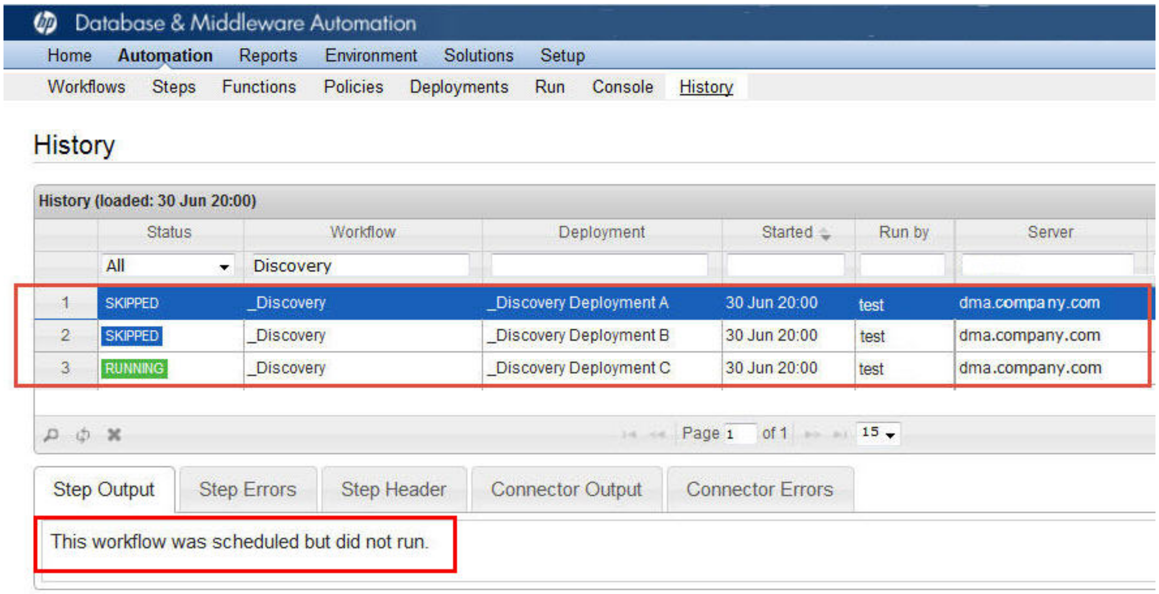
Deployments Are Skipped if Another Deployment of Same Workflow Is Running

By default, HP DMA only allows a single deployment of a workflow to run at the same time. This is true for either manual or scheduled deployment executions. If you desire to run multiple deployments of the same workflow at the same time, HP DMA provides a parameter in the `dma.xml` file that allows you to do so.

Symptoms

You may observe these symptoms if HP DMA is limited to only a single deployment of a workflow at a time:

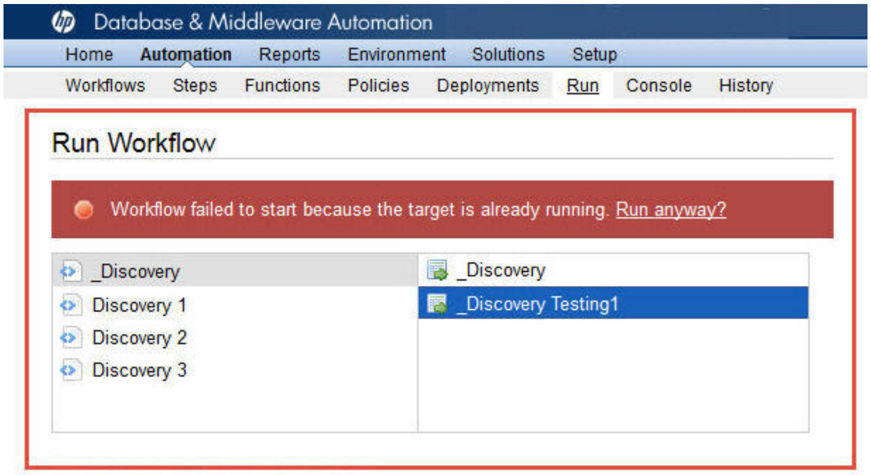
- If multiple deployments of the same workflow are scheduled at the same time, the History page shows that the deployment is "skipped" and gives the message "This workflow was scheduled but did not run":



	Status	Workflow	Deployment	Started	Run by	Server
	All	Discovery				
1	SKIPPED	_Discovery	_Discovery Deployment A	30 Jun 20:00	test	dma.company.com
2	SKIPPED	_Discovery	_Discovery Deployment B	30 Jun 20:00	test	dma.company.com
3	RUNNING	_Discovery	_Discovery Deployment C	30 Jun 20:00	test	dma.company.com

This workflow was scheduled but did not run.

- If you attempt to manually execute such a deployment, you receive this warning:


Database & Middleware Automation
Home Automation Reports Environment Solutions Setup
Workflows Steps Functions Policies Deployments Run Console History
Run Workflow

Workflow failed to start because the target is already running. Run anyway?

_Discovery
Discovery 1
Discovery 2
Discovery 3
_Discovery
_Discovery Testing1

Solution

You can solve this problem by adding the `Schedulerskipchecklevel` parameter to the `dma.xml` file:

1. Stop the DMA service:

   ```
   $ service dma stop
   ```

2. Open the `dma.xml` file in a text editor. For example:

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

3. Key in the following line to add the `Schedulerskipchecklevel` parameter to the file:

   ```
   <Parameter name="com.hp.dma.core.action.Schedulerskipchecklevel" value="1" />
   ```

   Note: To revert to the default functionality (only one deployment of the same workflow can run at a time), change the value to "2".

4. Save your changes to the `dma.xml` file.

5. Restart the DMA service:

   ```
   $ service dma restart
   ```

Sybase 15.7 Patch Workflow Error

In case you get the following error:

`Copy of <Sybase Source Install folder> to <Sybase backup folder> failed: cp: cannot create regular file <sybase file name> : Permission denied`, perform the steps below to resolve the error.

1. Take a copy of all the files and folders in the Sybase backup location.

   Example: `cp /opt/app/syb_backup/* <user-sybase-home>/syb_backup`

2. Delete all files and folders in the Sybase backup location.

   Example: `rm -rf /opt/app/syb_backup/*`

3. Run the Sybase 15.7 patch workflow.

Performance Issues

Use the following information to help you identify and resolve performance issues that occur when running HP DMA.

Intermittently Unable to Log In and System Freezes

When you run many (more than 10) HP DMA workflows at the same time, you may experience intermittent performance issues:

- HP DMA becomes slow for users who are logged in
- New users are unable to log in
- HP DMA freezes

You can resolve this by changing the HP DMA configuration:

1. Stop HP DMA:

   ```
   # service dma stop
   ```

2. Open the `dma.xml` file in a text editor. For example:

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

3. Add the following lines to the file:

   ```
   <Parameter name="com.hp.dma.core.action.WorkflowStarter.poolSize" value="40" />
   <Parameter name="com.hp.dma.core.action.WorkflowStarter.maxPoolSize" value="40"
   />
   ```

4. Save your changes to the `dma.xml` file.

5. Start HP DMA:

   ```
   # service dma start
   ```

Maintenance

This section provides information about HP DMA maintenance capabilities:

- Reset the password for the HP DMA Initial Admin (dma_initial_admin) account.
- Update the Self-Signed SSL Certificate—generate a new Self-Signed SSL Certificate and distribute your certificate to your managed servers.

Use the following information to help you properly maintain your HP DMA system.

Reset the HP DMA Initial Admin password

For security reasons you may want to reset the password for the HP DMA Initial Admin (dma_initial_admin) account.

HP DMA provides a script to change the password for the HP DMA Initial Admin (dma_initial_admin) account.

To obtain online help:

Run the following command on the HP DMA server (on one line):

```
$ sh /opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/changeInitialAdminPassword.sh [-
help]
```

Here, `-help` is optional.

Method 1: To reset the password interactively

Perform these steps on the HP DMA server:

1. Run the following command (on one line):

   ```
   $ sh /opt/hp/dma/server/tomcat/webapps/dma/WEB-
   INF/changeInitialAdminPassword.sh -prompt
   ```

2. Enter the new password at the prompt.
3. Reconfirm the password at the prompt.

Method 2: To reset the password on the command line

> **Note:** Use the command line procedure only to integrate the password change into an automated process since the new password may be observed when entered in the command line.

Run the following command on the HP DMA server (on one line):

```
$ sh /opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/changeInitialAdminPassword.sh -password <password>
```

Here, <*password*> is the new password.

Results

If the password is successfully reset you will receive the message:

```
Successfully updated the dma_intial_admin password.
```

If the password is not successfully reset you will receive the message:

```
Failed to update the dma_initial_admin password.
```

Update Self-Signed SSL Certificate

This 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 includes:

- Update Self-Signed SSL Certificate on the HP DMA Server
- Update Self-Signed SSL Certificate on the HP DMA Client

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/.keystore
   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/.keystore
   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 .

   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/.keystore
   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):

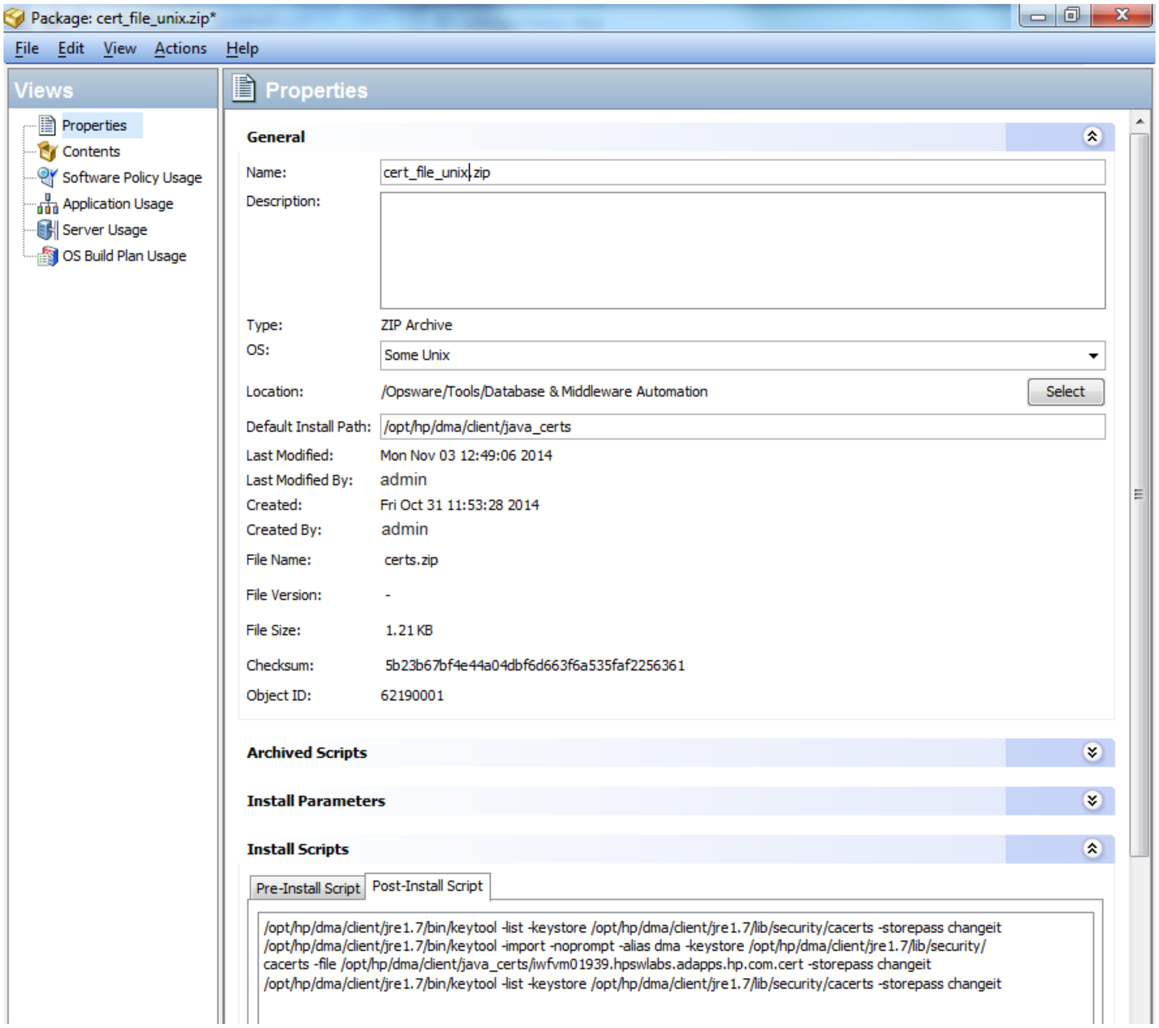
```
/opt/hp/dma/client/jre1.7/bin/keytool -list -keystore /opt/hp/dma/client/
jre1.7/lib/security/cacerts -storepass <password>
```

```
/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:



Name: cert_file_unix.zip
Description:
Type: ZIP Archive
OS: Some Unix
Location: /Opsware/Tools/Database & Middleware Automation
Default Install Path: /opt/hp/dma/client/java_certs
Last Modified: Mon Nov 03 12:49:06 2014
Last Modified By: admin
Created: Fri Oct 31 11:53:28 2014
Created By: admin
File Name: certs.zip
File Version: -
File Size: 1.21 KB
Checksum: 5b23b67bf4e44a04dbf6d663f6a535faf2256361
Object ID: 62190001

```
/opt/hp/dma/client/jre1.7/bin/keytool -list -keystore /opt/hp/dma/client/jre1.7/lib/security/cacerts -storepass changeit
/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/iwfvm01939.hpswlabs.adapps.hp.com.cert -storepass changeit
/opt/hp/dma/client/jre1.7/bin/keytool -list -keystore /opt/hp/dma/client/jre1.7/lib/security/cacerts -storepass changeit
```

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"
      ```

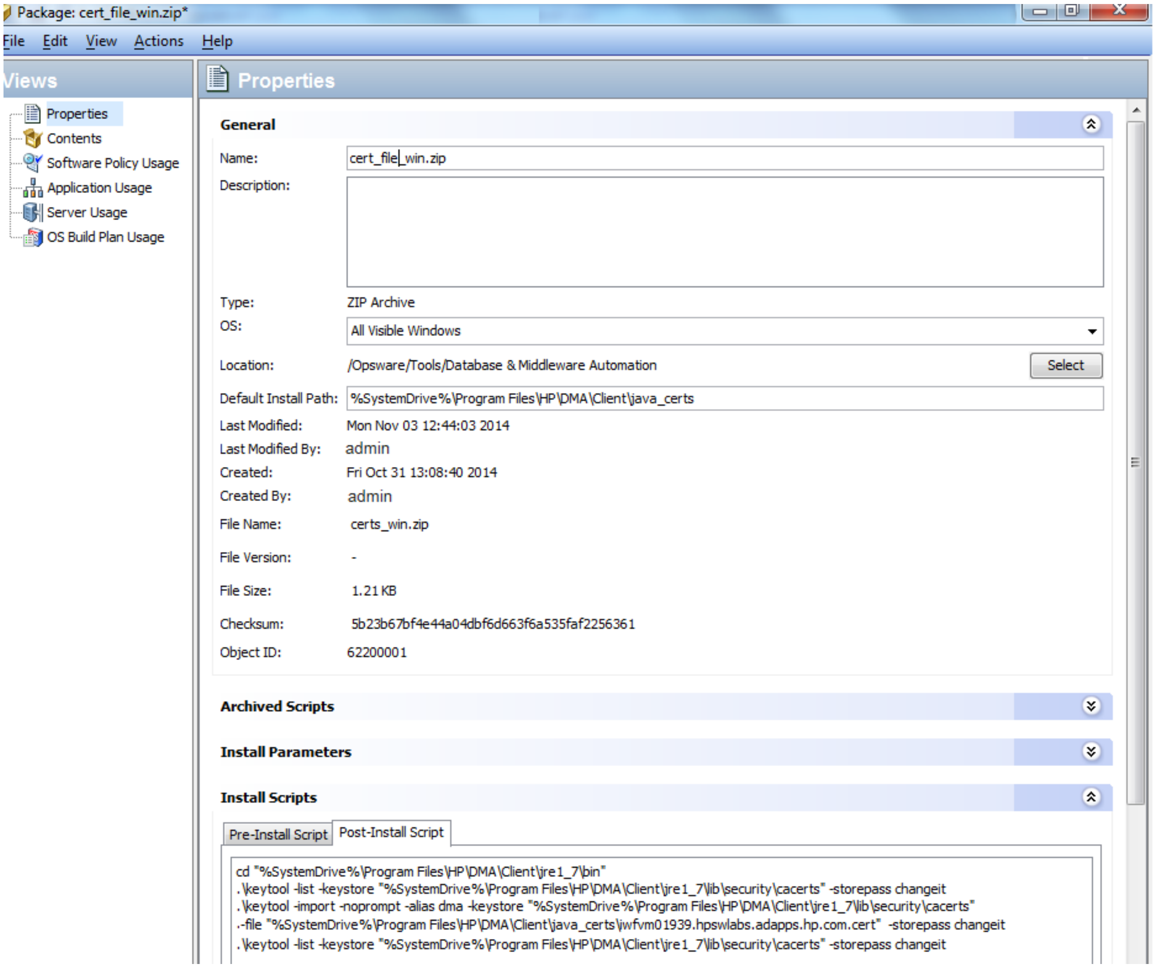
```
.\keytool -list -keystore "%SystemDrive%\Program Files\HP\DMA\Client\jre1_
7\lib\security\cacerts" -storepass <password>
```

```
.\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:



Name: cert_file_win.zip
Description:
Type: ZIP Archive
OS: All Visible Windows
Location: /Opsware/Tools/Database & Middleware Automation
Default Install Path: %SystemDrive%\Program Files\HP\DMA\Client\java_certs
Last Modified: Mon Nov 03 12:44:03 2014
Last Modified By: admin
Created: Fri Oct 31 13:08:40 2014
Created By: admin
File Name: certs_win.zip
File Version: -
File Size: 1.21 KB
Checksum: 5b23b67bf4e44a04dbf6d663f6a535faf2256361
Object ID: 62200001

```
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 changeit
.\keytool -import -noprompt -alias dma -keystore "%SystemDrive%\Program Files\HP\DMA\Client\jre1_7\lib\security\cacerts"
.-file "%SystemDrive%\Program Files\HP\DMA\Client\java_certs\jwfvm01939.hpswlabs.adapps.hp.com.cert"  -storepass changeit
.\keytool -list -keystore "%SystemDrive%\Program Files\HP\DMA\Client\jre1_7\lib\security\cacerts" -storepass changeit
```

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.

Chapter 2: Special Configurations

This chapter contains information about non-default HP DMA configurations:

Change the Default Port and Security Level

HP DMA uses port 8443 and HTTPS protocol by default. If you prefer, you can change this to another port (for example, 8080) and the protocol from secure to non-secure (for example, HTTP).

To change the HP DMA **port:**

1. Stop HP DMA:

   ```
   # service dma stop
   ```

2. Open the `server.xml` file in a text editor. For example:

   ```
   # vi /opt/hp/dma/server/tomcat/conf/server.xml
   ```

3. On line 84, set the desired port and security protocol:

   a. For a secure port (default), set the line as follows:

      ```
      <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
       maxThreads="150" scheme="https" secure="true"
       clientAuth="false" sslProtocol="TLS"
       keystoreFile="/opt/hp/dma/server/.keystore"/>
      ```

   b. For a non-secured port, set the line as follows:

      ```
      <Connector port="8080" protocol="HTTP/1.1" SSLEnabled="false"
       maxThreads="150" scheme="http" secure="false"
       clientAuth="false" sslProtocol="TLS"
       keystoreFile="/opt/hp/dma/server/.keystore"/>
      ```

4. Save your changes to the `server.xml` file.

5. Open the `dma.xml` file in a text editor. For example:

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

6. Change the port number specified in the value of the `webServiceUrl` parameter to the same port that you specified in step 3.

   ```
   <Parameter name="com.hp.dma.core.webServiceUrl"
   value="https://dma01.mycompany.com:8443/dma"/>
   ```

7. Save your changes to the `dma.xml` file.

8. Start HP DMA:

   ```
   # service dma start
   ```

Use a Proxy Server with HP DMA

A proxy server can be used to provide additional security for HP DMA communications. This topic shows you how to use an HP Server Automation (SA) Satellite as a proxy server.

Caution: If the `trustAllCertificates` value in the `dma.xml` file is set to false, you must have a subject alternate name (SAN) as part of your signed certificate:

- The SAN must be type IP.
- The SAN value must be the IP address—not the domain name—of the HP DMA server.

To set up the SAN, append `-ext SAN=ip:xx.xx.xxx.xxx` to the end of the `keytool` command, replacing `xx.xx.xxx.xxx` with the desired IP address.

The format of the `keytool` command that sets up SAN is:

/opt/hp/dma/server/jre/bin/keytool -genkeypair -alias <*keyalias*> -keyalg RSA -keysize 2048
-dname "CN=<*DMAserver*>,OU=<*orgunit*>,O=<*org*>,L=<*location*>,S=<*state*>,
C=<*country*>" -keypass <*password*> -keystore <*storefile*> -storepass <*password*>
-validity <numberdays> -ext SAN=ip:xx.xx.xxx.xxx

For additional information, see "Configure SSL on the HP DMA Server" in the *HP DMA Installation Guide*.

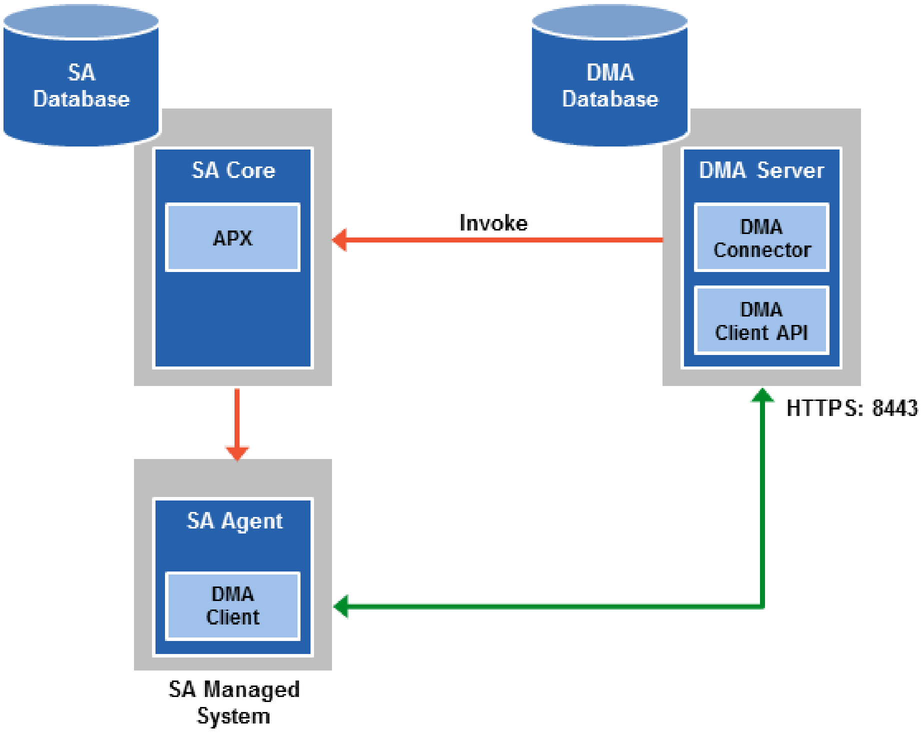
Note: The diagrams in this topic show simplified configurations of servers and communication paths. Real-world situations are much more complex with multiple SA Cores mapped to multiple SA Managed Servers. Multiple SA Satellites may also be configured.

For more information, see the technical white paper: *Configure HP DMA and SA to Use the SA Gateway Network as a Proxy Network*. This document is available on the HP Software Support web site: https://softwaresupport.hp.com/

Default HP DMA Communications

The following diagram shows how HP DMA communications work by default (without a proxy server):

1. HP DMA invokes SA to run the DMA Client on the target SA managed server.
2. SA communicates with the SA agent on the target server.
3. The SA agent invokes the DMA Client.
4. The DMA Client communicates with the DMA Server using HTTPS on port 8443.

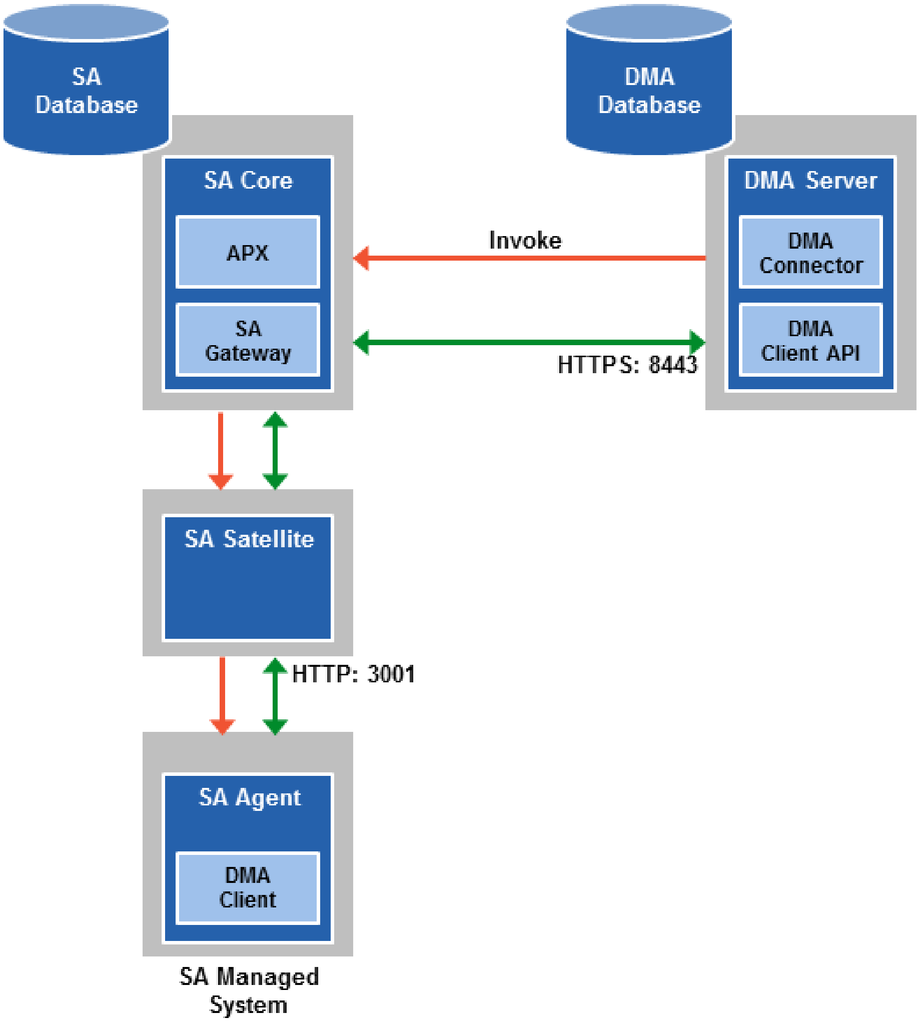


Using an SA Satellite as a Proxy Server

The following diagram shows how HP DMA communications work with an SA Satellite serving as a proxy:

1. HP DMA invokes SA to run the DMA Client on the target SA managed server.
2. SA communicates across the SA Satellite to the SA agent on the target server.
3. The SA agent invokes the DMA Client.
4. The DMA Client communicates using HTTPS via the SA Satellite proxy.

   In this case, the DMA Client uses the same port used by SA on the SA Satellite to forward information to the SA Gateway. The SA Gateway then forwards the information to the DMA Server.



How HP DMA Manages Proxy Communication

HP DMA uses two Custom Fields to control proxy communication:

- `west_proxy_address` contains the full URL of the proxy including the proxy port (or the keyword SA_auto_select).

> **Note:** Set the `west_proxy_address` to SA_auto_select if you want the target server to determine which SA Satellite to use as a proxy.

- `west_proxy_in_use` tells HP DMA whether a proxy server will be used. Valid values are:

TRUE	Use the proxy specified in the `west_proxy_address`
FALSE	Do not use a proxy
not set	Do not use a proxy, or defer to the organization or server level
anything else	Implies true

> **Tip:** It is best practice to only use values of TRUE, FALSE, and field not set. Note that `west_proxy_in_use` is not case-sensitive.

These Custom Fields can be defined at both the organization level and the server level. This enables you to use a proxy server for communication with some targets but not others—or use different proxy servers to communicate with different targets.

If the proxy Custom Fields are defined at both the organization level and the server level, the server level proxy information takes precedence over the organization level proxy information.

The following table shows how HP DMA will communicate if `west_proxy_in_use` has values at both the organization level and the server level.

Proxy Precedence	Server value is TRUE	Server value is FALSE	Server value is not set
Organization value is TRUE	Use the proxy specified for the server	Do not use a proxy for this server	Use the proxy specified for the organization
Organization value is FALSE	Use the proxy specified for the server	Do not use a proxy for this server	Do not use a proxy for this server
Organization value is not set	Use the proxy specified for the server	Do not use a proxy for this server	Do not use a proxy for this server

How to Set Up a Proxy Server

To set up a proxy server for HP DMA, you must make two changes to the HP DMA infrastructure:

1. Add a new EgressFilter rule to the SA Gateway configuration to allow forwarding to port 8443 on the DMA Server. This involves updating a configuration file that resides on the SA Core and restarting the SA Gateway.
2. If your SA Satellite environment uses SA realms, specify the `saRealm` connector parameter in the `dma.xml` configuration file.
3. Create and configure the two Custom Fields that instruct HP DMA to route traffic through the proxy server. This procedure is performed in the HP DMA UI.

Instructions for making each of these changes are provided here. For more information about the SA Satellite and SA Gateway, see the HP Server Automation documentation library, which is available on the HP Software Support web site:

https://softwaresupport.hp.com/

Configure the SA Core Gateway Properties

On the SA Core, add a new EgressFilter rule to the SA Gateway configuration of each slice within the SA Core to allow forwarding to port 8443 on the DMA Server. This procedure must be performed by an SA administrator.

> **Note:** An egress filter rule is only necessary on each slice within the same realm within the SA Core that the HP DMA Server is connected to. It is not required for any other SA Core, Satellite, or slices belonging to a different realm.

To add the new EgressFilter rule:

1. For every facility that is not a Satellite facility, perform the following steps to add a new `EgressFilter` entry to the gateway configuration file:

   a. Create or edit the gateway configuration file:

   `/etc/opt/opsware/opswgw-cgws1-<`*`REALM_NAME`*`>/opswgw.custom`

   > **Note:** SA customizations for the SA Core configurations must go in the `opswgw.custom` file. *`<REALM _NAME>`* is the name of the realm for the SA Core, and can be found in the `opswgw.properties` file (look for `opswgw.Realm=`*`<REALM_NAME>`*).

   b. Add the egress filter in the following form to the `opswgw.custom` file:

   `opswgw.EgressFilter=tcp:`*`<DMAServer>`*`:`*`<DMAPort>`*`:*:*`

Here *<DMAServer>* is the resolvable host name of your DMA Server and *<DMAPort>* is the port configured for DMA (default is 8443).

c. Save the file.

2. Restart the SA Gateway by using the following command:

```
/etc/init.d/opsware-sas restart opswgw-cgws
```

> **Caution:** Restarting the SA Gateway will disrupt traffic—be sure to restart it at a safe time.

3. If all slice Core Gateways have been restarted and if a load balancer gateway is used, then restart the load balancer gateway.

```
service opsware-sas restart opswgw-lgws
```

> **Caution:** The load balancer gateway must be restarted *after* all other gateways.

Specify the Server Automation Realm

When installed in a Satellite configuration, SA can manage servers with overlapping IP addresses. This situation can occur when servers are behind NAT devices or firewalls. Servers with overlapping IP addresses must reside in different SA realms.

If your environment uses SA realms, you must specify the `saRealm` connector parameter to enable HP DMA to correctly route traffic through the SA Gateway network.

> **Caution:** If you specify the `saRealm` parameter, you must specify the IP address (not the host name) of your HP DMA server in the `webServiceUrl` parameter.

> **Note:** To specify the SA realm while the HP DMA Server is being installed, perform these directions after baselining is completed.

To specify the SA realm:

1. Stop the DMA service: `service dma stop`
2. Open the `/opt/hp/dma/server/tomcat/conf/Catalina/localhost/dma.xml` file in a text editor.
3. Set the `saRealm` parameter:

```
<Parameter name="com.hp.dma.conn.sa.SAConnector.saRealm" value="<REALM_NAME>"/>
```

Here, *<REALM_NAME>* is the name of the realm of the SA core that the HP DMA server is connected to.

4. Specify the IP address of your HP DMA server in the `webServiceUrl` parameter:

   ```
   <Parameter name="com.hp.dma.core.webServiceUrl"
   value="https://<dmaIPaddress>:8443/dma"/>
   ```

   The `dma.xml` file should now look similar to this:

   ```
   <?xml version="1.0" encoding="UTF-8"?>
   <Context allowLinking="true" disableURLRewriting="true"
      path="/dma" privileged="true" swallowOutput="true"
      workDir="/var/opt/hp/dma/work/dma">
    <Valve className="org.apache.catalina.valves.AccessLogValve"
      directory="/var/log/hp/dma/" pattern="%h %l %u %t '%r' %s %b
      %S" prefix="localhost_access." suffix=".log"/>
    <Parameter name="com.hp.dma.core.webServiceUrl"
      value="https://192.0.2.0:8443/dma"/>
    <Parameter name="com.hp.dma.conn.trustAllCertificates" value="false" />
    <Parameter name="com.hp.dma.conn.sa.SAConnector.saRealm" value="REALM_NAME" />
    <Resource auth="container"
      driverClassName="oracle.jdbc.OracleDriver"
      factory="com.hp.dma.util.DmaTomcatContextHandler"
      maxActive="20" maxIdle="5" maxWait="2000" name="jdbc/dma"
      password="{AES}54dd1d97a915c4c3c8d0db986a1218db62008816fb924"
      type="javax.sql.DataSource"
      url="jdbc:oracle:thin:@dma1.mycompany.com:1521:DMA"
      username="dma"/>
   </Context>
   ```

5. Save the `dma.xml` file.

6. Start the DMA service:

   ```
   $ service dma start
   ```

Create and Configure the HP DMA Custom Fields

In the HP DMA web UI, create (if necessary) and configure the proxy communication Custom Fields.

You can specify proxy information for both organizations and individual servers. If both are specified, the server level proxy information takes precedence over the organization level proxy information (see Proxy Precedence).

To create and configure the Custom Fields to use proxy communication:

1. Decide whether your proxy is at the organization level or the server level.

   > **Note:** You can specify Custom Fields for both organizations and individual servers. If both are specified, the server level information takes precedence over the organization level information.

2. Go to Environment > Custom Fields to create the new Custom Fields at either the Organization or

Server level (alternatively, you can add Custom Fields when the organization or server is open in the Environment page):

- `west_proxy_in_use` with type List and options TRUE or FALSE
- `west_proxy_address` with type Text

3. Specify the Custom Field values at the organization level, the server level, or both (see Proxy Precedence):

   - Go to Environment > Dashboard > <*organization_name*> (*Optional:* > <*server_name*>)

     > **Note:** This must be performed by an HP DMA user who has a role with Write permission for the pertinent organizations (or Administrator capability).

     > **Tip:** If you do not see this Custom Field, be sure that **Show empty values** is selected.

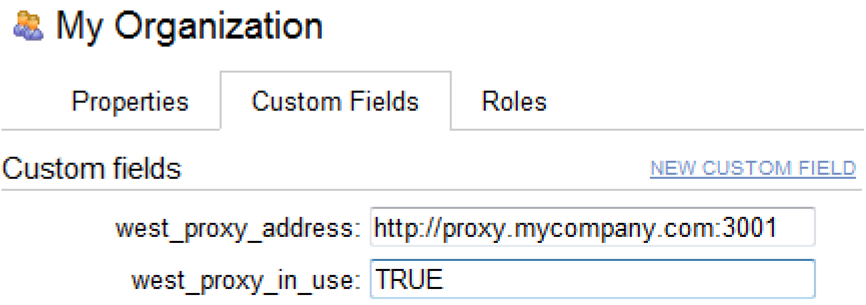
   - Set `west_proxy_address` to the full URL of the proxy, including the port, in this format:

     `http://<proxy_hostname>:<proxy_port>`

     > **Tip:** If you have multiple SA Satellites, and you want the target server to determine which SA Satellite to use as a proxy, set `west_proxy_address` to SA_auto_select.

   - Set `west_proxy_in_use` to TRUE, FALSE, or blank.

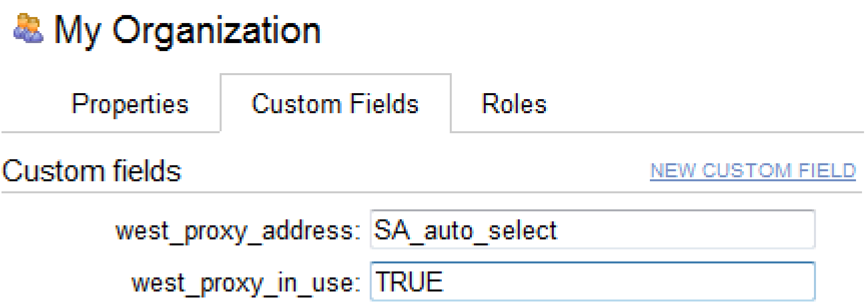
Example 1: Use a specific proxy server for all servers in an organization



west_proxy_address: http://proxy.mycompany.com:3001

west_proxy_in_use: TRUE

Example 2: Have the target server determine which SA Satellite to use as a proxy



west_proxy_address: SA_auto_select

west_proxy_in_use: TRUE

Note: You can easily adjust how the proxy server will be used. To stop using the proxy, simply set the value of `west_proxy_in_use` to FALSE. You do not need to delete the `west_proxy_address` value, because the `west_proxy_in_use` value controls whether or not the proxy is used.

Specify a Renamed Windows Administrator User

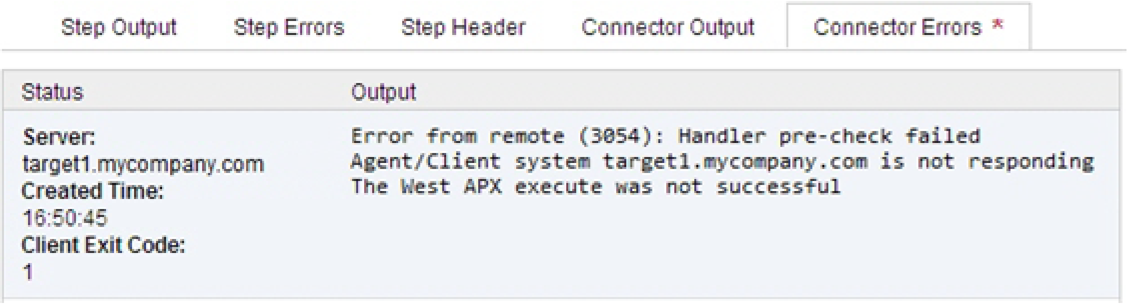
This topic shows you how to make changes necessary to accommodate Windows targets where the Windows Administrator user has been renamed.

There are two configuration changes required to accommodate these targets. These changes must be performed in the order shown.

Change Required	Where Performed	Number of Times Performed
Update the HP DMA Automation Platform Extension (APX) to allow non-default Windows Administrator user names. See Update the HP DMA APX.	On one SA Slice server	Only once
Create and configure a new HP DMA Custom Field that will be used to specify the Windows Administrator user name at either the organization or server level. See Create and Configure the HP DMA Custom Field.	In HP DMA	Once per relevant organization or server

Instructions for making each of these changes are provided here.

If you do not make these changes, any workflow executed against a Windows target where the Windows Administrator user has been renamed will be aborted, and the following connector error will be reported on the History page:



Status	Output
Server: target1.mycompany.com Created Time: 16:50:45 Client Exit Code: 1	Error from remote (3054): Handler pre-check failed Agent/Client system target1.mycompany.com is not responding The West APX execute was not successful

Update the HP DMA APX

Perform the following procedure only once on one SA Slice server.

> **Note:** The following steps must be performed by an SA user (<*SA_APX_User*>) who belongs to a group with the following SA privileges:
>
> - List, read, write, and execute permissions on the objects in the `/DMA_APX` folder.
> - OGSH permission to Launch Global Shell.
> - Manage Extensions (Read & Write) permission under Automation Platform Extension.
> - List, Read, and Write permission on the `/DMA_APX` folder.
>
> For more information about the SA permissions, see the HP Server Automation documentation library, which is available on the HP Software Support web site:
>
> https://softwaresupport.hp.com/

To update the HP DMA APX:

1. Open the `/DMA_APX` folder in the SA Library.
2. Double click Program Extension and select Update West Apx user on Windows.
3. On the Actions menu, select Run Program Extension.
4. Go to Run Program Extension > Program > Next.
5. Follow the instructions to List, Add, or Remove Windows Administrator users.
6. Select Start Job. The users will be listed, added, or removed according to the options that you selected.

Create and Configure the HP DMA Custom Field

The final change required is to create and configure an HP DMA Custom Field called `agent_username_win` that will contain the Windows Administrator user name for each Windows target server.

To create and configure the Custom Field:

1. Decide whether you want the Windows Administrator user name at the organization level or the server level.

   > **Note:** You can specify Custom Fields for both organizations and individual servers. If both are specified, the server level information takes precedence over the organization level

information.

2. Go to Environment > Custom Fields to create the new Custom Field at either the Organization or Server level (alternatively, you can add a Custom Field when the organization or server is open in the Environment page):

   `agent_username_win` with type Text

   Tip: If each Windows server has a different Windows Administrator user name, you will need to specify this user name for each server.

   If many Windows servers in the same organization have the same Windows Administrator user name, it will be more convenient to specify the user name at the organization level.

   You can create both organization and server level Custom Fields for this purpose. If you specify a value for both the organization and the server Custom Field, HP DMA will use the server value.

3. For each organization or server where you want to specify the Windows Administrator user name:

   Go to Environment > Dashboard > <*organization_name*> (*Optional:* > <*server_name*>) to specify the Windows Administrator user name in the `agent_username_win` Custom Field.

   Note: This must be performed by an HP DMA user who has a role with Write permission for the pertinent organizations (or Administrator capability).

   Tip: If you do not see this Custom Field, be sure that **Show empty values** is selected.

Note: If you want HP DMA to run workflows on Windows targets as a specific Windows domain user, also see Run as a Windows Domain User on the next page.

Run as a Windows Domain User

This topic shows you how to make the necessary changes to run workflows on Windows targets as a specific Windows domain user.

> **Note:** If you have a Windows 2012 server as a managed client, that system needs .Net 3.5 installed when you are running with a domain user configuration.

> **Note:** The specified domain user must:
>
> - Be a member of the Administrators group on the target server.
> - Have User Account Control (UAC) disabled on the target server.
> - Have login access to the pertinent database or middleware application (for example: SQL Server or IBM WebSphere Application Server) on the target server. This enables HP DMA to discover information about the target environment.

There are two methods to provide the Windows domain user and password:

- Configure Windows Domain User Using Custom Fields
- Configure Windows Domain User Using Runtime Parameters

Configure Windows Domain User Using Custom Fields

If you create and specify valid values for the following Custom Fields, all workflows executed against the pertinent targets will run as the Windows domain user that you specify:

- `domain_username_win`
- `domain_password_win`

  > **Note:** The value of `domain_password_win` is encrypted before it is stored.

To use this method, you must create and configure the new Custom Fields:

1. Decide whether you want the Windows domain user at the organization level or the server level.

   > **Note:** You can specify Custom Fields for both organizations and individual servers. If both are specified, the server level information takes precedence over the organization level information.

2. Go to Environment > Custom Fields to create the new Custom Fields at either the Organization or

Server level (alternatively, you can add Custom Fields when the organization or server is open in the Environment page):

- `domain_username_win` with type Text
- `domain_password_win` with type Password

> **Tip:** If each Windows server requires a different Windows domain user, you will need to specify this user name for each server.
>
> If many Windows servers in the same organization will use the same Windows domain user, it will be more convenient to specify the user name at the organization level.
>
> You can create both organization and server level Custom Fields for this purpose. If you specify a value for both the organization and the server, HP DMA will use the server value.

3. For each organization or server where you want to run workflows on Windows targets as a specific Windows domain user:

   Go to Environment > Dashboard > <*organization_name*> (*Optional:* > <*server_name*>) to specify values for the new Custom Fields.

   > **Note:** This must be performed by an HP DMA user who has a role with Write permission for the pertinent organizations (or Administrator capability).

   > **Tip:** If you do not see this Custom Field, be sure that **Show empty values** is selected.

> **Note:** If you have renamed the Windows Administrator account on your Windows target servers, you must also perform the procedures required to Specify a Renamed Windows Administrator User on page 72.

Configure Windows Domain User Using Runtime Parameters

You can specify the Windows domain user at the time you execute a deployment with runtime parameters.

> **Note:** When you use this method, the Windows domain user and password are not stored within HP DMA.

> **Tip:** This method is only available for SQL Server workflows.

To use this method, you must do the following for the pertinent workflow:

1. Find the workflow in the following table to identify the step where the Windows domain user runtime parameters are located (usually the step that gathers the advanced parameters):

Workflow	Step
MS SQL - Install Standalone SQL Instance	MS SQL - Advanced Parameters - Install Standalone
MS SQL - Install Clustered SQL Instance	MS SQL - Gather Advanced Parameters For Install Clustered SQL Instance
MS SQL - Add Node to Cluster	MS SQL - Advanced Parameters - Add Node to Cluster
MS SQL - Upgrade Standalone SQL Instance	MS SQL - Advanced Parameters - Upgrade Standalone
MS SQL Create Database	MS SQL Advanced Parameters Create Database
MS SQL Drop Database	MS SQL Parameters Drop Database
MS SQL - Install Patch	MS SQL - Advanced Parameters - Install Patch
MS SQL Rollback Patch	MS SQL Gather Advanced Parameters for Rollback Patch
Backup and Restore MS SQL Database	Gather Advanced Parameters for MS SQL Database Backup and Restore
Backup MS SQL Database	Gather Advanced Parameters for MS SQL Database Backup
Restore MS SQL Database	Gather Advanced Parameters for MS SQL Database Restore
MS SQL - Compliance Audit	Gather Advanced Parameters for MS SQL Compliance
DB Release for SQL Server	MS SQL - Parameters - DB Release for SQL Server
Discovery	Discover SQL Databases

2. When you make a copy of the workflow, expand the step, and then set the Windows domain user parameters to **- User selected -**.

   > **Note:** The pertinent parameters are based on the solution type:

Provisioning	Installer Account Installer Password
Patching, refresh, compliance, and release management	Instance Account Instance Password
Discovery	SQL Instance Account SQL Instance Password

3. When you create a deployment from the copy of the workflow, set the parameter types to **Runtime Value**.
4. When you execute the deployment, specify the Windows domain user name and password for the parameters.

Note: If you have renamed the Windows Administrator account on your Windows target servers, you must also perform the procedures required to Specify a Renamed Windows Administrator User on page 72.

Change the Number of Active Connections

This topic shows you how to change the number of active database connections that HP DMA uses. This may improve workflow execution speed, depending on how many workflows are running at the same time and the complexity of those workflows.

To change the number of active connections:

1. As root, stop the HP DMA server:

   ```
   $ service dma stop
   ```

2. Open the following file in a text editor:

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

3. Modify the following parameters:

Parameter Name	Default Value	Suggested New Value
maxActive	20	50
maxWait	2000	3000

   The parameter values that will work best are highly dependent on your environment. Several iterations may be required to optimally tune these parameters.

4. Start the HP DMA server again:

   ```
   $ service dma start
   ```

Chapter 3: Reference Information

This chapter contains the following information:

Topic	Description
HP Software Documentation	Links to additional HP DMA documentation.
HP DMA Baseline Options	The complete list of all the `dmaBaselineData.sh` options.
About the SA Client	What the SA Client looks like and how to download it from the SA server.
Workflow Execution ScripT	Information about the WEST program and how to terminate it, if necessary.

HP Software Documentation

HP Database and Middleware Automation Documentation

The following documents are included in the HP DMA documentation library:

- *HP DMA Installation Guide*
- *HP DMA Troubleshooting Guide* (this document)
- *HP DMA Administrator Guide*
- *HP DMA User Guide*
- *HP DMA Quick Start Tutorial*
- *HP DMA Concepts Guide*
- *HP DMA Release Notes*
- *HP DMA Support Matrix*
- *HP DMA Solution Pack User Guides*

The latest versions of these documents are available on the HP Software Support web site:

https://softwaresupport.hp.com/

HP DMA API Reference WebHelp is available on all HP DMA Servers at:

```
https://<DMA_SERVER>:8443/dma/api
```

Here, *<DMA_SERVER>* is the fully qualified host name of your HP DMA server.

HP Server Automation Documentation

The latest versions of SA documents are available on the HP Software Support web site:

https://softwaresupport.hp.com/

HP Live Network connector Documentation

The following documents are included in the HP Live Network connector documentation library:

- *HP Live Network connector User Guide*
- *LNc Release Notes*

The latest versions of these documents are available on the HP Live Network web site:

1. Go to the following HP Live Network connector page:

   https://hpln.hp.com/group/hp-live-network-connector

2. Click the RESOURCES link.
3. Open Resources.
4. Open the Documentation folder.
5. Download the latest version of the documents.

Note: You must sign in to HP Live Network using your HP Passport credentials. (See Support on page 4 for more information about obtaining an HP Passport account.)

HP DMA Baseline Options

The following table gives a complete list of all the `dmaBaselineData.sh` options:

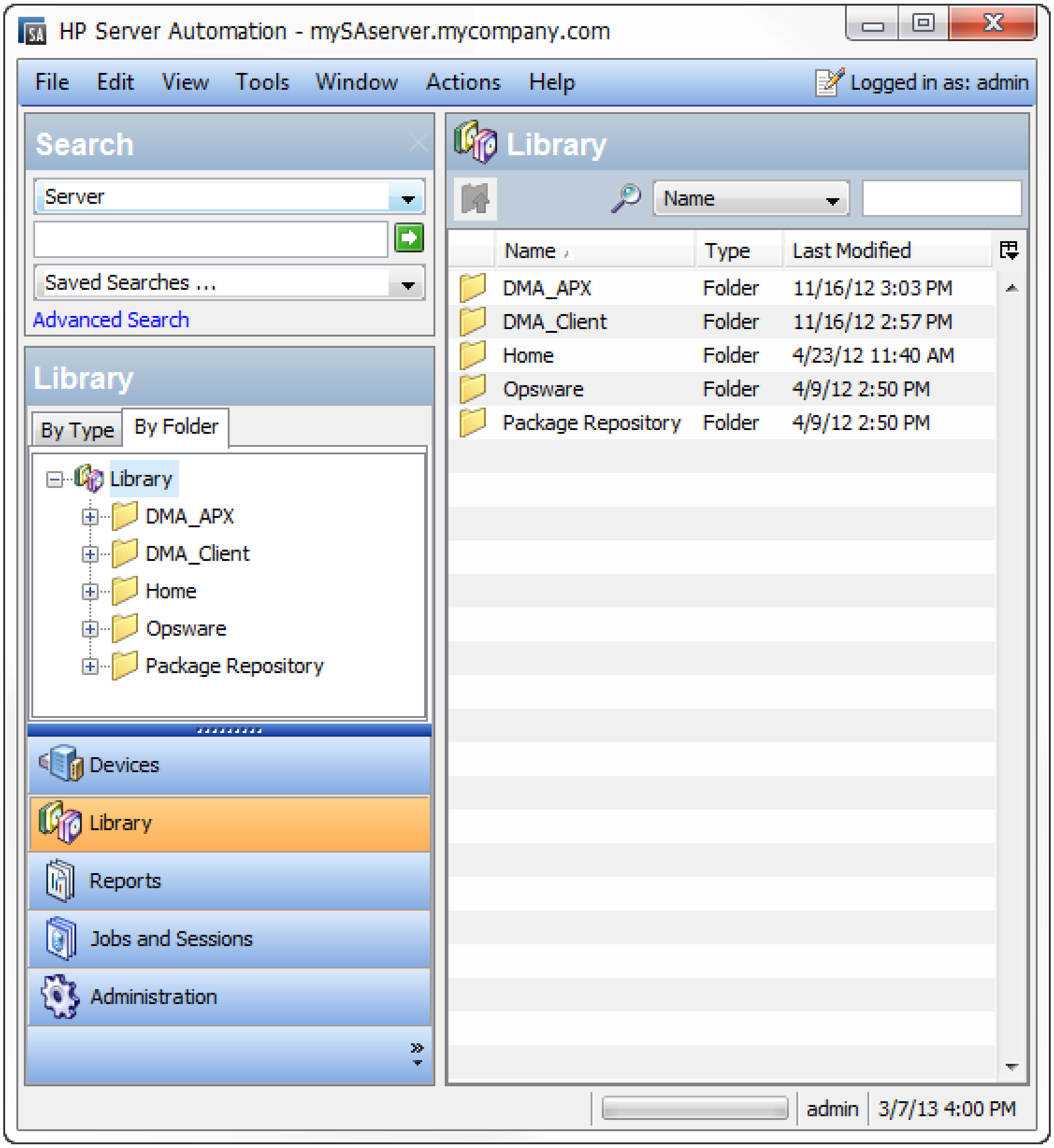
Option	Example Argument Value	Description
-?,--help		Print this usage message.
-c,--create-tables		Create tables for database.
-cc,--create-context		Create a context file with the specified settings.
-context,--deployed-context-file <*dma.xml*>	dma.xml	Fully qualified path to the deployed context file to get database connection settings.
-dbh,--database-hostname <*arg*>	oracle.mycompany.com	The database host name for the Java Database Connectivity (JDBC) connection.
-dbp,--database-port <*arg*>	1521	The database port for the Java Database Connectivity (JDBC) connection.
-dbpw,--database-password <*dbpasswordValue*>	dbpassword	The password used to connect to the database.
-dbs,--database-sid <*arg*>	dma	The database SID for the Java Database Connectivity (JDBC) connection.
-dbts,--database-tablespace <*arg*>	/u01/app/oracle/oradata/dma	The base directory for the database tablespace creation.
-dbtype,--database-type <*arg*>	oracle	(optional) The underlying database type. The default is oracle.
-dbu,--database-username <*dbusernameValue*>		The username used to connect to the database.

Option	Example Argument Value	Description
-dmah,--dma-hostname *<dmahostnameValue>*	dma.mycompany.com	Set the fully qualified host name of the HP DMA server. **Note:** If this value is not specified, the default is the server where the script is running.
-e,--erase		Erase existing data and add baseline data. **Caution:** Do not do this unless instructed to by HP Support.
-jdbccs,--jdbc-connection-string *<connectionString>*	jdbc:<*DBTYPE*>:thin:@<*HOST*>:<*TNS_PORT*>:<*SID*> or jdbc:<*DBTYPE*>:thin:@//<*HOST*>:<*TNS_PORT*>/<*ORACLE_SERVICE_NAME*>	The Java Database Connectivity (JDBC) Connection String used to connect to the database. The default <*TNS_PORT*> is 1521. **Note:** Other connection string syntax is possible. Consult your Oracle DBA for the company standard.
-okeys,--overwrite-keys		Overwrite public and private key in the database if they exist **Caution:** Do not do this unless instructed to by HP Support.
-privkey,--private-key-file *<privateKeyFilename>*		File containing the private key.
-pubkey,--public-key-file *<publicKeyFilename>*		File containing the public key.
-sahostname,--server-automation-hostname *<sahostnameValue>*	saserver.mycompany.com	The fully qualified host name of the SA server.

Option	Example Argument Value	Description
-sapassword,--server-automation-password <*sapasswordValue*>		The password used to connect to SA.
-sausername,--server-automation-username <*sausernameValue*>		The username used to connect to the SA.
-sqlfile,--baseline-sqlfile <*baselineSQLfile*>		The baseline file containing SQL insert statements
-t,--test		Test the underlying database connection.

About the SA Client

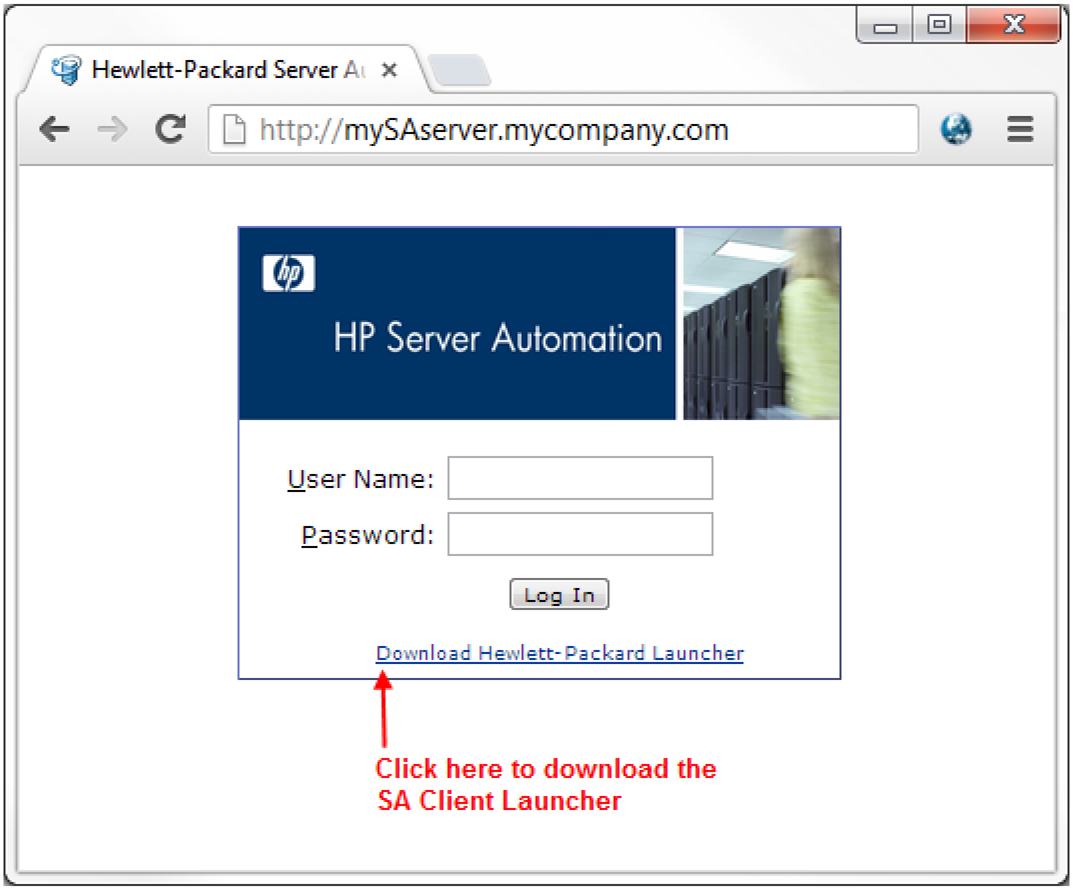
The SA Client is a powerful Java client for the HP Server Automation System. It provides the look-and-feel of a Microsoft Windows desktop application with the cross-platform flexibility of Java.



Name	Type	Last Modified
DMA_APX	Folder	11/16/12 3:03 PM
DMA_Client	Folder	11/16/12 2:57 PM
Home	Folder	4/23/12 11:40 AM
Opsware	Folder	4/9/12 2:50 PM
Package Repository	Folder	4/9/12 2:50 PM

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:


Hewlett-Packard Server A
http://mySAserver.mycompany.com
HP Server Automation
User Name:
Password:
Log In
Download Hewlett-Packard Launcher
Click here to download the
SA Client Launcher

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/

Workflow Execution ScripT

Each HP DMA target uses a program called Workflow Execution ScripT (WEST) to communicate with the HP DMA server. WEST does the following things:

- Executes workflow steps
- Provides the output (stdout, stderr, return code, and end time) for a specific step's execution

WEST is installed on each target server when you attach and remediate the DMA Client Files software policy on that target .

Under certain circumstances, you may need to manually terminate WEST on a target server. This would be necessary, for example, if the HP DMA server name was specified incorrectly when the `dmaBaselineData` command was executed, and a workflow execution was subsequently attempted (see HP DMA Client Fails to Contact HP DMA Server on page 18).

To terminate WEST on UNIX targets:

1. Find the process ID for the HP DMA client:

   ```
   ps - ef | grep west
   ```

2. Kill that process.

To terminate WEST on Windows targets:

1. In the Windows Task Manager, go to the Processes tab.
2. Sort the processes by Image Name.
3. Find the `java.exe` process whose Location is as follows:

   ```
   <install_dir>\HP\DMA\Client\jre1_7\bin
   ```

   By default on Windows Server 2008 R2, for example, this is:

   ```
   C:\Program Files\HP\DMA\Client\jre1_7\bin
   ```

   To determine the Location of a process, right-click the process Image Name, and select **Properties**.

4. Right-click the pertinent `java.exe` process, and select **End Process**.