Hewlett Packard Enterprise

HPE Database and Middleware Automation

Ultimate Edition

Software Version: 10.40
Linux, Solaris, AIX, and HP-UX

Installation Guide

Document Release Date: December 2015
Software Release Date: December 2015

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. HPE 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 HPE 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

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

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 **the Register** link at the top of the HPE Software Support page.

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

Support

Visit the HPE 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 HPE Software offers.

HPE 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 HPE 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 HPESW Solution and Integration Portal Web site. This site enables you to explore HPE Product Solutions to meet your business needs, includes a full list of Integrations between HPE 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**

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

Installing

This section provides information on installing HPE DMA.

Topics	Description
"System Requirements" below	Lists prerequisites for installing HPE DMA.
"Installing the HPE DMA" on page 15	Provides step by step instructions for installing HPE DMA.
"Upgrading to HPE DMA 10.40" on page 30	Provides step by step instructions for upgrading HPE DMA.
"Integrating HPE DMA with HP SA" on page 34	Provides information about HP SA integration.
"Silent Installation" on page 46	Provides information on automated installation for basic use cases.
"Uninstalling the HPE DMA" on page 57	Provides step by step instructions for uninstalling HPE DMA.

System Requirements

You must meet the following requirements before you can install HPE DMA 10.40.000.000.

Topic	Description
"Installation Media Contents" below	Description of the contents of the HPE DMA 10.40.000.000 installation media.
System Requirements	List of required products, platforms, hardware, and software .
Sizing Recommendations	Information about the minimum recommended CPU count, RAM, and disk space for the HPE DMA server and the HPE DMA database server.
"Obtaining a Signed Server Certificate"	Information about obtaining a server certificate signed by a trusted Certificate Authority.
"Configuring the Oracle Database" on page 12	Description of how the Oracle Database needs to be configured before it can be used by HPE DMA 10.40.000.000.
"Configuring the PostgreSQL Database" on page 14	Description of how the PostgreSQL Database needs to be configured before it can be used by HPE DMA 10.40.000.000.

Installation Media Contents

The HPE DMA 10.40.000.000 installation media—zipped folder. When you download the zipped folder, unzip the folder, and extract the contents, you will see contains the following folders and files:

Folder Name	Description
Top level folder	
readme.txt	Instructions and information about files on the media.
DMA_10.40.000.000_Open_ Source_ Licenses.zip	This file contains the license agreements for the Open Source software used by HPE DMA.
DMA_10.40.000.000_Server_and_Client folder	
dma-server-10.40.000.000-0.x86_ 64.rpm	The rpm file that will install the HPE DMA 10.40 server.
dma-sa-client-10.40.000.000-0.x86_ 64.rpm	The rpm file that will install the HPE DMA 10.40 client that enables HPE DMA to integrate with HP Server Automation (SA).
Discovery.zip	Solution pack containing workflows that you can use to discover: • Oracle, SQL Server, Sybase, and DB2 databases on target servers. • IBM WebSphere, Oracle Weblogic, and JBoss middleware applications on target servers.
Promote.zip	Solution pack containing workflows that you can use to promote HPE DMA workflows (and related automation items) from a source HPE DMA server to a destination HPE DMA server.
DMA_10.40.000.000_Documentation folder	
buildinfo.txt	Information about how the installation media was constructed
DMA_10.40.000.000_ Installation_ Guide.pdf	HPE DMA Installation Guide—this document
DMA_10.40.000.000_ Planning_ Guide.pdf	HPE DMA Planning Guide
DMA_10.40.000.000_ Release_ Notes.pdf	HPE DMA Release Notes
DMA_10.40.000.000_ Support_Matrix.pdf	HPE DMA Support Matrix
DMA_10.40.000.000_Open_ Source_ Third_Party_ Licenses.pdf	HPE DMA Open Source and Third-Party Software License Agreements
DMA_10.40.000.000_Database_Solution_Packs folder	
AdvancedDBPatching.zip	Tools that you can use to automate Oracle Database patching CRS or Grid Home, RAC Home, CRS Patchset, Grid Standalone Patch, and Standalone Grid.
AdvancedDBProvisioning.zip	Tools that you can use to automate Oracle Database provisioning, including CRS, ASM, RAC, and Dataguard.

DBCompliance.zip	Tools that you can use to audit your database environment for compliance with a specific security benchmark— for Oracle, MS SQL, Sybase, and DB2 databases.
DBPatching.zip	Tools that you can use to patch database components in an efficient, automated way—for Oracle, SQL Server, Sybase, and DB2 databases.
DBProvisioning.zip	Tools that you can use to create and install new databases—for Oracle, SQL Server, Sybase, and DB2 databases.
DBRefresh.zip	Tools that you can use to move the contents of a database. For Oracle databases you can use RMAN or Data Pump. For SQL Server databases you can backup and restore. For Sybase Databases you can dump and load.
DBReleaseManagement.zip	Tools that you can use to update any schema, data, server configuration, or security settings—for Oracle, SQL Server, and Sybase databases.
DMA_10.40.000.000_Middleware_Solution_Packs folder	
ASConfigManagement.zip	Tools that you can use to manage the configuration of application servers, including clusters, data sources, and web servers—for IBM WebSphere—and to configure data sources—for JBoss.
ASPatching.zip	Tools that you can use to automate the process of applying fixes and updates to application servers—for IBM WebSphere and Oracle WebLogic.
ASProvisioning.zip	Tools that you can use to automate the process of installing application servers—for IBM WebSphere, Oracle WebLogic, and JBoss.
ASReleaseManagement.zip	Tools that you can use to automate the process of deploying an application file or a web archive file (.war or .ear) within the application server—for IBM WebSphere and JBoss.
DMA_10.40.000.000_Install folder	
dma_install.sh install-options.txt installhelperscript.sh	Tools that automate the installation of HPE DMA.
readme.txt	Instructions and information about files on the media.
dma_remove.sh remove-options.txt removehelperscript.sh	Tools that automate the removal of HPE DMA.
DMA_Express_10.40_Edition	
DMA_Express_10.40_Client_Solution_ Pack (also known as DMA Runtime)	Includes all of the HPE DMA Express flows for the DMA Express Client
DMA_Express_10.40_Database_ Content_Pack	Includes all of the HPE DMA Express flows for databases

DMA_Express_10.40_ Documentation	Includes the HPE DMA Express User Guide and HPE DMA Express Support Matrix
DMA_Express_10.40_ Middleware_ Content_Pack	Includes all of the HPE DMA Express flows for Middleware
DMA_Express_10.40_Util_ Content_ Pack	Includes a set of utilities for use with HPE DMA Express Edition
DMA_Express_10.40_Open_ Source_ Licenses.zip	Includes all of the HPE DMA Express Open Source license information
readme.txt	Instructions and information about files on the media.

For more information, refer to HPE DMA documentation provided under DMA_Express_10.40.000.000folder in the installation or access the most recent version from https://softwaresupport.HPE.com.

Tip: Always check to see if there are more recent HPE DMA patches available online. Due to frequent releases, it is possible that the files provided on the HPE DMA 10.40.000.000 installation media have since been updated.

To obtain the recent HPE DMA patch:

1. Go to the following web site: https://softwaresupport.hp.com/
2. Sign in using your HPE Passport credentials.
3. Your dashboard experience is based on your SAID. Under My Products, select database and middleware automation.
4. Look under Software Patch to determine whether a more recent patch is available.
5. If there is a more recent patch, select the following:
   Product: Database and Middleware Automation

   Version: Your desired version (or do not specify to view all versions)

   Document Type: Manuals

Refer these documents for your convenience:

- Documentation Library—Provides links to all HPE DMA documents available for the release.
- All Manuals Download—A ZIP file containing all HPE DMA documents available for the release.

Obtaining a Signed Server Certificate

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

Tip: Make sure you check your company's security policy for the correct procedure.

To obtain a signed certificate, you must generate a certificate signing request for your HPE DMA server and submit it to your CA. The CA will send you a digitally signed certificate via email. You can then import the signed certificate into the keystore. (See "Configuring SSL on the HPE DMA Server" on page 23 for more information.)

Configuring the Oracle Database

This section describes how to create and configure the Oracle database that will be used by HPE DMA 10.40.000.000.

You need a username and password for this Oracle database.

Have your database administrator (DBA) create an Oracle Database Enterprise Edition database to be used by HPE DMA. Make sure the Oracle Listener and database are up and running.

Depending on how your company manages Oracle Database, do one of the following things:

- Have your DBA create the Oracle Instance and the two tablespaces.
- Perform the Steps to Configure the Oracle Database documented below.

Your Oracle Database database must be up and running before installing HPE DMA.

Steps to Configure the Oracle Database

This section shows you how to configure an Oracle database that will be used by HPE DMA 10.40.000.000.

Note: If you use the automated installation process, you do not need to follow the instructions in this section.

In the commands that follow, replace the variables (found within <>'s) with values appropriate for your environment:

Variable	Example	Description
<*database_username*>	dma	Oracle database username
<*database_password*>	myOraclePassword	Oracle database password
<*Oracle_SID*>	dma	Oracle Database Instance
<*DMA_data_file*>	`/u01/app/oracle/oradata/dma/dma_data1.ora`	Fully qualified path to the `hpdma_data` file
<*file_size*>	100	File size in MB, a number from 1 to 10000
<*DMA_indx_file*>	`/u01/app/oracle/oradata/dma/dma_indx.ora`	Fully qualified path to the `hpdma_indx` file

On your Oracle Database system, perform the following steps:

1. Connect to the Oracle database and create new table spaces for data file and index file. HPE DMA uses the default table space `hpdma_data` and `hpdma_indx` if new table spaces are not created.

   For a full description of all the baseline options, see "HPE DMA Baseline Options" on page 20.

   > **Tip:** Consult your DBA on the autoextends options.

   - In most cases run this command: `sqlplus / as sysdba`
   - If you have multiple databases set up with remote authentication configured, run the following command instead: `sqlplus /@<Oracle_SID> as sysdba`

   ```
   create tablespace <data-tablespace_name> datafile '<DMA_data_file>' size
   <file_size>M autoextend on;
   create tablespace <index-tablespace_name> datafile '<DMA_indx_file>' size
   <file_size>M autoextend on;
   exit;
   ```

2. If you do not already have an existing user, create the user, and give the user permissions. For example:

   ```
   create user <database_username> identified by <database_password> default tablespace
   hpdma_data;
   grant connect,resource to <database_username>;
   grant create public synonym to <database_username>;
   ```

   > **Tip:** If the database password changes in the future, see Oracle Database Password Changed.

   > **Tip:** If you prefer restrictive privileges to the <*database_username*>, you can grant only connect but not the resource.

3. If you are using Oracle 12c or not granted RESOURCE role, execute the following commands:

   ```
   alter user <database_username> quota <file_size>M on <data-tablespace_name>;
   alter user <database_username> quota <file_size>M on <index-tablespace_name>;
   ```

   Alternatively, if you prefer to use a <database_role> pertaining to the DMA product, execute the following command:

   ```
   Grant UNLIMITED TABLESPACE to <database_role>
   ```

4. Start the TNS listener after creating the database.

Configuring the PostgreSQL Database

This section describes how to create and configure the PostgreSQL database that will be used by HPE DMA 10.40.000.000.

You need a username and password for this PostgreSQL database.

Have your database administrator (DBA) create a PostgreSQL 9.3.5 database to be used by HPE DMA. Make sure the PostgreSQL service and database are up and running.

Depending on how your company manages PostgreSQL database, do one of the following things:

- Have your DBA create the PostgreSQL Instance and the two tablespaces.
- Perform the Steps to Configure the PostgreSQL Database documented below.

Your PostgreSQL database must be up and running before installing HPE DMA.

Steps to Create and Configure the PostgreSQL Database

This section shows you how to configure a PostgreSQL database that will be used by HPE DMA 10.40.000.000.

In the commands that follow, replace the variables (found within <>'s) with values appropriate for your environment:

Variable	Example	Description
<*database_username*>	dma	PostgreSQL database username
<*database_password*>	myPostgreSQLPassword	PostgreSQL database password
<*database_name*>	dma	PostgreSQL Instance
<*DMA_data_file*>	`/home/data`	Fully qualified path to the `hpdma_data` file
<*DMA_indx_file*>	`/home/data`	Fully qualified path to the `hpdma_indx` file

On your PostgreSQL system, perform the following steps:

1. Connect to the PostgreSQL database and create the `hpdma_data` and `hpdma_indx` tablespaces.
   - Run the `psql` command to connect to the sql prompt.
   - If you have multiple databases set up with remote authentication configured, run the following command instead: `psql <database name>` as sysdba.

   ```
   CREATE TABLESPACE tablespace_name [OWNER user_name] LOCATION 'directory'
   ```

   Example: `CREATE TABLESPACE hpdma_data [ OWNER postgres ] LOCATION '/home/data'`

Installing the HPE DMA

This section contains the following topics and should be performed in order:

Topic	Description
"Installing the HPE DMA Server"	Step-by-step instructions about how to install the DMA server.
"Configuring SSL on the HPE DMA Server"	Step-by-step instructions about how to configure SSL on the DMA server.
"Installing the HPE DMA Client for SA"	Step-by-step instructions about how to install the DMA client.
"Integrating HPE DMA with HP SA"	Step-by-step instructions about how to integrate DMA with HP Server Automation. These steps should be performed by the SA administrator.
Start HPE DMA	Directions to start DMA.
Set Up HPE DMA	General information about how to use DMA to set up the connector, roles, capabilities, and targets, and to import a solution pack.

Note: An automated script is available that can speed up the installation process. For information about this script, see "Automated HPE DMA Installation".

Installing the HPE DMA Server

This stage shows you how to install the HPE DMA server.

> **Note:** If you use the automated installation process, you do not need to follow the instructions in this section. See the "Silent Installation" on page 46 section for instructions.

In the commands that follow, replace the variables (found within <>'s) with values appropriate for your environment:

Variable	Example	Description
<database_ username>	dma	Oracle Database/PostgreSQL username—must be the same username that you used when you created your Oracle database/PostgreSQL in "Configuring the Oracle Database" on page 12 "Configuring the PostgreSQL Database" on page 14
<database_ password>	myOraclePassword	Oracle Database/PostgreSQL password—must be the same password that you used when you created your Oracle/PostgreSQL database in Steps to "Configuring the Oracle Database" on page 12Create and Configure the Oracle Database / "Configuring the PostgreSQL Database" on page 14
<DMA_server>	dma.mycompany.com	Fully qualified host name of the HPE DMA server **Note:** This cannot be `localhost`.
<Oracle_SID>	dma	Oracle Database Instance—must be the same instance that you used when you created your Oracle database in "Configuring the Oracle Database" on page 12
<database_name>	dma	PostgreSQL instance—must be the same instance that you used when you created your PostgreSQL database in "Configuring the PostgreSQL Database" on page 14

<*Oracle_ Server*>/<*PostgreSQL server*>	oracle.mycompany.com	Fully qualified host name of the Oracle Database/PostgreSQL server—must be the same server that you used when you created your Oracle/PostgreSQL database in "Configuring the Oracle Database" on page 12 "Configuring the PostgreSQL Database" on page 14 **Note:** This cannot be `localhost`.
<*jdbc_string*> (Oracle)	`jdbc:oracle:thin:@ oracle.mycompany.com: 1521:dma`	Java Database Connectivity (JDBC) connection string in the following format: `jdbc:oracle:thin:@<`*`Oracle_ Server`*`>: 1521:<`*`Oracle_SID`*`>` Other connection string syntax is possible. Consult your Oracle DBA for the company standard.
<*jdbc_string*> (PostgreSQL)	`jdbc:postgresql:// postgres.mycompany.com:5432/postgres`	`jdbc:postgresql://<postgres_ server_name>:5432/<database_ name>`
<*SA_Server*>	saserver.mycompany.com	Fully qualified host name of the Server Automation server

On your Red Hat Enterprise Linux HPE DMA server (<*DMA_server*>), perform the following tasks:

1. Obtain the `dma-server-10.40.000.000-0.x86_64.rpm` file from the HPE DMA installation media under the DMA_10.40.000.000_Server_and_Client folder.
2. Run the following commands as root to install the HPE DMA server:

   ```
   $ cd DMA_10.40.000.000_Server_and_Client
   $ rpm -ivh dma-server-10.40.000.000-0.x86_64.rpm
   ```

   Note: Only run the installation command one time.

3. Baseline your database. This will create your schema and put the database into the default state. Run the following commands as root. For example:

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

   Note: Replace the arguments in the following command with values appropriate for your environment. For readability, the options are listed on separate lines—you must build the command

> in a single line. If you cut and paste from this PDF, make sure that the dashes (--) copy correctly.
>
> For a full description of all the baseline options, see "HPE DMA Baseline Options" on page 20.
>
> This command does not baseline the connector. You will configure the connector later (see Configure the Connector).

Baseline your database for Oracle by performing the following:

```
$ sh ./dmaBaselineData.sh --create-tables
--create-context
--database-username <database_username>
--database-password <database_password>
--jdbc-connection-string <jdbc_string>
--dma-hostname <DMA_server>
--tablespace-data <data-tablespace_name>
--tablespace-indx <index-tablespacefile_name>
```

Use the `--tablespace-data` and `--tablespace-indx` options if you created table space data file and index file other than the default `hpdma_data` data file and `hpdma_indx` index file.

> **Note:** If you receive an error, see Troubleshooting.

Baseline your database for PostgreSQL by performing the following:

```
$ sh ./dmaBaselineData.sh --create-tables
--create-context
--database-username <database_username>
--database-password <database_password>
--jdbc-connection-string <jdbc_string>
--dma-hostname <DMA_server>

--database-type postgres
```

4. On your HPE DMA server, run the following script command to copy the required JAR files from the SA server to the HPE 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.

> **Note:** You have completed installing the initial stage—the command line setup—of the HPE DMA server.
>
> In the next stage you will configure SSL on the HPE DMA server.

Starting the HPE DMA

The first time you start HPE DMA you must log in as the default initial HPE DMA administrator (`dma_initial_admin`) to configure the operating environment.

1. As root, start the DMA 10.40.000.000 server. For example:

   ```
   $ service dma start
   ```

2. Use a web browser to connect to the HPE DMA server:

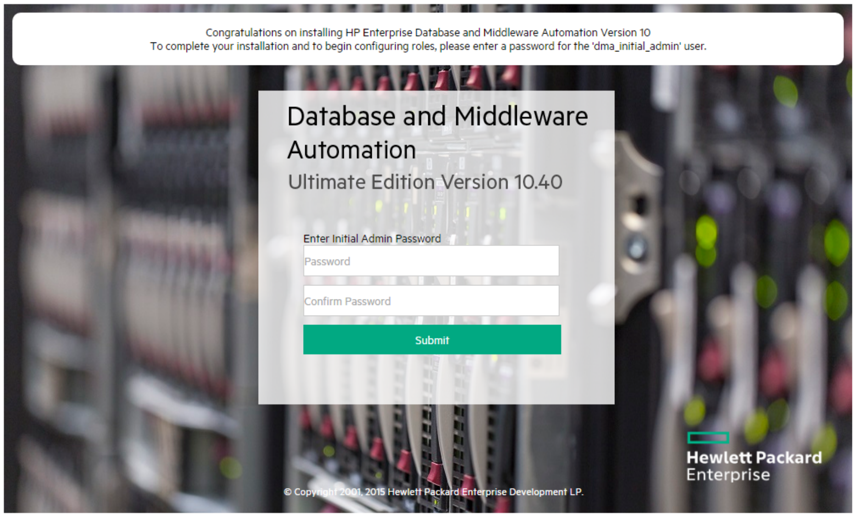
   `https://<DMA_Server>:8443/dma`

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

   > **Note:** If you use the Internet Explorer browser and cannot log in, see Login Errors.

3. Accept the certificates.

   You will see the following page:



Congratulations on installing HP Enterprise Database and Middleware Automation Version 10
To complete your installation and to begin configuring roles, please enter a password for the 'dma_initial_admin' user.

Database and Middleware Automation
Ultimate Edition Version 10.40

© Copyright 2001, 2015 Hewlett Packard Enterprise Development LP.

4. Enter an initial password for the dma_initial_admin user, retype the password, and then click **Submit**.
5. To log in, enter `dma_initial_admin` for the username, enter the new password for the password, and then click **Login**.

If you enter incorrect credentials 1-4 times	You will receive the message: Credentials are incorrect or do not allow login.
If you enter incorrect credentials 5 times	You will receive the message: Max Number of logins attempted. Locking account.
If you enter incorrect credentials more than 5 times	The account will be locked for one hour and you will receive the message: Account is locked.

> **Note:** Next you will perform the initial HPE DMA setup using the HPE DMA user interface.

HPE 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, that can resolve into either an IPv4 or IPv6 address.
-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.
-dmah,--dma-hostname <*dmahostnameValue*>	dma.mycompany.com	Set the fully qualified host name of the HPE DMA server, that can resolve into either an IPv4 or IPv6 address. **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 HPE Support.
-jdbccs,--jdbc-connection-	jdbc:<*DBTYPE*>:thin:@	The Java Database Connectivity (JDBC)

Option	Example Argument Value	Description
string <*connectionString*>	<*HOST*>:<*TNS_PORT*>:<*SID*> or jdbc:<*DBTYPE*>:thin:@//<*HOST*>:<*TNS_PORT*>/<*ORACLE_SERVICE_NAME*>	Connection String used to connect to the database. The default <*TNS_PORT*> is 1521. 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 HPE 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, that can resolve into either an IPv4 or IPv6 address.
-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.
-tsda,--tablespace-data <*datafile_name*>		The baseline option to specify data file table space name.
-tsin,--tablespace-indx <*indexfile_name*>		The baseline option to specify data index table space name.

Installing the HPE DMA Client for SA

This stage shows you how to install the HPE DMA Client for SA on the HPE DMA server.

Note: If you use the automated installation process, you do not need to follow the instructions in this section.

Note: The HPE DMA Client for SA is used to create an HPE DMA software policy in Server Automation (SA). This needs to be done once per SA mesh.

On the HPE DMA server, get the `dma-sa-client-10.40.000.000-0.x86_64.rpm` file from the HPE DMA installation media under the `DMA_10.40.000.000_Server_and_Client` folder, and then run the following commands as root:

```
$ cd DMA_10.40.000.000_Server_and_Client
```

```
$ rpm -ivh dma-sa-client-10.40.000.000-0.x86_64.rpm
```

Note: You have completed installing the HPE DMA Client for SA.

In the next stage you will integrate HPE DMA with Server Automation.

For information about integrating HPE DMAwith HP Server Automation, see "Integrating HPE DMA with HP SA" on page 34.

Configuring SSL on the HPE DMA Server

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

1. "Generating a Private Key for the Server" below
2. "Generating the Certificate Signing Request to Obtain Signed Server Certificates" on the next page
3. "Importing the SSL Server Certificates" on page 25
4. "Configuring the HPE DMA Server to Use Your Certificate" on page 27
5. "Verifying the SSL Connection" on page 29

For a production environment, you should have the server certificate signed by a trusted Certificate Authority (CA).

Note: For testing purposes—not for a production environment—you may be able to use a self-signed server certificate.

Caution: If you are using an SA gateway infrastructure as a proxy network, 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 HPE DMA server.

For detailed instructions and an example of the `keytool` command that sets up the SAN, see .

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

About the keytool utility

Many procedures in this section use the `keytool` utility, which is located in the following directory on the HPE DMA server:

```
/opt/hp/dma/server/jre/bin
```

Caution: To follow the procedures in this document as written, add `/opt/hp/dma/server/jre/bin` to your path before executing the `keytool` command.

Run the following command to verify which `keytool` will be used:

```
which keytool
```

Generating a Private Key for the Server

The first step in configuring SSL on the HPE DMA server is to generate a private key for that server. You can do this by using the `keytool` utility that is part of the Java Runtime Environment (JRE).

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

To generate a private key for the server:

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

   /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*>

   > **Caution:** If you are using an SA gateway infrastructure as a proxy network, see Using a Proxy Server for how to modify the `keytool` command to set up the SAN.

   The variables used here refer to the following information:

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

   For example:

   ```
   /opt/hp/dma/server/jre/bin/keytool -genkeypair -alias tomcat -keyalg RSA
   -keysize 1024 -dname "CN=myserver.mycompany.com,OU=IT,O=mycompany,
   L=Fort Collins,S=Colorado,C=US" -keypass mypassword
   -keystore /opt/hp/dma/server/.mykeystore -storepass mypassword -validity 365
   ```

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

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

   ```
   /opt/hp/dma/server/jre/bin/keytool -list -v -keystore <storeFile>
   -storepass <password>
   ```

Generating the Certificate Signing Request to Obtain Signed Server Certificates

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

Tip: Make sure you check your company's security policy for the correct procedure.

If you have not already obtained signed certificates, generate a certificate signing request for your HPE DMA server and submit it to your CA. The CA will send you digitally signed certificates via email. You can then import the signed certificates into the keystore.

To generate the certificate signing request for the private-public key pair:

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

   ```
   /opt/hp/dma/server/jre/bin/keytool -certreq -v -alias <keyalias>
   -keypass <password> -keystore <storefile> -storepass <password>
   ```

   For example:

   ```
   /opt/hp/dma/server/jre/bin/keytool -certreq -v -alias tomcat
   -keypass mypassword -keystore /opt/hp/dma/server/.mykeystore
   -storepass mypassword
   ```

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

To receive the certificates from your CA:

In response to your request, the CA will send you a signed server certificate. Your CA may also send you the root certificate and any intermediate certificates required.

Note: The root and intermediate certificates may be bundled in a single file, or they may be delivered as separate files. Your CA will provide instructions for importing the root and any intermediate certificates into the keystore.

If your certificates are delivered in the body of an email message (versus a file), copy the certificates into a file. For example: `myserver.mycompany.com.cer`

Caution: Before you proceed, make a copy of your keystore.

Note: Next, you will import the contents of this file into the keystore.

Importing the SSL Server Certificates

Note: The order of operations is important–you must import the root certificate and any intermediate certificates before you import your signed server certificate. This will enable you to properly chain your server certificate to the root certificate.

Follow the instructions that your CA provided for importing the root and any intermediate certificates into the keystore.

To import the signed server certificate into your keystore, perform the following tasks:

1. To import the root and intermediate certificates, execute the following command (all on one line) for each of the certificates that your CA provided:

> **Note:** Your CA may provide any or all of these certificates:
>
> - Root certificate
> - Primary intermediate certificate
> - Secondary intermediate certificate

```
/opt/hp/dma/server/jre/bin/keytool -import -v -noprompt -trustcacerts
-alias <keyalias> -file <CAcert> -keystore <storefile> -storepass <password>
```

The variables used here refer to the following information:

Variable	Description	Examples

<keyalias>	Unique alias for the server's private key. This will be used to associate the server certificate with its private key.	For root certificate:
		`my-root-cert`
		For primary intermediate certificate:
		`my-cert-pri`
		For secondary intermediate certificate:
		`my-cert-sec`

<CAcert>	File that contains the contents of the certificate.	For root certificate:
		`CA-root-cert.cer`
		For primary intermediate certificate:
		`CA-cert-pri.cer`
		For secondary intermediate certificate:
		`CA-cert-sec.cer`

<storefile>	Fully qualified keystore file name.	`/opt/hp/dma/server/.mykeystore`
<password>	The password for both the keystore and the private key.	`mypassword`

2. To import your signed server certificate, execute the following command (all on one line):

```
/opt/hp/dma/server/jre/bin/keytool -import -v -noprompt -alias <keyalias>
-file <my-cert> -keystore <storefile> -storepass <password> -trustcacerts
```

Here, *<my-cert>* is the file that contains your signed certificate and *<keyalias>* is the same alias as for the private key. For example:

```
/opt/hp/dma/server/jre/bin/keytool -import -v -noprompt -alias my-root-cert
-file myserver.mycompany.com.cer -keypass mypassword
-keystore /opt/hp/dma/server/.mykeystore -storepass mypassword -trustcacerts
```

3. Run the following command to verify the contents of your keystore (all on one line):

```
/opt/hp/dma/server/jre/bin/keytool -list -keystore <storeFile>
-storepass <password>
```

For example:

```
/opt/hp/dma/server/jre/bin/keytool -list
-keystore /opt/hp/dma/server/.mykeystore -storepass mypassword
```

You should see the following type of output:

```
Keystore type: JKS
Keystore provider: SUN
Your keystore contains 2 entries
myrootcert, Aug 15, 2011, trustedCertEntry,
Certificate fingerprint (MD5): B5:95:C3:7C:61:A2:60:48:43:84:D5:70:29:F1:AC:E9
myserver, Aug 15, 2011, PrivateKeyEntry,
Certificate fingerprint (MD5): A4:E5:D7:3D:10:12:11:C2:F8:8B:29:E4:9B:97:21:07
```

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

> **Tip:** To view more detailed information, you can use the –v option with this command:

```
/opt/hp/dma/server/jre/bin/keytool -list –v -keystore <storeFile>
-storepass <password>
```

Configuring the HPE DMA Server to Use Your Certificate

After you add your server certificate to the keystore, this section directs you to do the following:

- Edit the <Connector> element in the `server.xml` file for the HPE DMA Web Server
- Change the trustAllCertificates value in the `dma.xml` file to false

To configure the HPE DMA server to use your certificate:

1. As root, stop the HPE DMA Server using the following command:

   `service dma stop`

2. Open the following file in a text editor:

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

3. Identify the default SSL Connector element:

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

4. If commented out, remove the comment delimiters (`<!--` and `-->`) around the SSL Connector element.
5. Specify the following attributes:

   ```
   <Connector port="<SSLport>" protocol="HTTP/1.1" SSLEnabled="true"
   scheme="https" secure="true" sslProtocol="TLS" keystoreFile="<storefile>"
   keyAlias="<keyalias>" keystorePass="<password>"/>
   ```

   The variables used here represent the following information:

Variable	Description
<keyalias>	Unique alias for the server's private key (see "Generating a Private Key for the Server" on page 23).
<SSLport>	Port that will be used for: • SSL communication between the HPE DMA Server and the HPE DMA clients • Accessing the HPE DMA user interface
<storefile>	Keystore file name. For example: /opt/hp/dma/server/.mykeystore
<password>	The password for both the keystore and this private key.

For example:

```
<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true"
scheme="https" secure="true" sslProtocol="TLS"
keystoreFile="/opt/hp/dma/server/.mykeystore"
keyAlias="myserver" keystorePass="mypassword"/>
```

6. Save the `server.xml` file.
7. Open the following file in a text editor:

   `/opt/hp/dma/server/tomcat/conf/Catalina/localhost/dma.xml`
8. Identify the following line:

   ```
   <Parameter name="com.hp.dma.conn.trustAllCertificates" value="true"/>
   ```
9. Set the value to false.

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

   If the line does not exist, add it.
10. Locate the following line:

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

    For example:

    ```
    <Parameter name="com.hp.dma.core.webServiceUrl"
    value="https://dmaserver.mycompany.com:8443/dma"/>
    ```
11. Ensure that the *<DMAServer>* specified in the webServiceUrl value matches the *<DMAServer>* configured in the public certificate. They must both be IP addresses or both be host names.

12. If you changed the *`<SSLport>`* in the `server.xml` file, also change the *`<SSLport>`* specified in the webServiceUrl value:

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

    Here, *`<SSLport>`* must match the *`<SSLport>`* configured in the `server.xml` file. For example:

    ```
    <Parameter name="com.hp.dma.core.webServiceUrl"
    value="https://dmaserver.mycompany.com:443/dma"/>
    ```

13. Save the `dma.xml` file.
14. As root, start the HPE DMA Server by using the following command:

    ```
    service dma start
    ```

Verifying the SSL Connection

To verify your SSL connection, perform the following steps:

1. Log in to your HPE DMA server.
2. HTTPS protocol indicates that the HPE DMA Server is communicating with the HPE DMA Client using SSL.
3. The lock icon (🔒) in the address bar indicates that the HPE DMA Server is communicating with the HPE DMA Client using SSL.

   If there is a problem with the website security certificate, you will see a shield icon (🛡) with a warning message.
4. For a test, execute an HPE DMA deployment.
5. When it finishes, navigate to the Automation > History page.
6. Select your deployment and then choose the Step Output tab in the bottom pane.
7. Verify that the deployment ended in SUCCESS—or at least did not have any errors indicating client-server communication issues.
8. Choose the Connector Output tab in the bottom pane.
9. Check that the following line is not in the output:

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

   If it is in the output, go back to "Configuring the HPE DMA Server to Use Your Certificate" on page 27, make the change in the `dma.xml` file, and then execute the deployment again.

If the above tests all pass, your SSL certificate is properly configured.

> **Note:** You have completed configuring SSL on the HPE DMA server.
>
> In the next stage you will install the HPE DMA client for SA.

Upgrading to HPE DMA 10.40

This section shows you how to upgrade from HPE DMA version 10.2xx, 10.30.000.000, or 10.30.001.000 to 10.40.000.000.

Security Note

As part of the upgrade from HPE DMA from 10.21 (or earlier) to HPE DMA 10.22 (or later), HPE DMA changes the `server.xml` file to increase HPE DMA security settings. HPE recommends that you keep the settings as implemented by the upgrade process.

If you want to revert the `server.xml` file, you can find a backup in `/opt/hp/dma/server/save`.

Note: Refer to the *HPE DMA Release Notes* for information about backward compatibility.

Tip: To take advantage of the features and enhancements of the new 10.40.000.000 workflows, after you have upgraded the HPE DMA server you must import the 10.40.000.000 solution pack, make a copy of the pertinent 10.40.000.000 workflow, and then merge your customizations into it.

Pre-upgrading requirements

Before you upgrade to version 10.40.000.000 of HPE DMA, perform the following steps, as root:

1. Create a backup of the database before starting this process.

   Caution: You **MUST** create a backup of the database to be able to revert back to HPE DMA10.30.000.000.

2. Stop HPE DMA:

   ```
   $ service dma stop
   ```

   Tip: If there are multiple HPE DMA servers configured to connect to a single database, you must stop all of them.

To upgrade to 10.40.000.000:

1. Go to the HPE DMA 10.40.000.000 installation media under the DMA_10.40.000.000_Server_and_Client folder.
2. On each HPE DMA server to be upgraded do the following to upgrade the HPE DMA server:

   Note: If you cut and paste from this PDF, make sure that the dashes (--) copy correctly.

   ```
   $ rpm --upgrade dma-server-10.40.000.000-0.x86_64.rpm
   ```

   Note: The new upload classes are in the server RPM file.

3. On one HPE DMA server per SA server, use the baseline command to upgrade your database. Run the following commands as root. For example:

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

> **Note:** When you upgrade HPE DMA you only need to use the baseline `-context` option because the following information is in the context file: <*database_username*>, <*database_password*>, and the JDBC connection string.
>
> For readability, the option is listed on a separate line—you must build the command in a single line.
>
> For a full description of all the baseline options, see "HPE DMA Baseline Options" on page 20.

> **Caution:** When you run the baseline command exactly as given you will maintain your HPE DMA database. If you use the --erase option you will lose your customized HPE DMA data.

```
$ sh ./dmaBaselineData.sh
-context /opt/hp/dma/server/tomcat/conf/Catalina/localhost/dma.xml
```

> **Note:** If you run this command on more than one server or run it more than once, it will not harm anything.

> **Note:** If you receive an error, see Troubleshooting.

4. Go to the HPE DMA 10.40.000.000 installation media under the DMA_10.40.000.000_Server_and_Client folder.
5. On one HPE DMA server per SA server, do the following to upgrade the HPE DMA Client for SA:

   > **Note:** If you cut and paste from this PDF, make sure that the dashes (--) copy correctly.

   ```
   $ rpm --upgrade dma-sa-client-10.40.000.000-0.x86_64.rpm
   ```
6. Have your SA administrator reinstall the Import the HPE DMA APX on the SA core.

   To do this, follow the instructions in "Importing the HPE DMA APX" on page 37. Note: The `/DMA_APX` folder will not be created since it already exists.
7. If you are also updating the SA core, rerun the script command to copy the required JAR files from the SA server to the HPE DMA server. On your HPE DMA server, run the following example command (enter as a single line):

   ```
   $ sh /opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/copyJars.sh
   <SA_Server>
   ```
8. Have your SA administrator reinstall the DMA Client Files policy on the SA core.

   To do this, follow the instructions in "Installing the DMA Client Files Policy" on page 39:

   a. Use the same folder (`/DMA_Client`) as in Step 1.

   b. Do steps 2 and 3.
9. Have your SA administrator remediate the DMA Client Files policy on all managed servers that use that policy:

   > **Note:** All servers attached to the policy that has changed must be remediated.
   >
   > Make sure that you have the following:
   >
   > - All of the managed servers are visible to you.
   >
   > - You have write permission.

a. Open the policy.

b. Go to **Server Usage** and select all of the servers that have the policy attached to them.

c. Right-click and choose **Remediate**.

> **Tip:** If you have hundreds of servers, it will be easier to do this using groups.

d. Click **Start Job**.

> **Tip:** If you do not remediate the policy for a server you will receive an error "Policy must be remediated" when you run a workflow that uses that server as a target.

10. Restart all HPE DMA servers using the following command:

```
$ service dma start
```

To revert an upgrade from the HPE DMA Server:

> **Caution:** You can only revert an upgrade if you created a backup of your database **BEFORE** you upgraded to version 10.40.000.000.

If you wish to revert the HPE DMA 10.40.000.000 upgrade back to a previous version (for example, 10.30.000.000), do the following:

1. Stop the HPE DMA server, as root:

   ```
   $ service dma stop
   ```

2. Restore the database from the backup.
3. Run the following command to revert back to HPE DMA 10.30.000.000.

   > **Note:** If you cut and paste from this PDF, make sure that the dashes (--) copy correctly.

   ```
   $ rpm --upgrade --oldpackage dma-server-10.30.000.000-0.x86_64.rpm
   ```

4. Upload and reinstall the HPE DMA 10.30.000.000 APX.
5. Detach the DMA Client Files policy from all managed servers and then remediate.
6. Delete the DMA Client Files policy and all packages in the `/DMA_Client` folder and then reinstall the policy using the policy install process from HPE DMA 10.30.000.000.
7. Attach the DMA Client Files policy to all desired managed servers and then remediate again.
8. Restart the HPE DMA server:

   ```
   $ service dma start
   ```

After you have upgraded to HPE DMA10.40, you must integrate with HP Server Automation. For information about integrating with HP Server Automation, see "Integrating HPE DMA with HP SA" on the next page

Integrating HPE DMA with HP SA

Caution: This stage of the installation process integrates HPE DMA with Server Automation (SA) and should be performed by an SA administrator—someone with SA administrator privileges and access.

HPE DMA uses HP Server Automation (SA) as an agent infrastructure. HPE DMA integrates with SA to authenticate users, associate users with groups, and determine user privileges. HPE DMA uses SA to acquire knowledge of servers and to send requests to execute workflows on servers. Before HPE DMA can actually work, you have to perform a series of integration steps on your SA system as well as on your new HPE DMA server.

You should work closely with your SA administrator to perform the tasks listed below. Your SA administrator may have guidelines or policies for specific aspects of the integration—for example, setting up SA users with HPE DMA access privileges. Furthermore, your SA administrator may have implemented a fine-grained security model requiring different users to perform different tasks in the list below. It is a good idea to delegate the actual SA integration to your SA administrator.

Note: Any server that will be used as an HPE DMA target needs to be managed by SA. It must also have the DMA Client Files software policy.

This section contains the following topics and should be performed in order:

Topic	Description
"SA Integration Requirements"	Information about the requirements that must be satisfied before integrating HPE DMA with SA.
"Overview of the HPE DMA and HP Server Automation Integration Process"	Overview of the steps to integrate with SA—to be performed by the SA administrator.
"Importing the HPE DMA APX"	Detailed instructions for the SA administrator to configure the SA Automation Platform Extension (APX) to be used by HPE DMA.
"Installing the DMA Client Files Policy"	Detailed instructions for the SA administrator to install and remediate the DMA Client Files policy.
"Settting SA Groups and Users"	Detailed instructions about the SA groups and SA users that need to be set up by the SA administrator along with their required permissions.

SA Integration Requirements

You must meet the following requirements before you can integrate DMA 10.40.000.000 with Server Automation (SA):

- Make sure that you have met all the general HPE DMA installation requirements in "System Requirements" on page 7.
- You have already installed and configured the HPE DMA server software. If you have not done so, see "Installing the HPE DMA Server" on page 16.
- You have already installed and configured the HPE DMA Client for SA. If you have not done so, see "Installing the HPE DMA Client for SA" on page 22.
- The HPE DMA server software and the HPE DMA Client for SA software must be installed on the same system. This system will be referred to as the HPE DMA server in the following instructions.

Overview of the HPE DMA and HP Server Automation Integration Process

The SA administrator needs to perform the following general steps:

1. Install the HPE DMA Automation Platform Extension (APX) on the SA server.
2. Install the DMA Client Files policy on the SA server.
3. Attach and remediate the DMA Client Files policy on all SA managed servers that will be used as HPE DMA targets.
4. Set up the SA groups that will have HPE DMA access privileges.
5. Set up the SA user that HPE DMA will use to connect to SA. This user must be permitted to access SA APIs.

In the commands that follow, replace the variables (found within <>'s) with values appropriate for your environment:

Variable	Example	Description
<SA_Server>	saserver.mycompany.com	Fully qualified host name of the Server Automation server
<DMA_server>	dma.mycompany.com	Fully qualified host name of the HPE DMA server

Support for SA 10.60

Database and Middleware Automation (DMA) Ultimate Edition now supports Server Automation (SA) 10.60.

SA 10.60 can be a fresh install or an upgrade from earlier version.

This section provides information on upgrading and integrating DMA 10.40 with SA 10.60.

1. Stop the DMA service.
2. On the DMA server:
   a. Upgrade JRE to version 1.8.
   b. Delete **twistclient.jar** and **wlclient*.jar** files from `/opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/lib/`.

   c. Copy the **opswclient.jar** file from `<SA_install_dir_10.60>/twister/` to `/opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/lib/` directory.

   d. Run the following command to change the ownership of the **opswclient.jar** file:

      ```
      chown hpdma:hpdma opswclient.jar
      ```

   e. Run the following command to copy binaries to the SA server:

      ```
      sh /opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/copyJars.sh <FQDN of SA Core>
      ```

3. Start the DMA service.

Importing the HPE DMA APX

This topic shows you how to configure the SA Automation Platform Extension (APX) for HPE DMA.

The HPE DMA APX can be imported into Server Automation Virtual Appliance 10 (SAVA) or Server Automation Enterprise Edition (Enterprise SA):

- For SAVA: The HP Live Network connector (LNc) must be used.
- For Enterprise SA: LNc can be used or the APX can be imported manually.

HPE Live Network Connector Overview

Follow the SAVA or Enterprise SA instructions for configuring the HP Live Network connector. The APX is contained in the `content.sa_dma` HPE LN Stream. SAVA uses the "Command-line Web Utilities Launcher" to configure LNc. Enterprise SA uses an installation of HP Live Network connector (LNc).

After the stream is loaded, the following APXs will be visible in the `/DMA_APX` folder:

- Update West Apx user on Windows
- westApx

Note: This user who will run the Update West APX must have read, write, and execute permission on the objects within the `/DMA_APX` folder.

SAVA Installation of the HPE DMA APX

Note: This method can only be used for SAVA.

From the SA client, as a user with list and execute permission on the objects in the `/Opsware/Tools/Administrative Extensions` folder, do the following:

1. Go to the Library > By Type tab, and then select Extensions > Web.
2. From Web, select the Command-line Web Utilities Launcher.
3. Select HPE Live Network Connect (the default).
4. To write the configuration to SAVA, execute the following command:

   ```
   /opt/opsware/hpln/lnc/bin/live-network-connector write-config
   --username=<username> --password=<password> --stream=content.sa_dma
   ```

   Here *<username>* and *<password>* are your HPE Passport user name and password.

   Note: Additional configuration can be added to the configuration using the `--add` option in the `live-network-connector` command. See *HP Live Network connector User Guide* for more information.

5. To download and import using the saved configuration, execute the following command:

   ```
   /opt/opsware/hpln/lnc/bin/live-network-connector download-import
   ```

   The default is `download-import`, so after the configuration is set up `download-import` is not required for this HP Live Network connector command.

Enterprise SA Manual Import of the HPE DMA APX

Tip: The following steps must be performed by an SA administrator.

The SA user (<*SA_APX_User*>) who imports the HPE DMA APX must belong to a group with the following privileges:

- SA Global Shell (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.

  If the `/DMA_APX` folder does not yet exist, this user must have List, Read, and Write permission on the `/` (root) folder, where the `/DMA_APX` folder will be created.

Note: This method can only be used for Enterprise SA.

If HP Live Network connector is configured for `content.sa_dma`, then you do not need to manually import the HPE DMA APX.

1. Work with the HPE DMA user with root-level access to the HPE DMA server (or the user that installed the RPMs on the HPE DMA server) to do the following:

   On the HPE DMA server, copy the HPE DMA APX to the SA server Global Shell. For example:

   ```
   $ scp -P 2222 /opt/hp/dma/server/client_bits/westapx.zip
   <SA_APX_user>@<SA_Server>:westapx.zip
   ```

   ```
   $ scp -P 2222 /opt/hp/dma/server/client_bits/updateWinAdmin.zip
   <SA_APX_user>@<SA_Server>:updateWinAdmin.zip
   ```

2. Log in to the SA server Global Shell, and install the HPE DMA APX using the defaults, for example:

   ```
   $ ssh -p 2222 <SA_APX_user>@<SA_Server>
   ```

   ```
   $ apxtool import westapx.zip
   ```

   ```
   $ apxtool import updateWinAdmin.zip
   ```

   By default this places the APX in `/DMA_APX`. If you want to place it somewhere else use the `-f <folder>` option.

   To skip the prompts, add `-F` to the end of the command or else respond Y to all Y/N prompts.

   Note: This creates the `/DMA_APX` (or <*folder*>) folder.

Installing the DMA Client Files Policy

This topic shows you how to install the DMA Client Files policy on the SA server and then to attach and remediate the DMA Client Files policy on all SA managed servers that will be used as HPE DMA targets.

Tip: The following steps must be performed by an SA administrator.

The SA user (<*SA_Policy_User*>) who installs the policy must belong to a group with the following privileges:

- Manage Software Policy—Read & Write under Policy Management.
- Manage Package—Read & Write under Package Management.
- List, Read, Write, and Execute permissions on the folder (`/DMA_Client`) that will contain the HPE DMA packages and policy.

Note: The following instructions assume that the HPE DMA Client for SA is installed on the HPE DMA server.

Follow these steps to install the DMA Client Files policy on your SA server, <*SA_Server*>:

1. In the SA Client, create a `/DMA_Client` folder.
2. As root on the HPE DMA server, go to the `client_bits` folder and then run the `dma_upload` script using your <*SA_Policy_User*> account. For example:

   ```
   $ cd /opt/hp/dma/server/client_bits
   ```

   ```
   $ sh ./dma_upload.sh -host <SA_Server> -user <SA_Policy_User>
    -password <SA_Policy_Password>
    -keyFile /opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/publicKey
    -folderName /DMA_Client
   ```

   Note: If you omit the password option (-password), you will be prompted for the password.

3. *Optional:* To verify that the policy has been properly uploaded, perform the following steps in the SA Client:

   Go to **Library** > **By Folder** > `DMA_Client`

   The `DMA_Client` folder should be populated. Verify that the DMA Client Files policy is included.
4. For each server that will be used as an HPE DMA target, attach and remediate the DMA Client Files policy.

Settting SA Groups and Users

This topic shows you how to set up the necessary SA groups and users for HPE DMA.

> **Tip:** The following steps must be performed by an SA administrator.
>
> Your SA administrator may have a security model that is more finely grained. Follow your SA policies for naming and granting permissions to groups.

HPE DMA User Groups

The following table provides examples of the types of user groups that you will need to use and manage HPE DMA in your environment.

Group Type	Example Name	Capability Required	Description
HPE DMA administrators	DMA Admins	Administrator	Users in this group will perform HPE DMA administrative duties.
Users who will create HPE DMA workflows	DMA Workflow Creators	Workflow Creator	Users in this group will have the ability to create HPE DMA workflows. **Note:** Once a workflow is created, it can be modified using Role Based Access (RBAC) as needed.
Users who will run HPE DMA workflows	DMA Workflow Runners	Login Access	Users in this group will have the ability to run HPE DMA workflows.

To set up your HPE DMA user groups:

1. On the SA server to which HPE DMA will connect, create each of the groups listed in the table and any additional groups that you need.
2. Grant the following permissions to each group:
   - 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 HPE DMA

     In order to add servers to HPE DMA organizations, a user must also have permission to see those servers in SA. This requires either Read permission on the pertinent customer or facility or Read permission on the device group (or groups) where the servers reside, depending on how your SA administrator manages permissions.

   > **Note:** Use the SA Client to grant these permissions.
3. Add at least one user to each group.

Later, you will register these groups as HPE DMA roles (see Register HPE DMA Roles) and assign each role the appropriate HPE DMA capability (see Assign HPE DMA Capabilities).

HPE DMA Connector User

An additional SA user, <*dma_connector_user*>, is required to configure the HPE DMA connector to SA (see Configure the Connector).

> **Note:** This user does not need to be a member of any of the SA groups that you just created.
>
> This user will be used by HPE DMA to connect to SA whenever a specific, personalized SA account cannot be used—for example, to verify whether a login is allowed.

To create the HPE DMA connector user:

1. On the SA server to which HPE DMA will connect, create a new SA user (for example: dma_connector_user).
2. Grant this new user the following permissions:
   - List, Read, and Execute permission for the `/DMA_Client` folder
   - List permission for all parent folders of the `/DMA_Client` folder
   - Managed Servers and Groups
   - Manage Software Policy (READ)
   - READ access to all managed servers that will be added to HPE DMA

     This requires either Read permission on the pertinent customer or facility or Read permission on the device group (or groups) where the servers reside, depending on how your SA administrator manages permissions.

> **Note:** This completes the SA installation and integration steps that must be done by the SA administrator.
>
> Next you should start HPE DMA.

Using SA Gateway Network as a Proxy Network

This section describes how to configure HPE Database and Middleware Automation (HPE DMA) and HP Server Automation (SA) to enable the use of the SA Gateway Network as a Proxy Network for HPE DMA communication traffic.

Goal

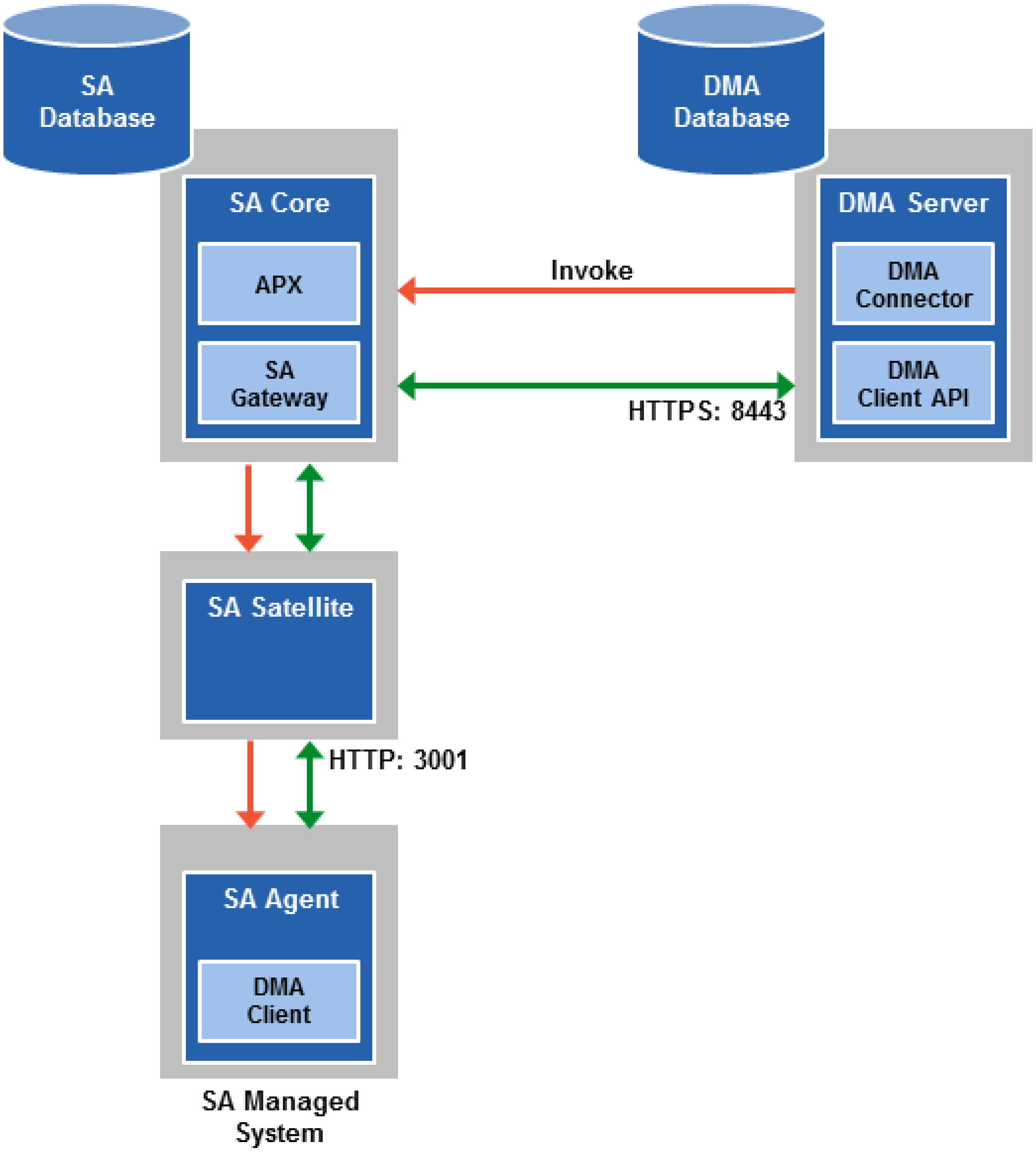
When you follow the instructions provided in this section, you will create a configuration that allows HPE DMA traffic to be routed through the SA Gateway Network from the managed server back to the HPE DMA Server. By following the instructions in this section you can avoid having to open up any extra firewall ports from a Managed Server.

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

1. HPE 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 routes the information to the HPE DMA Server.

   > Note: You can configure HPE DMA with a port other than 8443 (8443 is the default).



Prerequisites

Before you can perform the procedures in this section, your environment must meet the following minimum requirements:

- An SA mesh environment (SA 10.x) with one or more SA Cores must exist, with optional Satellites (for example, using Satellite to SA Core over a Gateway rather than directly connecting the managed server and HPE DMA Server).
- You must have administrative access to all SA Core servers within the mesh and the HPE DMA Server.
- HPE DMA 10.10 (or later) is required.

> Note: An existing HPE DMA Server installation is not required. These steps can be completed during the installation process. For more information, see HPE DMA Installation Guide for version 10.10 (or later), section “Install the HPE DMA Client for SA”.

Process Overview

You will utilize the following process to complete the configuration:

1. Add the egress filter to the SA Core Gateway configuration. This is required for the HPE DMA Server to be allowed as a traffic target. (See Step 1: How to Configure the SA Core Gateway Properties.)
2. Add the SA Realm of the SA Core (that the HPE DMA Server is connected to) into the HPE DMA Server context file. (See Step 2: How to Configure the SA Realm Parameter in the HPE DMA Server.)
3. Add and configure the Custom Fields

   within the HPE DMA Server Environment page. (See Setting the Realm in the dma.xml file specifies the Realm of the SA Core to which DMA is connected. The client on the target server receives this information when a workflow starts. The DMA client tells the SA agent that the traffic in SA needs to be routed to this Realm so that DMA will receive the communication. The egress filter in the Realm where DMA exists allows the communications in the Realm to leave the SA network and arrive at the DMA server. Because there is no guarantee which slice within the Realm will receive the communication, all slices in the Realm need the egress filter.

> For more information, see HPE DMA Installation Guide for version 10.10 (or later), section “Specify the Server Automation Realm.”

4. Step 3: How to Add and Configure Custom Fields on the HPE DMA Server)

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

Step 1: How to Configure the SA Core Gateway Properties

An EgressFilter rule must be added to the gateway properties of each slice within the SA Core that the HPE DMA Server is connected to:

1. a. If it does not already exist, create the 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>).

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

   ```
   opswgw.EgressFilter=tcp:<HPE DMA Server IP Address>:8443:*:*
   ```

3. Restart the gateway by issuing the following command:

   ```
   se4. Repeat steps 1-3 for each slice with the same realm within the SA Core to which
   the HPE DMA Server is connected.rvice opsware-sas restart opswgw-cgws
   ```

4. Repeat steps 1-3 for each slice with the same realm within the SA Core to which the HPE DMA Server is connected.
5. 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
   ```

   Important: The load balancer gateway must be restarted after all other gateways

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

Step 2: How to Configure the SA Realm Parameter in the HPE DMA Server

If the HPE DMA Server has already been installed, do the following:

1. Open the following file for editing:

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

2. Ensure that the webServiceUrl parameter is specified with an IP Address, as a hostname specification will not work when using the SA Gateway Network as a Proxy Network.
3. Add the following parameter line beneath the other parameters already specified:

   ```
   <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 HPE DMA Server is connected to.
4. Restart the HPE DMA Server by issuing the following command:

   ```
   service dma restart
   ```

If the HPE DMA Server is being installed, repeat the above directions after baselining is completed and before starting the HPE DMA Server.

The dma.xml file should now look similar to the following:

```
<?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" />
```

Note: Setting the Realm in the dma.xml file specifies the Realm of the SA Core to which DMA is connected. The client on the target server receives this information when a workflow starts. The DMA client tells the SA agent that the traffic in SA needs to be routed to this Realm so that DMA will receive the communication. The egress filter in the Realm where DMA exists allows the communications in the Realm to leave the SA network and arrive at the DMA server. Because there is no guarantee which slice within the Realm will receive the communication, all slices in the Realm need the egress filter.

For more information, see HPE DMA Installation Guide for version 10.10 (or later), section “Specify the Server Automation Realm.”

Step 3: How to Add and Configure Custom Fields on the HPE DMA Server

Create and configure the two Custom Fields that instruct HPE DMA to route traffic through the proxy server. This procedure is performed in the HPE DMA UI or via HPE DMA REST API commands. See the API documentation at https://my.dma.server.com:8443/dma/api.

Configuring HPE DMA Custom Fields for Proxy Communication

HPE DMA uses two Custom Fields to control proxy communication:

- west_proxy_in_use tells HPE DMA whether a proxy server will be used. Valid values are TRUE and FALSE: Or SA_auto_select versus an actual URL.
- 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.

  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 HPE 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 the proxy specified for this server	Use the proxy specified for the organization

Organization value is FALSE	Use the proxy specified for the server	Do not use the proxy specified 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 the proxy specified for this server	Do not use a proxy for this server

Silent Installation

HPE DMA provides an automated installation process to simplify and speed up the initial installation of HPE DMA for basic configurations, plus an automated removal process to uninstall HPE DMA that was installed using the automated installation:

Automated HPE DMA process	Description
"Automated HPE DMA Installation"	Installs HPE DMA on a single server when Oracle Database is already installed and the SA installation already exists: • Configures the Oracle database for HPE DMA • Installs the HPE DMA Server • Installs the HPE DMA Client for SA **Note:** If you want a more complex HPE DMA configuration (for example, high available or disaster recovery), you need to install HPE DMA by following the instructions in "Installing the HPE DMA".
"Automated uninstallation of HPE DMA"	Uninstalls HPE DMA that was installed using the automated installation: • *Optional*: Removes the Oracle database that was configured for HPE DMA • Runs the RPM commands to uninstall the HPE DMA Server and SA Client • Deletes the HPE DMA folders **Note:** If HPE DMA was installed manually, you need to uninstall HPE DMA by following the instructions in "Uninstalling the HPE DMA".

The DMA_10.40.000.000_Install folder also contains the following scripts:

File Name	Description
dma_install.sh install-options.txt installhelperscript.sh	Scripts that automate the installation of HPE DMA
dma_remove.sh remove-options.txt removehelperscript.sh	Scripts that automate the removal of HPE DMA

Automated HPE DMA Installation

The automated HPE DMA installation allows you to install HPE DMA on a single server in a basic configuration. Oracle Database must already be installed and the SA installation must already exist.

The benefits of using this automated installation are to simplify and speed up the installation—so that you do not need to key in many lengthy commands (for example,configuring the HPE DMA database and running the RPMs). It provides a simple install for a simple environment.

On the other hand, manual installation provides full control of the HPE DMA configuration. If you want a more complex HPE DMA configuration (for example, high available or disaster recovery), you need to install HPE DMA by following the instructions in "Installing the HPE DMA".

The automated installation works for the following configuration:

- A single HPE DMA Server.
- The SA Server host address is different than the HPE DMA Server host address.
- The Oracle database that HPE DMA uses can be located on either the HPE DMA Server or the SA Server.

> **Note:** Please read "Requirements" and "What the process does" **before** starting this automation—to ensure that it is appropriate for your environment.

Requirements

Before you can use the automated HPE DMA installation process, ensure that you meet the following requirements:

- These requirements in the "System Requirements" section:
  - Supported Products and Platforms—operating system, Server Automation, Oracle Database.
  - Sizing Recommendations
  - Other Requirements
- Your DBA has created an Oracle database to be used by HPE DMA. The Oracle Listener and database are up and running.

  > **Note:** The automated process will configure the Oracle database for HPE DMA.

- The HPE DMA 10.40.000.000 installation media is available and mounted.
- You have credentials to log in as root on the server where you run the script.
- If the HPE DMA database is not on the HPE DMA Server, then you need the password for the Oracle root user.

What the process does

The automated HPE DMA installation process (`dma_install.sh`) does the following:

Automation step	Replaces manual installation section
Adds the Oracle listener to `listener.ora`—if that entry does not already exist. Adds the HPE DMA tablespaces, creates the HPE DMA user credentials, grants the user the requisite permissions, and then sets the quota to unlimited for the data and index tablespace files.	"Configuring the Oracle Database"
Unpacks and installs the HPE DMA Server RPM file from the HPE DMA 10.40.000.000 installation media. For example: `/<mnt_dir>/DMA_10.40.000.000_Server_and_Client/dma-server-10.40.000.000-0.x86_64.rpm` Creates the baseline using the `dmaBaselineData.sh` script. Copies the required JAR files from the SA Server to the HPE DMA Server using the `copyJars.sh` script.	"Installing the HPE DMA Server"
Unpacks and installs the HPE DMA client for SA RPM file from the HPE DMA 10.40.000.000 installation media. For example: `/<mnt_dir>/DMA_10.40.000.000_Server_and_Client/dma-sa-client-10.40.000.000-0.x86_64.rpm`	"Installing the HPE DMA Client for SA"

Performing the automated installation of HPE DMA

Perform the following when logged in as root:

1. If you have not done so already, mount the HPE DMA 10.40.000.000 installation media.
2. Set up the installation parameters:
   a. Copy the `install-options.txt` file from the HPE DMA 10.40.000.000 installation media to a local directory. For example:

      ```
      $ cp /<mnt_dir>/DMA_10.40.000.000_Install/install-options.txt <local_dir>/.
      ```

   b. Open the `install-options.txt` file in a text editor. For example:

      ```
      $ vi <local_dir>/install-options.txt
      ```

   c. Specify values for the parameters:

Parameter	Example	Description
sa	`saserver.mycompany.com`	Server Automation host address.
sid	`orcl`	Oracle SID of the HPE DMA database. If SA and HPE DMA share the same database, specify the SA SID.
dma_db_ host	`dmaserver.mycompany.com`	The host address where the HPE DMAOracle database is located. May be either the HPE DMA Server host address or the SA Server host address.

datafile	`/u01/app/oracle/oradata/<sid>/dma_data1.ora`
	If the SID is orcl:
	`/u01/app/oracle/oradata/orcl/dma_data1.ora`
		The fully-qualified Oracle data file. Replace <*sid*> with the SID value.

indxfile	`/u01/app/oracle/oradata/<sid>/dma_indx.ora`
	If the SID is orcl:
	`/u01/app/oracle/oradata/orcl/dma_indx.ora`
		The fully-qualified Oracle index tablespace file. Replace <*sid*> with the SID value.

dbuser	`dma`	HPE DMA database username to be used after the database is created.
dbpass	*`<dma_password>`*	HPE DMA database password to be used after the database is created.
filesize	`100M`	Maximum file size of datafile, in MB.

   d. Save your changes to the `install-options.txt` file.

      Tip: Since this options file contains sensitive information, after you run the script you may want to either delete the file or change the values for dbuser and dbpass.

3. Run the script that automates the process to install HPE DMA:
   a. Start the script in the mount directory:

      ```
      $ cd /<mnt_dir>/DMA_10.40.000.000_Install
      ```

      ```
      $ ./dma_install.sh <local_dir>/install-options.txt
      ```

      The script displays log information while running.

      If the HPE DMA database is not on the HPE DMA Server, you will be prompted for the password for the Oracle root user.
   b. Example execution:

      ```
      STARTING DMA INSTALLATION
      ########################################################################
      <<<< Loading the options file..  >>>>
      <<<< DMA installation starting >>>>
      ########################################################################
      Launching DMA Installation..
      +DMA Host               = dmaserver.mycompany.com
      +DMA Pack               = ../DMA_10.40_Server_and_Client/dma-server-10.40-
      0.x86_64.rpm
      +SA Host                = saserver.mycompany.com
      +SID                    = orcl
      +DB User                = dma
      +Data Tablespace Name  = HPDMA_DATA
      +Indx Tablespace Name  = HPDMA_INDX
      +Data File              = /u01/app/oracle/oradata/orcl/dma_data1.ora
      +Index File             = /u01/app/oracle/oradata/orcl/dma_indx.ora
      +File Size              = 100M
      ########################################################################
      <<<< Making an entry in listener.ora >>>>
      Making listener entry in oracle home : /u01/app/oracle/product/11.2.0/db_1
      SID name already exists!
      <<<< User will be created now. >>>>
      Tablespaces has been created sucessfully
      <<<< Oracle Listener starting now..>>>>
      LSNRCTL for Linux: Version 11.2.0.1.0 - Production on 10-NOV-2014 09:28:13
      Copyright (c) 1991, 2009, Oracle.  All rights reserved.
      TNS-01106: Listener using listener name LISTENER has already been started
      <<<< Unpack dma distribution and install >>>>
      Preparing...
      ##################################################
      Performing an installation
      dma-server
      ##################################################
      HPE DMA 10.40.0 Installation completed.
      Please read the install documentation at /opt/hp/dma/server/readme.txt to
      complete the installation.
      <<<< Creating baseline >>>>
      10 Nov 2014 09:28:20,843 INFO  DMABaselineData - Saved context file:
      opt/hp/dma/server/tomcat/conf/Catalina/localhost/dma.xml
      ```

```
10 Nov 2014 09:28:20,846 INFO  DMABaselineData - Context file has been
created.
10 Nov 2014 09:28:21,675 INFO  DMABaselineData - Using specified context for
settings (command line overrides ignored) file:
/opt/hp/dma/server/tomcat/conf/Catalina/localhost/dma.xml
10 Nov 2014 09:28:36,195 INFO  DMABaselineFile - DMA baseline file is
'/opt/hp/dma/server/db_sql/dma-oracle/dma_baseline.sql'
10 Nov 2014 09:28:36,289 INFO  DMABaselineFile - DMA Download Software file
is '/opt/hp/dma/server/db_sql/dma-oracle/dma_download_software.xml'
10 Nov 2014 09:28:36,565 INFO  DMADownloadSoftwareUpgrader - Download
Software successfully saved during baseline
10 Nov 2014 09:28:36,565 INFO  DMADownloadSoftwareUpgrader - Updated Download
Software step
10 Nov 2014 09:28:36,795 INFO  DMABaselineData - Keys have been initialized.
10 Nov 2014 09:28:36,819 INFO  DMABaselineData - DMA baselining has
completed.
Downloading wlclient_rmi_addon.jar from saserver.mycompany.com
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
Dload  Upload   Total   Spent    Left  Speed
^M  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--
 0^M100 75282  100 75282    0     0  1498k      0 --:--:-- --:--:-- --:--:--
1598k
Placing wlclient_rmi_addon.jar in /opt/hp/dma/server/tomcat/webapps/dma/WEB-
INF/lib/
Downloading wlclient.jar from saserver.mycompany.com
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
Dload  Upload   Total   Spent    Left  Speed
^M  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--
 0^M100  508k  100  508k    0     0  21.6M      0 --:--:-- --:--:-- --:--:--
23.6M
Placing wlclient.jar in /opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/lib/
Downloading twistclient.jar from saserver.mycompany.com
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
Dload  Upload   Total   Spent    Left  Speed
^M  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--
 0^M 29 36.7M   29 10.7M    0     0  36.0M      0  0:00:01 --:--:--  0:00:01
36.2M^M100 36.7M  100 36.7M    0     0
68.6M      0 --:--:-- --:--:-- --:--:-- 68.8M
Placing twistclient.jar in /opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/lib/
Preparing...
##################################################
package dma-sa-client-10.40-0.x86_64 is already installed
<<<< Setting up dma.xml  >>>>
<<<< Going to start/restart DMA service now! >>>>
Removing old working dir of /var/opt/hp/dma/work/dma
Starting HPE DMA Server
Using CATALINA_BASE:   /opt/hp/dma/server/tomcat
Using CATALINA_HOME:   /opt/hp/dma/server/tomcat
Using CATALINA_TMPDIR: /opt/hp/dma/server/tomcat/temp
Using JRE_HOME:        /opt/hp/dma/server/jre
Using CLASSPATH:
/opt/hp/dma/server/tomcat/bin/bootstrap.jar:/opt/hp/dma/server/tomcat/bin/tom
cat-juli.jar
Tomcat started.
########################################################################
DMA install is complete. Please launch
https://dmaserver.mycompany.com:8443/dma
DMA Installation logs are kept at: /var/log/dma_install_logs
DMA Application logs are available at: /var/log/hp/dma
Installation completed in 27 seconds
########################################################################
```

Verifying the automated installation of HPE DMA

Perform the following after the automated installation is complete:

1. Verify that you received a "DMA install is complete" message. If you received a "DMA install was unsuccessful" message, review the installation script log file that is found at `/var/log/dma_install_logs`.
2. Open `https://<dma_server>:8443/dma` in a web browser—to verify that the HPE DMA web interface is available—and then close.
3. Follow the instructions in the following sctions,to integrate HPE DMA with Server Automation:

   "Integrating HPE DMA with HP SA"
   - "SA Integration Requirements"
   - "Importing the HPE DMA APX"
   - "Installing the DMA Client Files Policy"
   - "Settting SA Groups and Users"
4. Follow the instructions in the following section, to configure SSL:

   "Configuring SSL on the HPE DMA Server"
   - "Configuring SSL on the HPE DMA Server"
   - "Generating a Private Key for the Server"
   - "Generating the Certificate Signing Request to Obtain Signed Server Certificates"
   - "Importing the SSL Server Certificates"- "Configuring the HPE DMA Server to Use Your Certificate"
   - "Verifying the SSL Connection"
5. Follow the instructions in teh following section, to start HPE DMA:

   Start HPE DMA
6. Follow the instructions in the following to set up HPE DMA:

   Set Up HPE DMA
   - Configure the Connector
   - Register HPE DMA Roles
   - Assign HPE DMA Capabilities
   - Add Available Targets
   - Import an HPE DMA Solution Pack

Congratulations! You now have HPE DMA up and running!

Automated uninstallation of HPE DMA

The automated HPE DMA removal allows you to remove (uninstall) HPE DMA that was installed using the automated installation. If HPE DMA was installed manually, you need to uninstall HPE DMA by following the instructions in "Uninstalling the HPE DMA".

You choose whether or not to remove HPE DMA's Oracle database based on an input parameter.

Note: Please read "Requirements" and "What the process does" **before** starting this automation—to ensure that it is appropriate for your environment.

Requirements

Before you can use the automated HPE DMA removal process, ensure that you meet the following requirements:

- The HPE DMA 10.40.000.000 installation media is available and mounted.
- You have credentials to log in as root on the server where you run the script.
- You need the Oracle user and password for the HPE DMA database.
- If the HPE DMA database is not on the HPE DMA Server, then you need the password for the Oracle root user.

What the process does

The automated HPE DMA removal process (`dma_remove.sh`) does the following:

Automation step	Replaces manual installation section
Optionally removes the Oracle tablespaces and datafiles that HPE DMA created. Runs the RPM commands to uninstall the HPE DMA Server and the SA Client. Deletes the HPE DMA folders. **Note:** The script does NOT remove the user because Oracle is still active—if you want, your Oracle DBA can remove the user after the script has completed. The script does NOT restart the database so it will not interfere with other users.	"Uninstalling the HPE DMA"

Performing the automated uninstallation of HPE DMA

Perform the following when logged in as root:

1. If you have not done so already, mount the HPE DMA 10.40.000.000 installation media.
2. Set up the removal parameters:
   a. Copy the `remove-options.txt` file from the HPE DMA 10.40.000.000 installation media to a local directory. For example:

      ```
      $ cp /<mnt_dir>/DMA_10.40.000.000_Install/remove-options.txt <local_dir>/.
      ```

   b. Execute this query to determine which RPM packages are installed—you will need this information when you set the removal parameters:

      ```
      $ rpm -qa | grep dma
      ```

   c. Open the `remove-options.txt` file in a text editor. For example:

      ```
      $ vi <local_dir>/remove-options.txt
      ```

   d. Specify values for the parameters:

Parameter	Example	Description
dmapack	`dma-server-10.40.000.000-0.x86_64.rpm`	The HPE DMA Server RPM filename for the current version of HPE DMA (do not include `.rpm`).
saclient	`dma-sa-client-10.40.000.000-0.x86_64.rpm`	The HPE DMASA Client RPM filename for the current version of HPE DMA (do not include `.rpm`).
sa	`saserver.mycompany.com`	Server Automation host address.
sid	`orcl`	Oracle SID of the HPE DMA database. If SA and HPE DMA share the same database, specify the SA SID.
dma_db_ host	`dmaserver.mycompany.com`	The host address where the HPE DMAOracle database is located. May be either the HPE DMA Server host address or the SA Server host address.
dbuser	`dma`	HPE DMA database username. Only needed if remove_dma_db is set to true.
dbpass	*<dma_password>*	HPE DMA database password. Only needed if remove_dma_db is set to true.
remove_ dma_db	false	Determines whether the HPE DMA tables and data will be completely removed. Valid values are true and false. **Tip:** Leaving the HPE DMA tables and data intact can be useful in a development environment.

e. Save your changes to the `remove-options.txt` file.

> **Tip:** Since this options file contains sensitive information, after you run the script you may want to either delete the file or change the values for dbuser and dbpass.

3. Run the script that automates the process to remove HPE DMA:

   a. Start the script in the mount directory:

```
$ cd /<mnt_dir>/DMA_10.40.000.000_Install
$ ./dma_remove.sh <local_dir>/remove-options.txt
```

The script displays log information while running.

When prompted whether you want to continue the removal script, respond `yes`.

If the HPE DMA Oracle database is not on the HPE DMA Server, you will be prompted for the password for the Oracle root user.

b. Example execution:

```
########################################################################
NOTE : THIS WILL UNINSTALL DMA
########################################################################
Do you still want to continue with the uninstallation?(yes/no) <<<< Loading
the options file..  >>>>
###################################################################
Launching DMA UNInstallation..
+DMA Host              = IWFVM02090.hpswlabs.adapps.hp.com
+DMA Pack              = dma-server-10.40-0.x86_64
+SA Host               = IWFVM00597.hpswlabs.adapps.hp.com
+SID                   = orcl
+DB User               = dma
+Data Tablespace Name  = HPDMA_DATA
+Indx Tablespace Name  = HPDMA_INDX
###################################################################
<<<< The DMA DB will be removed now. >>>>
Dropping user
Dropping Tablespace
User and Tablespaces removed sucessfully
<<<< Stopping DMA and removing it now..  >>>>
Stopping HPE DMA Server
Using CATALINA_BASE:   /opt/hp/dma/server/tomcat
Using CATALINA_HOME:   /opt/hp/dma/server/tomcat
Using CATALINA_TMPDIR: /opt/hp/dma/server/tomcat/temp
Using JRE_HOME:        /opt/hp/dma/server/jre
Using CLASSPATH:
/opt/hp/dma/server/tomcat/bin/bootstrap.jar:/opt/hp/dma/server/tomcat/bin/tom
cat-juli.jar
waiting for processes to exit
waiting for processes to exitShutting down DMA service before uninstalling
DMA.
HPE DMA Server is not running
The Uninstall of this product does not remove files and directories created
by DMA.
To clean your system of DMA please remove the following folders
/opt/hp/dma/server,
/var/opt/hp/dma/work/dma, and /var/log/hp/dma.
---------------------------------------------
DMA server has been removed successfully..
DMA logs are at: /var/log/dma_install_logs
-------------------- ------------------------
```

Verifying the automated uninstallation of HPE DMA

Perform the following after the automated removal has completed:

1. Verify that you received the "DMA server has been removed successfully.." message. If the removal was not successful, review the removal script log file that is found at `/var/log/dma_install_logs`.
2. Verify that you **cannot** open `https://<dma_server>:8443/dma` in a web browser.
3. - Follow the instructions to remove HPE DMA from the managed servers:
   - "Uninstalling the HPE DMA"
   - "Uninstall HPE DMA from the Managed Servers"
4. If the script removed the HPE DMA database, your Oracle DBA can now delete the HPE DMA user.
5. Your SA administrator can now clean up the HPE DMA integrations with SA.

You have successfully uninstalled HPE DMA!

Uninstalling the HPE DMA

This section shows you how to uninstall HPE DMA from the HPE DMA Server and the HPE DMA managed servers.

Note: An automated script is available that can speed up the removal process if HPE DMA was installed with the automated install process. For information about this script, see "Automated uninstallation of HPE DMA".

Uninstalling HPE DMA from the HPE DMA Server and SA Client

To uninstall HPE DMA from the HPE DMA Server,:

1. As root, stop the HPE DMA service, for example:

   ```
   $ service dma stop
   ```

2. Run the following query to verify the HPE DMA RPM installation:

   ```
   $ rpm -qa | grep dma
   ```

   You can locate the current version of HPE DMA in the results:

   ```
   dma-server-<DMA_Version>-0.x86_64
   dma-sa-client-<DMA_Version>-0.x86_64
   ```

   For example: If your current version of HPE DMA is 10.40.000.000, your results will look like this:

   ```
   dma-server-10.40.000.000-0.x86_64.rpm
   dma-sa-client-10.40.000.000-0.x86_64.rpm
   ```

3. Run the following commands as root to uninstall HPE DMA:

```
$ rpm -e dma-server-<DMA_Version>-0.x86_64
$ rpm -e dma-sa-client-<DMA_Version>-0.x86_64
```

In these lines, replace <*DMA_Version*> with the HPE DMA version from your query.

4. To finish cleaning up after you uninstall HPE DMA, you can remove the following folders:

```
/opt/hp/dma/server
/var/opt/hp/dma/work/dma
/var/log/hp/dma
```

Uninstall HPE DMA from the Managed Servers

To uninstall HPE DMA from the managed servers (the HPE DMA Client):

1. In SA, detach the managed server from the DMA Client Files policy and then remediate the target.
2. To completely remove HPE DMA from the target execute the appropriate command:
   - For Linux: `rm -rf /opt/hp/dma/client/`
   - For Windows: `rmdir /S /Q %SYSTEMDRIVE%\Progra~1\HP\DMA\Client`

Note: To completely uninstall HPE DMA, work with your Oracle DBA/PostgreSQL to uninstall the HPE DMA schema and tablespaces from Oracle Database/PostgreSQL and work with your SA administrator to remove the HPE DMA integrations with SA.

Uninstalling DMA from the DMA Server and SA Client

To uninstall HPE DMA from the HPE DMA Server,:

1. As root, stop the HPE DMA service, for example:

   ```
   $ service dma stop
   ```

2. Run the following query to verify the HPE DMA RPM installation:

   ```
   $ rpm -qa | grep dma
   ```

   You can locate the current version of HPE DMA in the results:

   ```
   dma-server-<DMA_Version>-0.x86_64
   dma-sa-client-<DMA_Version>-0.x86_64
   ```

   For example: If your current version of HPE DMA is 10.40, your results will look like this:

   ```
   dma-server-10.40.000.000-0.x86_64.rpm
   dma-sa-client-10.40.000.000-0.x86_64.rpm
   ```

3. Run the following commands as root to uninstall HPE DMA:

   ```
   $ rpm -e dma-server-<DMA_Version>-0.x86_64
   $ rpm -e dma-sa-client-<DMA_Version>-0.x86_64
   ```

   In these lines, replace <*DMA_Version*> with the HPE DMA version from your query.

4. To finish cleaning up after you uninstall HPE DMA, you can remove the following folders:

```
/opt/hp/dma/server
/var/opt/hp/dma/work/dma
/var/log/hp/dma
```

Uninstalling DMA from Managed Servers

To uninstall HPE DMA from the managed servers (the HPE DMA Client):

1. In SA, detach the managed server from the DMA Client Files policy and then remediate the target.
2. To completely remove HPE DMA from the target execute the appropriate command:
   - For Linux: `rm -rf /opt/hp/dma/client/`
   - For Windows: `rmdir /S /Q %SYSTEMDRIVE%\Progra~1\HP\DMA\Client`

Note: To completely uninstall HPE DMA, work with your Oracle DBA/PostgreSQL to uninstall the HPE DMA schema and tablespaces from Oracle Database/PostgreSQL and work with your SA administrator to remove the HPE DMA integrations with SA.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Installation Guide (Database and Middleware Automation 10.40)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to hpe_dma_docs@hpe.com.

We appreciate your feedback!