



# Database and Middleware Automation

Software Version: 10.50.001.000

Linux, Solaris, AIX, and HP-UX

## Installation Guide

Document Release Date: May 2017

Software Release Date: May 2017



**Hewlett Packard**  
Enterprise

## 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. Hewlett Packard Enterprise 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 Hewlett Packard Enterprise 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

© 2012-2016 Hewlett Packard Enterprise Development LP

### 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

To check for recent updates or to verify that you are using the most recent edition of a document, go to: <https://softwaresupport.hpe.com/>.

This site requires that you register for an HP Passport and to sign in. To register for an HP Passport ID, click **Register** on the HPE Software Support site or click **Create an Account** on the HP Passport login page.

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

## Support

Visit the HPE Software Support site at: <https://softwaresupport.hpe.com/>.

Most of the support areas require that you register as an HP Passport user and to sign in. Many also require a support contract. To register for an HP Passport ID, click **Register** on the HPE Support site or click **Create an Account** on the HP Passport login page.

To find more information about access levels, go to: <https://softwaresupport.hpe.com/web/softwaresupport/access-levels>.

**HPE Software Solutions Now** accesses the HPSW Solution and Integration Portal website. 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 website is <https://softwaresupport.hpe.com/km/KM01702731>.

## 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

Install .....	5
Support matrix .....	5
Requirements .....	6
Platform requirements .....	6
Hardware requirements .....	7
Software requirements .....	7
Servers .....	8
Ports .....	8
Firewalls .....	8
Privileges .....	9
Supported browsers for DMA .....	9
Supported DMA target platforms .....	9
Performance and sizing .....	10
Hardware and Infrastructure Sizing .....	10
DMA Client Sizing .....	11
Pre-installation tasks .....	12
Meet the hardware and software requirements .....	14
Obtaining a signed server certificate .....	15
Configuring the Oracle database .....	16
Steps to Configure the Oracle Database .....	16
Configuring the PostgreSQL database .....	19
Steps to Create and Configure the PostgreSQL Database .....	19
Choose your installation method .....	21
Regular installation .....	21
Installing DMA Server .....	22
Start DMA .....	26
DMA baseline options .....	28
Applying the license .....	30
Installing DMA Client for SA .....	31
Silent installation .....	31
Process overview .....	33
Perform the automated installation of DMA .....	34
Verify the automated installation of DMA .....	38
Post-installation task .....	39
Configure SSL on the DMA Server .....	40
About the keytool utility .....	40
Generate a Private Key for the Server .....	41

Generate the Certificate Signing Request to Obtain Signed Server Certificates .....	42
Import the SSL Server Certificates .....	43
Configure the DMA Server to Use Your Certificate .....	45
Verify the SSL Connection .....	47
Set up DMA .....	49
Configure the Connector .....	49
Register DMA roles .....	52
Assign DMA capabilities .....	54
Add available targets .....	55
Add servers .....	55
Granting permissions .....	56
Import a solution pack .....	58
Obtaining the patch files .....	58
Accessing the DMA solution packs .....	59
Importing the solution pack .....	59
Versioning and importing Solution Packs .....	60
Uninstall DMA 10.50.001.000 .....	61
Uninstall .....	61
UninstallDMA from the Managed Servers .....	62
Silent uninstall .....	62
Requirements .....	63
What the process does .....	63
Performing the automated uninstallation of DMA .....	63
Verify the automated uninstallation of DMA .....	66
Send documentation feedback .....	67

# Install

This section includes the following topics to help you install DMA:

A full installation of Database and Middleware Automation 10.60.000.000 includes the following components:

Core components

- DMA Server
- DMA Client for SA

For instructions to install these two components, ["Choose your installation method" on page 21](#).

## Support matrix

This section provides information about the supported hardware and software that you must have in order to successfully install and run DMA.

- ["Requirements" on the next page](#)
- [Workflow support matrix](#)
- ["Performance and sizing" on page 10](#)

# Requirements

This section provides information about the supported hardware and software that you must have in order to successfully install and run DMA.

## Platform requirements

The DMA version 10.50.001.000 server requires the following server platform infrastructure:

Server Platform Infrastructure	Product	Version
DMA Server platform	Red Hat Enterprise Linux	5.8, 6.1, 7 (or later), 64-bit
	SUSE Enterprise Linux	11 (or later) 64-bit
Server Management Tool	Server Automation	Server Automation Ultimate Edition 10.1x and 10.2x (SA 10.1x and 10.2x)
		Server Automation Enterprise Edition 10.1x and 10.2x (SA 10.0x and 10.2x)
		Server Automation 10.0x Standard Edition (SAVA 10.0x)
	DCA Virtual Appliance	DCA Virtual Appliance 2016.01
DMA Backend Database Tool	Oracle Database Enterprise or Standard Edition	12.1.0.2 (container DB)
		11gR2
	PostgreSQL	9.3.5
Oracle Java	Java Runtime Environment (JRE)	Version 8 Update 92 (1.8_u92) on Linux, Windows, Solaris Version 8 Update 5 (1.8_u5) on HP-UX Version 8 Update 130 (1.8_u130) on AIX

**Note:** Although DMA works on other Linux operating systems, supports these certified versions.

## Hardware requirements

See the ["Performance and sizing" on page 10](#).

**Note:** DMA is fully supported to be installed and run on VMware versions 5 and 5.1 virtual machines.

## Software requirements

- Server Automation, any of the following versions:
  - Ultimate Edition 10.1x, 10.2x (SA 10.1x, 10.2x)
  - Standard Edition 10.10 (SAVA 10.10)
  - Enterprise Edition 10.0x, 10.2x (SA 10.0x, 10.2x)

**Note:** You must purchase this license separately.

- Oracle Database Enterprise Edition/PostgreSQL 9.3.5

**Note:** does not provide the Oracle Database and the PostgreSQL license to run DMA.

**Tip:** If you plan to co-locate DMA with SA 10.10 (or later)—which uses Oracle 12c—set up DMA to also use Oracle 12c (to only require a single version of Oracle).

- Java Runtime Environment (JRE) Version 7 Update 80 (1.7u80) and Version 7 Update 85 (1.7u85). The JRE 1.7u85 is supported only in AIX and HP-UX platforms.

### Server Automation (SA)

Server Automation needs to be up and running.

The person who integrates DMA with SA—probably your SA administrator—needs the following:

- Root access to the SA server
- Ability to create users, groups, and permissions
- OGS (SA Global Shell) access

This person should have the highest possible administrative rights. Although these rights may not be needed for all steps, they will help the process go smoothly.

## Servers

DMA and SA can run on the same server (OS instance).

DMA and SA can use the same Oracle/PostgreSQL installation and database, but each product needs to be configured in separate schemas.

## Ports

The following table provides a list of default ports used in DMA. You can configure different ports as required:

Server/Database	Port (default)
DMA	8443
Oracle Database	1521
PostgreSQL Database	5432
SA	443

## Firewalls

The firewalls need to have the following ports open:

- Incoming on the port configured for DMA, 8443 is the default port—or a proxy server can be used.
- Outgoing on the ports configured for Oracle Database/PostgreSQL, and SA.

**Tip:** For more information about how to set up a proxy server with DMA, see Using a proxy server section in Administration Guide.

If you are configuring DMA server with an IPv6 address, ensure that the firewall (for IPv6 traffic) is turned off or configured to do the following:

- Allow bi-directional communication on port 443 between DMA server and SA server
- Allow incoming communication to DMA server from all the DMA target servers that connect directly, on port 8443 (or whatever port DMA is server is configured to run on)
- Allow bidirectional communication between the DMA target servers and their respective SA Satellite proxy servers, on port 443.

Note: DNS resolution must be enabled across the infrastructure for IPv6 address resolution.



Note: If the default hostname does not resolve an IPv6 address, use the *-dmah* option while using the `dmaBaseline.sh` command, after installing DMA 10.40.

## Privileges

To install packages on all UNIX® machines you must log on as a user that has root access.

## Supported browsers for DMA

The DMA web UI supports the following browsers:

- Chrome
- Firefox
- Internet Explorer 10 and 11

## Supported DMA target platforms

DMA supports managed target servers that use the following operating systems:

- Linux
- Solaris
- AIX
- Windows
- HP-UX

For details regarding the operating systems and versions supported by each DMA workflow, see the DMA Support Matrix available at <https://softwaresupport.hpe.com/>. See Documentation Updates for information about accessing this website.

# Performance and sizing

This topic provides the sizing recommendations for the DMA hardware and infrastructure and also for the DMA Client.

## Hardware and Infrastructure Sizing

This section suggests deployment sizing guidelines to help you decide the hardware and infrastructure that you need to deploy DMA in your environment. This section lists the minimum recommended CPU count, RAM, and disk space for the DMA server and the DMA database server—the server that houses your Oracle/PostgreSQL database.

**Tip:** This topic does not give sizing recommendations for Server Automation (SA). The assumption is that SA is already up and running in your environment.

### DMA Deployment Modes

DMA supports the following deployment options:

- Single Server: Install both the DMA server and the DMA database on a single server
- Dual Server: Install DMA on one server and create the DMA database on a separate server

### Deployment sizing categories

Category	Number of DMA Clients
Small	<100
Medium	<500
Large	1,500+

**Note:** The number of clients is not an exact measure for sizing. Sizing depends greatly on what you do with the operational system.

### Recommended Sizing

The following table describes sizing suggestions for deploying the DMA server:

**Sizing recommendations for deploying the DMA server**

Category	Number of CPUs (2.66 GHz )	RAM	Disk Space
Small	1	4 GB	25 GB
Medium	2	8 GB	50 GB
Large	4	16 GB	100 GB

**Note:** The recommendations are minimum requirements for the installation. These recommendations are based on dual core installation.

If you install DMA on a virtual machine you must ensure that the actual available CPUs and RAM for the DMA server virtual machine meets the same requirements.

The following table describes sizing suggestions for deploying the DMA database component:

**Sizing recommendations for deploying the DMA database server**

Category	Number of CPUs (2.66 GHz )	RAM	Disk Space
Small	4	4 GB	50 GB
Medium	4	8 GB	100 GB
Large	4	16 GB	250 GB

**Note:** When considering sizing for these types of deployments, each sizing recommendation should be considered independently of whether or not the components are installed on the same server or on different servers. In other words, these sizing recommendations are additive.

If you install the DMA database on a virtual machine you must ensure that the actual available CPUs and RAM for the DMA database virtual machine meets the same requirements.

## DMA Client Sizing

This section suggests sizing guidelines for the DMA Client. The DMA Client is installed on each DMA Managed Server. The DMA Client consists of the software modules used by DMA to initiate and control workflow executions on the managed server, as well as the runtime software required for the DMA workflows.

The disk space required for the DMA Client depends on the number of workflow executions that are planned and whether the managed server will be used as an DMA development target. Thus, the required disk space is not fixed.

The following table outlines what you should consider to size the DMA Client's disk space correctly:

Directory	Description	Size
/opt/hp/dma	Contains the software modules used to initiate and run DMA workflows. This directory only contains static content.	For the current release, the required disk space is about 0.4 GB. The actual size varies slightly depending on the operating system of the managed server.
/var/opt/hp/dma	Not used in the current release. Will be used in future releases.	
/var/tmp/dma	Contains temporary files needed during workflow execution, such as step and function code.	<p>The disk space required for a workflow's execution depends on the workflow and the debug level that is used. Typically, a workflow's execution requires less than 15 MB of disk space, even with the maximum debug level. Unless specifically configured to keep the temporary files, DMA will delete the temporary files upon workflow completion.</p> <p>The disk space for this directory can be calculated as the number of workflows running in parallel multiplied by 15 MB.</p> <p>Development systems—where files may be kept for debugging—require additional disk space. The additional disk space depends on the number of workflows that run in parallel and number of workflow artifacts saved for debugging.</p>
Temporary directories	<p>User-specified directories on the managed server that hold temporary files. Some directories may contain installation binaries or patches that are either stored on the managed server or downloaded from Server Automation. Other directories may contain extracted ZIP files.</p> <p>Common parameter names are: Staging Directory, Download Location, Extract Location, Archive Location, and Download Target Destination.</p>	<p>Adequate disk space must be available in the temporary directories to avoid workflow failures. The size depends upon which workflows will be executed on a target and whether or not temporary files are deleted upon workflow completion.</p> <p>Refer to the workflow documentation for disk space requirements.</p>

## Pre-installation tasks

This section describes all the tasks that must be performed before you can install DMA.

- ["Meet the hardware and software requirements" on the next page](#)
- ["Obtaining a signed server certificate" on page 15](#)
- ["Configuring the Oracle database" on page 16](#)
- ["Configuring the Oracle database" on page 16](#)

## Meet the hardware and software requirements

Make sure that your system meets all of the software and hardware requirements for installing DMA.  
For more information, view the ["Requirements" on page 6](#) section of the Support matrix.

## 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:** Ensure 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 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. For instructions to import the signed certificate, see the [Configuring SSL on the DMA Server](#) section in the Administration guide.

## Configuring the Oracle database

This section describes how to create and configure the Oracle database used by DMA.

Before you configure the database:

- Ensure you have a username and password for this Oracle database.
- Have your database administrator (DBA) create an Oracle Database Enterprise Edition database to be used by DMA. Make sure the Oracle Listener and database are up and running.
- Have your DBA create the Oracle instance and the two tablespaces.
- Ensure the Oracle Database is up and running before installing DMA.
- Make sure the Oracle Listener is up and running.

## Steps to Configure the Oracle Database

Perform the following steps to configure This section shows you how to configure an Oracle database that will be used by DMA.

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

In the following commands, 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. 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 ["DMA baseline options" on page 28](#).

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

- In most cases, run the `sqlplus / as sysdba` command.
- If you have multiple databases setup with remote authentication configured, run the following command:

```
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 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 the Database password has changed section in the *Troubleshooting Guide*.

**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 DMA.

Before you configure the database:

- Ensure you have a username and password for this PostgreSQL database.
- Have your database administrator (DBA) create a PostgreSQL 9.3.5 database to be used by DMA. Make sure the PostgreSQL service and database are up and running.
- Have your DBA create the PostgreSQL instance and the two tablespaces.
- Ensure the PostgreSQL database is up and running before installing DMA.

## Steps to Create and Configure the PostgreSQL Database

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

In the following commands, 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 :

```
psql <database name> as sysdba.
```

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

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

# Choose your installation method

Choose the installation method that you want to use to install Database and Middleware Automation 10.50.001.000.

- ["Regular installation" below](#)
- ["Silent installation" on page 31](#)

## Regular installation

To perform the regular installation, perform the following steps in the prescribed order:

Topic	Description
<a href="#">"Installing DMA Server"</a>	Step-by-step instructions about how to install the DMA server.
<a href="#">"Installing DMA Client for SA"</a>	Step-by-step instructions about how to install the DMA client.

**Note:** An automated script is available that can speed up the installation process. For information about this script, see [Automated DMA Installation](#).

## Installing DMA Server

This section contains the steps to install the 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 31](#) section for instructions.

In the following commands, replace the variables (found within <>'s) with the 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 <a href="#">"Configuring the Oracle database" on page 16</a> or <a href="#">"Configuring the PostgreSQL database" on page 19</a>
<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 <a href="#">"Configuring the Oracle database" on page 16</a> or <a href="#">"Configuring the PostgreSQL database" on page 19</a>
<DMA_server>	dma.mycompany.com	Fully qualified host name of the DMA server.  <b>Note:</b> Here, the fully qualified host name is not the localhost.
<Oracle_SID>	dma	Oracle Database Instance—the same instance that you used when you created your Oracle database in <a href="#">"Configuring the Oracle database" on page 16</a>
<database_name>	dma	PostgreSQL instance—the same instance that you used when you created your PostgreSQL database in <a href="#">"Configuring the PostgreSQL database" on page 19</a>
<Oracle_Server>/<PostgreSQL server>	oracle.mycompany.com	Fully qualified host name of the Oracle Database/PostgreSQL server—must be the same

		<p>server that you used when you created your Oracle/PostgreSQL database in <a href="#">"Configuring the Oracle database" on page 16</a> or <a href="#">"Configuring the PostgreSQL database" on page 19</a></p> <p><b>Note:</b> Here, the fully qualified host name is not the localhost.</p>
<code>&lt;jdbc_string&gt;</code> (Oracle)	<code>jdbc:oracle:thin:@ oracle.mycompany.com: 1521:dma</code>	<p>Java Database Connectivity (JDBC) connection string in the following format:</p> <p><code>jdbc:oracle:thin:@&lt;Oracle_Server&gt;: 1521:&lt;Oracle_SID&gt;</code></p> <p>You can also specify other connection string syntax. Consult your Oracle DBA for the company standard.</p>
<code>&lt;jdbc_string&gt;</code> (PostgreSQL)	<code>jdbc:postgresql:// postgres.mycompany.com:5432/postgres</code>	<code>jdbc:postgresql://&lt;postgres_server_name&gt;:5432/&lt;database_name&gt;</code>
<code>&lt;SA_Server&gt;</code>	<code>saserver.mycompany.com</code>	Fully qualified host name of the Server Automation server.

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

1. Obtain the `dma-server-10.50.001.000-0.x86_64.rpm` file from the DMA installation folder under the `DMA_10.50.001.000_Server_and_Client` folder.
2. Run the following commands as root to install the DMA server:

```
$ cd DMA_10.50.001.000_Server_and_Client
```

```
$ rpm -ivh dma-server-10.50.001.000-0.x86_64.rpm
```

**Note:** Run the installation command only one time.

After the installation is complete, the following message is displayed:

Please redeem your licenses (using your SA ID) from Portal, using the `<lock ID>`. Server will be operational using the default license in place.

By default, DMA is installed with the `-instantOn` (trial) license.

**Note:** The `-instantOn` (trial) license is valid for 90 days. This is applicable for 10 database

licenses and 10 middleware licenses.

Save the <Lock ID> for your reference, as it is needed to generate your license(s). You can generate the license(s) at [Software Licensing](#) website.

**Note:** The <Lock ID> is also available in the Licensing Dashboard at [Software Licensing](#) website, after you apply the valid license.

After generating the license, copy the file to `/opt/hp/dma/server/lic/licImport/` folder. You can choose to apply the license while baselining the database in the next step or at a later time. For instructions to apply the license, see the ["Applying the license" on page 30](#) topic.

3. Baseline your database. This will create your schema and put the database into the default state. Run the following command 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 ["DMA baseline options" on page 28](#).

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>
```

If you have created a table space data file and an index file other than the default `hpdma_data` data file and `hpdma_indx` index file, use the `--tablespace-data` and `--tablespace-indx` options.

Baseline your database for PostgreSQL by running the following commands:



```
$ 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
```

**Note:** If you have more than one DMA Server connected to a single database, run the baseline command only from the primary DMA server. Also, redeem the licenses only for the LockID of the primary server.

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

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

**Note:** Run this command every time the SA Core is upgraded.

If you receive an error that the Oracle Listener is not running, perform the following troubleshooting steps:

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

```
su - oracle

ps -ef | grep tns
```

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

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

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

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

For other baseline error troubleshooting information, see the [Common baseline errors](#).

You have completed installing the initial stage—the command line setup—of the DMA server.

In the next stage you will configure SSL on the DMA server.

## Start DMA

The first time you start DMA you must log in as the default initial DMA administrator (dma\_initial\_admin) to configure the operating environment.

1. As root, start the DMA 10.50.001.000 server. For example:

```
$ service dma start
```

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

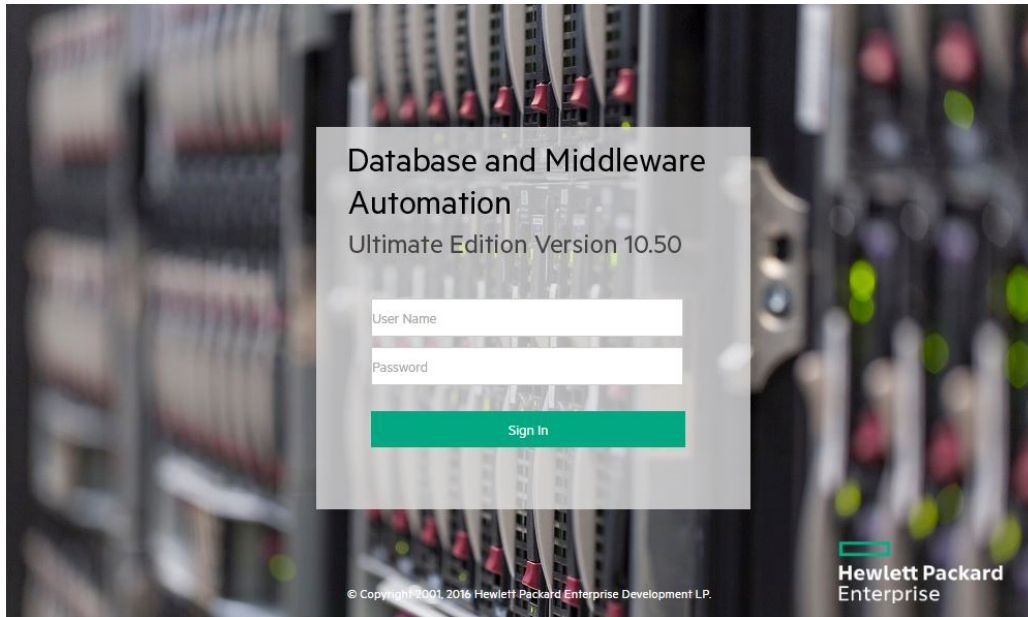
`https://<DMA_Server>:8443/dma`

Here, <DMA\_Server> is the fully qualified host name of your 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:



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.

Next, perform the initial DMA setup using the DMA user interface. For more information about setting up DMA, see the Setting up DMA section in the *Administration Guide*.

## 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 <server.xml>	server.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 DMA server, that can resolve into either an IPv4 or IPv6 address.  <b>Note:</b> 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.  <b>Caution:</b> Do not do this unless instructed to by Support.
-lic,--apply-license <arg>		License file that is to be applied
-licref,--lic-data-refresh		Refreshes the current licenses

Option	Example Argument Value	Description
		consumed/available in dma server
-lockid,--license-lockid <arg>		ID against which license is generated
-jdbc,--jdbc-connection-string <connectionString>	jdbc:<DBTYPE>:thin:@ <HOST>:<TNS_PORT>: <SID>  or jdbc:<DBTYPE>:thin:@// <HOST>:<TNS_PORT>/ <ORACLE_SERVICE_NAME>	The Java Database Connectivity (JDBC) Connection String used to connect to the database. The default <TNS_PORT> is 1521.  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  <b>Caution:</b> Do not do this unless instructed to by 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.

**Note:** If you have more than one DMA Server connected to a single database, run the baseline command only from the primary DMA server. Also, redeem the licenses only for the LockID of the primary server.

## Applying the license

To apply the license, run the baseline command with the following options:

<code>--apply-license &lt;arg&gt;</code>	Fully qualified path of the license file that is to be applied
<code>--license-lockid &lt;arg&gt;</code>	ID against which the license is generated

You must specify the above two license options in the baseline command, after you have created the table space data file and index file.

## Installing DMA Client for SA

This section information about installation of the DMA Client for SA on the DMA server.

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

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

On the DMA server, get the `dma-sa-client-10.50.001.000-0.x86_64.rpm` file from the DMA installation zipped folder under the `DMA_10.50.001.000_Server_and_Client` folder, and then run the following commands as root:

```
$ cd DMA_10.50.001.000_Server_and_Client
```

```
$ rpm -ivh dma-sa-client-10.50.001.000-0.x86_64.rpm
```

You have completed installing the DMA Client for SA.

In the next stage you will integrate DMA with Server Automation. For information about integrating DMA with Server Automation, see the Integration Guide.

## Silent installation

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

The automated installation works for the following configuration:

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

Using the automated installation simplifies and speeds up the installation, so that you do not need to key in lengthy commands (for example, configuring the DMA database and running the RPMs). The automated process performs the following tasks:

- Installs DMA on a single server when Oracle database is already installed and the SA installation already exists:

- Configures the Oracle database for DMA
- Installs the DMA Server
- Installs the DMA Client for SA

**Note:** If you want a more complex DMA configuration (for example, high available or disaster recovery), you must install DMA by following the instructions in the section .

The DMA\_10.50.001.000\_Install folder also contains the following scripts:

File Name	Description
dma_install.sh install-options.txt installhelperscript.sh	Scripts that automate the installation of DMA
dma_remove.sh remove-options.txt removehelperscript.sh	Scripts that automate the removal of DMA. For information about automated uninstallation, see <a href="#">"Silent uninstall" on page 62</a> .

**Note:** Before you begin to install DMA, read ["Requirements"](#) and ["Process overview"](#) to ensure that it is appropriate for your environment.

## Requirements

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

- The requirements in the following sections:
  - ["Requirements" on page 6](#)
  - ["Performance and sizing"](#)
- Your DBA has created an Oracle database to be used by DMA. The Oracle Listener and database are up and running.

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

- You have downloaded the DMA 10.50.001.000 installation binaries.
- You have credentials to log in as root on the server where you run the script.
- The password for the Oracle root user, in case the DMA database is not on the DMA Server.



## Process overview

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

Automation step	Replaces manual installation section
<p>Adds the Oracle listener to <code>listener.ora</code>, if the entry does not already exist. Adds the DMA tablespaces, creates the DMA user credentials, grants the user the requisite permissions, and then sets the quota to unlimited for the data and index tablespace files.</p>	<p>"Configuring the Oracle database"</p>
<p>Unpacks and installs the DMA Server RPM file from the DMA 10.50.001.000 installation folder. For example:</p> <pre data-bbox="240 800 1047 863">/ &lt;mnt_dir&gt; /DMA_10.50.001.000_Server_and_Client/dma-server-10.50.001.000-0.x86_64.rpm</pre> <p>Creates the baseline using the <code>dmaBaselineData.sh</code> script. Copies the required JAR files from the SA Server to the DMA Server using the <code>copyJars.sh</code> script.</p>	<p>"Installing DMA Server"</p>
<p>Unpacks and installs the DMA client for SA RPM file from the DMA 10.50.001.000 installation folder. For example:</p> <pre data-bbox="240 1041 1089 1104">/ &lt;mnt_dir&gt; /DMA_10.50.001.000_Server_and_Client/dma-sa-client-10.50.001.000-0.x86_64.rpm</pre>	<p>"Installing DMA Client for SA"</p>

## Perform the automated installation of DMA

Perform the following steps as root user:

1. Download and extract the installation files.
2. Set up the installation parameters:
  - a. Open the `install-options.txt` file in a text editor. For example:

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

- b. Specify values for the parameters:

Parameter	Example	Description
sa	saserver.mycompany.com	Server Automation host address.
sid	orcl	Oracle SID of the DMA database. If SA and DMA share the same database, specify the SA SID.
dma_db_host	dmaserver.mycompany.com	The host address where the DMAOracle database is located. May be either the 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	DMA database username to be used after the database is created.
dbpass	<dma_password>	DMA database password to be used after the database is created.
filesize	100M	Maximum file size of datafile, in MB.

- c. Save your changes to the `install-options.txt` file.
3. Run the script that automates the process to install DMA:
  - a. Start the script in the installation folder:

```
$ cd /<mnt_dir>/DMA_10.50.001.000_Install
```

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

The script displays log information while running.

If the DMA database is not on the DMA Server, specify the password for the Oracle root user when prompted.

- b. The following is an example execution:

```
STARTING DMA INSTALLATION
#####
<<<< Loading the options file.. >>>>
<<<< DMA installation starting >>>>
#####
Launching DMA Installation..
+DMA Host          = dmaserver.mycompany.com
+DMA Pack          = ../DMA_10.50.001.000_Server_and_Client/dma-
server-10.50.001.000-0.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
#####
DMA 10.50.001.000.0 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/server.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/server.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 --:--:-- --:--:-- --:--
-:--      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 --:--:-- --:--:-- --:--
-:--      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 --:--:~ --:~:~ --:~
-:~      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-10.50.001.000-0.x86_64 is already installed
<<<< Setting up server.xml >>>>
<<<< Going to start/restart DMA service now! >>>>
Removing old working dir of /var/opt/hp/dma/work/dma
Starting 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/tomcat-juli.jar
Tomcat started.
#####
DMA install is complete. Please launch
https://dmserver.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
#####
```

## Verify the automated installation of DMA

Perform the following steps to verify if 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 DMA web interface is available—and then close.
3. Integrate DMA with Server Automation. Follow the instructions in the Integrate with SA section in the *Integration Guide*.
4. Configure SSL. Follow the instructions in the Configure SSL on the DMA Server section in the *Installation Guide*.
5. Start the DMA Server. Follow the instructions in the Start DMA section in the *Installation Guide*.
6. Set up DMA. Follow the instructions in the Set up DMA section in the *Installation Guide*.

You now have DMA up and running.

## Post-installation task

After you install DMA 10.50.001.000, you must perform the following task:

- ["Configure SSL on the DMA Server" on the next page](#)
- ["Set up DMA" on page 49](#)
  - ["Configure the Connector" on page 49](#)
  - ["Register DMA roles" on page 52](#)
  - ["Assign DMA capabilities" on page 54](#)
  - ["Add available targets" on page 55](#)
  - ["Import a solution pack" on page 58](#)

# Configure SSL on the DMA Server

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

1. ["Generate a Private Key for the Server" on the next page](#)
2. ["Generate the Certificate Signing Request to Obtain Signed Server Certificates" on page 42](#)
3. ["Import the SSL Server Certificates" on page 43](#)
4. ["Configure the DMA Server to Use Your Certificate" on page 45](#)
5. ["Verify the SSL Connection" on page 47](#)

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 DMA server.

For detailed instructions and an example of the `keytool` command that sets up the SAN, see the Using a proxy server topic in the *Administration Guide*.

**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 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
```

## Generate a Private Key for the Server

The first step in configuring SSL on the 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 exist, the `keytool` will create it.

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

1. Log in to the 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, you must set up the SAN, see the Using a proxy server topic in the *Administration Guide* for steps 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 is used to associate the server certificate with its private key. For DMA, set to <code>tomcat</code> .
<DMAserver>	Fully qualified host name of the server hosting the 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: <code>/opt/hp/dma/server/.mykeystore</code>

<code>&lt;numberdays&gt;</code>	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>
```

## Generate 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 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 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
```

Your certificate request will appear on stdout.

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

**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.

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

## Import the SSL Server Certificates

This section provides the information about importing the SSL Server certificates into the keystore.

**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 is 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

- 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
```

- 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. 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>

```

## Configure the DMA Server to Use Your Certificate

After you add your server certificate to the keystore, perform the following steps:

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

**To configure the DMA server to use your certificate:**

1. As root, stop the 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.

- 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
<code>&lt;keyalias&gt;</code>	Unique alias for the server's private key (see <a href="#">"Generate a Private Key for the Server" on page 41</a> ).
<code>&lt;SSLport&gt;</code>	Port that is used for: <ul style="list-style-type: none"> <li>SSL communication between the DMA Server and the DMA clients</li> <li>Accessing the DMA user interface</li> </ul>
<code>&lt;storefile&gt;</code>	Keystore file name. For example: <code>/opt/hp/dma/server/.mykeystore</code>
<code>&lt;password&gt;</code>	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" />
```

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

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

- Identify the following line:

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

- 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://<DMA Server>:8443/dma"/>
```

For example:

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

11. Ensure that the `<DMA Server>` specified in the `webServiceUrl` value matches the `<DMA Server>` 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://<DMA Server>:<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 `server.xml` file.
14. As root, start the DMA Server by using the following command:

```
service dma start
```

## Verify the SSL Connection

To verify your SSL connection, perform the following steps:

1. Log in to your DMA server.
2. HTTPS protocol indicates that the DMA Server is communicating with the DMA Client using SSL.
3. The lock icon () in the address bar indicates that the DMA Server is communicating with the 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 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.
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 to ["Configure the DMA Server to Use Your Certificate" on page 45](#), modify the `server.xml` file, and then execute the deployment again.

You have completed configuring SSL on the DMA server.

In the next section you will install the DMA client for SA.



## Set up DMA

This section shows you how to initially set up DMA.

Two different DMA administrators must configure the DMA operating environment.

1. The initial default administrator, `dma_initial_admin`, must perform the following steps:
  - ["Configure the Connector" below](#)
  - ["Register DMA roles" on page 52](#)
  - ["Assign DMA capabilities" on page 54](#)
2. Next, an DMA user whose role has Administrator capability—for example, the DMA Admins role—must perform the following steps:
  - ["Add available targets" on page 55](#)
  - ["Import a solution pack" on page 58](#)

## Configure the Connector

This topic shows you how to configure the Connector that enables DMA and SA to communicate.

**Note:** You must configure the Connector only once.

Before you configure the Connector, you must copy the JAR files from SA server to be able to use the Connector. Perform the following steps to copy the JAR files and configure the Connector.

**Note:** These instructions assume that Server Automation is your server management tool.

DMA provides a script to copy the JAR files from the intended SA Core so that DMA can use the Connector.

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

**Caution:** Only connect to a different SA Core within the same SA Mesh.

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

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

Here, `<SA_Server>` is the fully qualified host name of the SA Server to use as the SA Core.

In the DMA user interface, you must supply the credentials to connect to the intended SA Core.

To configure the Connector:

1. Log in as `dma_initial_admin`.
2. Go to **Setup > Connectors**.
3. If a Connector already exists, click the tab that corresponds to the Connector for SA.

To add a new Connector, click **Add Connector** in the lower right corner.

4. Specify the information required.

For the Server Automation Connector, you would specify the host name, SA user name, and SA user's password:

The screenshot shows the 'Connector' configuration page in the DMA user interface. The page has a header with tabs: Configuration, Permissions, Capabilities, Roles, and Connector. The 'Connector' tab is selected. Below the tabs, there is a section titled 'Connector' with a blue help icon. Inside this section, there is a text input field containing 'SAsrvr001.mycompany.com'. Below this, there are three labeled input fields: 'Server Automation Host:' with the value 'SAsrvr001.mycompany.com', 'Server Automation Username:' with the value 'dma\_integration\_user', and 'Server Automation Password:' with a masked password represented by dots.

The user specified here must be a valid SA user with 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 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.

5. Click **Save**.

DMA performs a test to ensure that it can communicate with the server that you specify.

6. Stop and restart your DMA server:

```
# service dma stop
```

```
# service dma start
```

1. The older roles disappear from the Registered roles list.
2. Assign capabilities and permissions to these new roles.
3. (Optional) On the newly connected SA add the target servers and remediate.
4. Logout and login from DMA with proper user and check Environment tab to see that the latest servers are listed in Add Server section.

If yes, SA connector has been changed successfully.

## Register DMA roles


This topic shows you how to register the DMA roles.

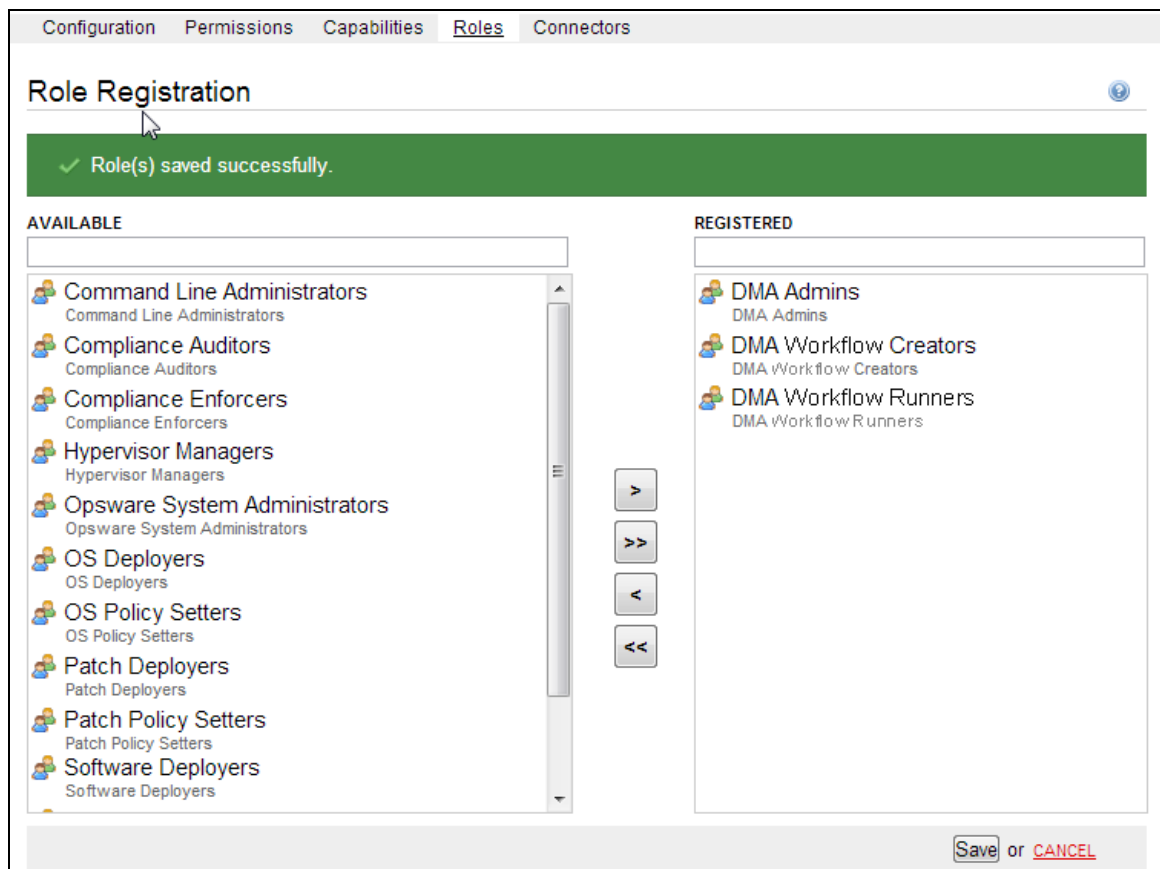
DMA obtains the complete set of available roles from Server Automation including the groups that your SA administrator configured while integrating DMA with SA. For more information, see the [Setting SA groups and users](#) section in the [Installation Guide](#).

While you are logged in as `dma_initial_admin`, do the following to register the roles that you want to use:

1. Go to **Setup > Roles**.

The roles that are available to be registered are listed on the left. The roles that are already registered are listed on the right.

2. Select a user group from the AVAILABLE list on the left and then click the  button. The selected role moves to the REGISTERED list on the right.



3. Click **Save** to save your changes.
4. Repeat the steps for all the roles that you want to register.

**Note:** When you register a new role, the **Login Access** capability is assigned to that role by default. You can disable this Capability in the **Setup > Capabilities** tab. For more information about Capabilities, see ["Assign DMA capabilities" on the next page](#).

## Assign DMA capabilities

This topic shows you how to assign DMA capabilities.

Capabilities are collections of related privileges. You must assign capabilities to each role that you registered in the previous step.

While you are logged in as `dma_initial_admin`, do the following to assign capabilities to roles:

1. Go to **Setup > Capabilities**.
2. Select a role on the left.
3. To assign a capability to a role, select the desired capabilities.

Role	Login Access	Workflow Creator	Administrator
DMA Admins	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DMA Workflow Creators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
DMA Workflow Runners	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

[LOGIN ALL](#) [CREATOR ALL](#) [ADMINISTRATOR ALL](#)

**Note:** Only the users with roles that have Administrator capability can import solution packs.

4. Click **Save** in the lower right corner.
5. Log out of DMA.

**Note:** This logs you out as the default initial administrator, `dma_initial_admin`.

**Note:** When you register a new role, the **Login Access** capability is assigned to that role by default. You can disable this Capability in the **Setup > Capabilities** tab.

## Add available targets

This task must be performed by the DMA Admin only.

This topic shows you how to make target servers available to DMA users. To perform all the tasks documented in this topic, you must log in to DMA as a user with Administrator capability, for example, a user with the DMA Admins role.

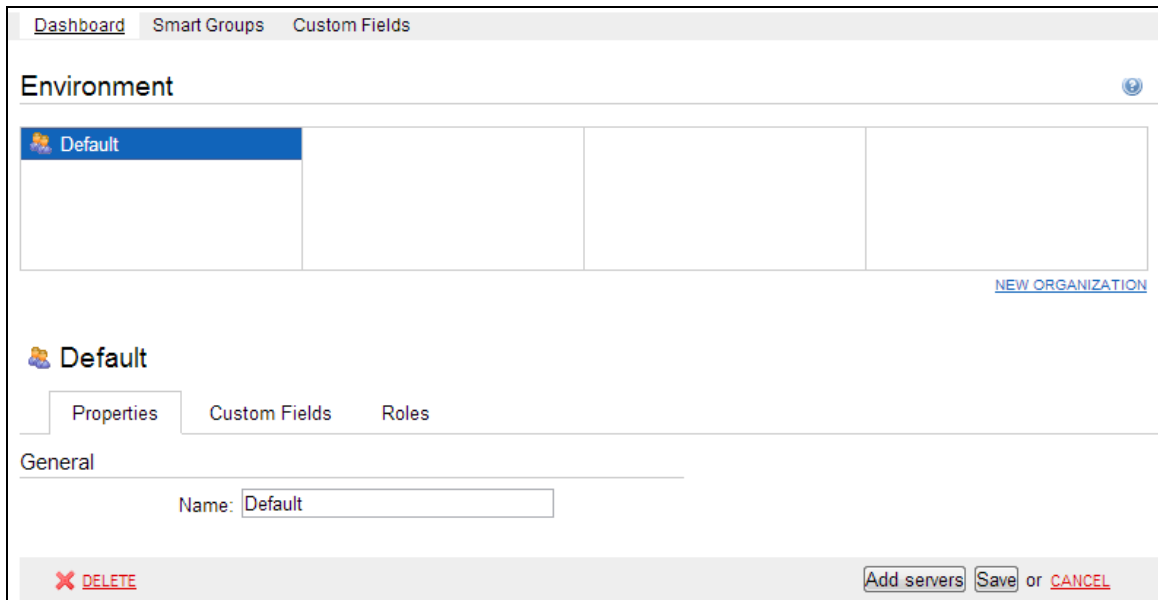
**Note:** If you receive an error, see the *Troubleshooting Guide*.

## Add servers

To add servers, perform the following steps:

1. Go to the **Environment** page.
2. In the top Environment box, click **Default**.

**Note:** If you want to create and use other organizations, refer to the *DMA Administrator Guide*.



The screenshot shows the 'Environment' page in the DMA interface. At the top, there are tabs for 'Dashboard', 'Smart Groups', and 'Custom Fields'. Below these is the 'Environment' header with a help icon. A table lists the available environments, with 'Default' selected and highlighted in blue. To the right of the table is a link for 'NEW ORGANIZATION'. Below the table, the 'Default' organization is expanded, showing tabs for 'Properties', 'Custom Fields', and 'Roles'. The 'General' tab is active, displaying a 'Name' field with the value 'Default'. At the bottom of the page, there is a 'DELETE' button with a red 'X' icon, and a row of buttons: 'Add servers', 'Save', and 'CANCEL'.

3. Click **Add servers** in the lower right corner. A new page is displayed.

4. Select any servers that you want to use as DMA targets.



**Note:** If no servers are available to add to the organization, see the *Troubleshooting Guide*.

5. Click **Add** and then click **Save** in the lower right corner.

## Granting permissions

To grant user roles permission to access the servers, do the following:

1. Go to **Setup > Permissions**.
2. Select the name of the role to which you want to grant server permissions, for example: DMA Admins.
3. Click **Organizations**.



4. Select the appropriate permissions for this role, for example: Read, Write, and Deploy.

The screenshot shows the 'DMA Admins' configuration interface. At the top, there are tabs for 'Configuration', 'Permissions' (selected), 'Capabilities', 'Roles', and 'Connector'. Below this, the 'DMA Admins' title is followed by sub-tabs: 'Deployments', 'Workflows', 'Steps', 'Policies', and 'Organizations' (selected). A search bar is present above a table. The table has columns for 'Organization', 'Read', 'Write', and 'Deploy'. The 'Default' organization is listed with all three permissions checked. Below the table are links for 'READ ALL', 'WRITE ALL', and 'DEPLOY ALL'. At the bottom right, there is a 'Save' button and a 'CANCEL' link.

Organization	Read	Write	Deploy
Default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[READ ALL](#) [WRITE ALL](#) [DEPLOY ALL](#)

**Save** or [CANCEL](#)

5. Click **Save** in the lower right corner.

## Import a solution pack

A solution pack is a set of DMA workflows, steps, functions, and policies that address a specific process or problem—such as database provisioning or application server patching. Each solution pack contains the following items:

- Workflow templates for commonly-recurring IT administration tasks
- Workflow steps to provide an automation library
- Functions that implement step actions
- Policies that define desired automation behavior
- Documentation that defines best practices followed in the workflow templates

This task must be performed by the DMA Admin only.

The following instructions assume that you have purchased a license for DMA. These instructions apply to any solution pack.

**Note:** Always check to see if there are more recent DMA patches available online. Due to frequent releases, it is possible that the solution packs provided on the installation media have been updated.

**Tip:** You should import the Discovery solution pack first. It is not automatically installed in DMA. You must import it if you want to use the discovery workflows.

## Obtaining the patch files

To obtain the most recent DMApatch files, perform the following steps:

1. Go to the following web site: <https://softwaresupport.hpe.com/>
2. Sign in using your HP 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, do the following:

- a. Click the link for the desired patch.
- b. Under **Download Information**, click the link to download the patch installation media.

## Accessing the DMA solution packs

To access the DMA solution packs, mount the ISO file of the DMA10.50.001.000 (or patch) installation media.

The solution packs are located in the following folders:

- The `DMA_10.50.001.000_Server_and_Client` folder contains the Discovery and Promote solution packs.

The Discovery solution pack is not automatically installed with DMA. You must import it if you want to use the discovery workflows.

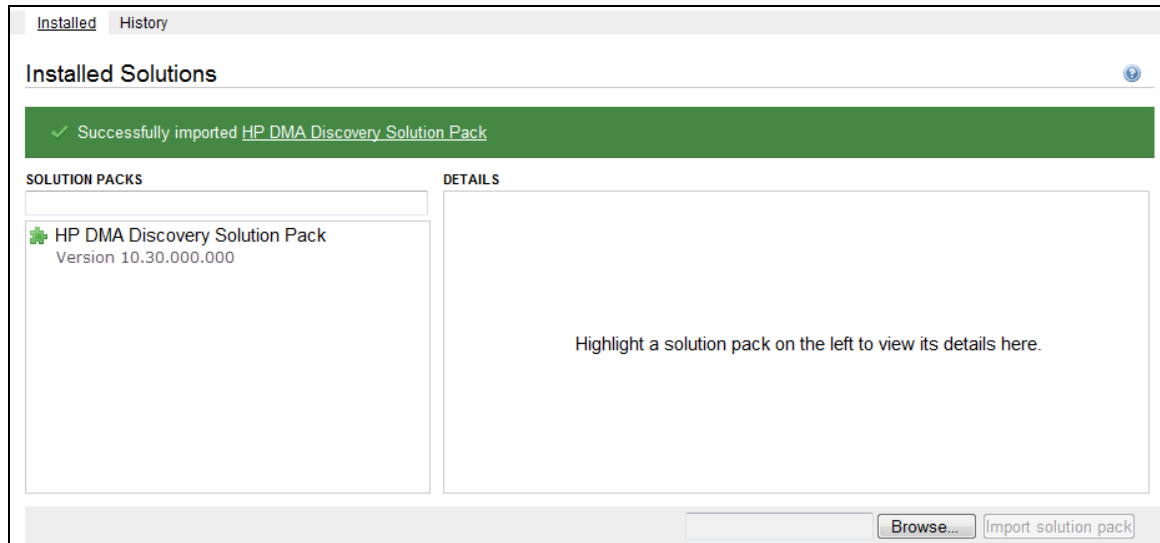
- The `DMA_10.50.001.000_Database_Solution_Packs` folder contains all of the database solution packs (provisioning, advanced provisioning, patching, advanced patching, compliance, refresh, and release management).
- The `DMA_10.50.001.000_Middleware_Solution_Packs` folder contains all of the application server solution packs (provisioning, patching, configuration management, and release management).

## Importing the solution pack

Perform the following steps to import the solution pack:

1. On the system where you have downloaded the installation files, open a web browser, and go to the following URL:  
  
`http://<DMA_server>/dma/login`
2. Log in to the DMA server using an account with Administrator capability.
3. On the **Solutions > Installed** tab, click **Browse** in the lower right corner. The **Choose File** dialog opens.

**Note:** **Browse** and the **Choose File** dialog box may have different names depending on the browser that you are using.



4. Locate and select the ZIP file for the desired solution pack, and click **Open**.
5. Click **Import solution pack**.

To view basic information about the solution pack, hover your mouse over its name in the left pane.

To view detailed information about the solution pack, click its name in the left pane. To view a list of the workflows that the solution pack contains, go to the **Workflows** tab.

This completes the initial set up process.

## Versioning and importing Solution Packs

You may not import a solution pack with a lower version than your currently existing solution pack. To return to a previous solution pack, use the Rollback feature. For more information, see the Roll back a Solution pack topic in the *Administration Guide*.

If you import two solution packs that share a component, the shared component is imported only once, and the higher-versioned component takes precedence over the lower-versioned component—provided both components are locked. For example:

- Say that solution pack X is installed, and it includes step ABC, version 2.
- Later, you import solution pack Y, which includes step ABC, version 1.
- In this case, step ABC is a shared component. The higher version of step ABC (version 2) takes precedence over the lower version (version 1), so version 2 is shared by both solution packs.

**Note:** The import process fails if it encounters an unlocked item (workflow, step, function, or policy) that needs to be updated. The import process also fails if the solution pack to be imported includes a step that has the same name and version as an existing step, but the steps differ in some way. This is a change from the previous behavior which was to overwrite the existing step if the names and versions were the same.

**Note:** An existing function with the same name as an imported function is always overwritten.

After you have imported a solution pack, you can run a workflow. For more information about workflows, see [Use](#).

## Uninstall DMA 10.50.001.000

Choose your unistallation method:

["Uninstall" below](#)

["Silent uninstall" on the next page](#)

## Uninstall

This section provides information on how to uninstall DMA from the DMA Server and the DMA managed servers.

**Note:** An automated script is available that can speed up the uninstallation process if DMA was installed with the automated install process. For information about this script, see ["Silent uninstall"](#).

Perform the following steps to uninstall DMA from the DMA Server:

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

```
$ service dma stop
```

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

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

You can locate the current version of 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 DMA is 10.50.001.000, your results will look like this:

```
dma-server-10.50.001.000-0.x86_64.rpm
dma-sa-client-10.50.001.000-0.x86_64.rpm
```

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

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

Here, replace `<DMA_Version>` with the DMA version from your query.

4. After uninstalling DMA, to finish cleaning up remove the following folders:

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

## Uninstall DMA from the Managed Servers

To uninstall DMA from the managed servers (the DMA Client), perform the following steps:

1. In SA, detach the managed server from the DMA Client Files policy and then remediate the target.
2. To completely remove 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 DMA, work with your Oracle DBA/PostgreSQL to uninstall the DMA schema and tablespaces from Oracle Database/PostgreSQL and work with your SA administrator to remove the DMA integrations with SA.

## Silent uninstall

The automated DMA uninstallation allows you to uninstall DMA that was installed using the automated installation. If DMA was installed manually, you need to uninstall DMA by following the instructions at ["Uninstall"](#).

You can choose to uninstall DMA's Oracle database based on an input parameter.

**Note:**

Before you begin to install DMA, read ["Requirements"](#) and ["What the process does"](#) to ensure that it is appropriate for your environment.

## Requirements

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

- You have downloaded and extracted the DMA 10.50.001.000 installation folder.
- You have credentials to log in as root on the server where you run the script.
- You have the Oracle user and password for the DMA database.
- You have the password for the Oracle root user, in case the DMA database is not on the DMA Server.

## What the process does

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

Automation step	Replaces manual installation section
<div>Removes the Oracle tablespaces and datafiles that DMA created. Runs the RPM commands to uninstall the DMA Server and the SA Client. Deletes the DMA folders.</div> <div><b>Note:</b> The script does not remove the user because Oracle is still active, the 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.</div>	<a href="#">"Uninstall"</a>

## Performing the automated uninstallation of DMA

Perform the following steps as root user:

1. Set up the uninstallation parameters:
  - a. Execute the following command to determine which RPM packages are installed:

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

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

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

- c. Specify values for the parameters:

Parameter	Example	Description
<code>dmapack</code>	<code>dma-server-10.50.001.000-0.x86_64.rpm</code>	The DMA Server RPM filename for the current version of DMA (do not include <code>.rpm</code> ).
<code>sacient</code>	<code>dma-sa-client-10.50.001.000-0.x86_64.rpm</code>	The DMA SA Client RPM filename for the current version of DMA (do not include <code>.rpm</code> ).
<code>sa</code>	<code>saserver.mycompany.com</code>	Server Automation host address.
<code>sid</code>	<code>orcl</code>	Oracle SID of the DMA database. If SA and DMA share the same database, specify the SA SID.
<code>dma_db_host</code>	<code>dmasever.mycompany.com</code>	The host address where the DMA Oracle database is located. The value may either be the DMA Server host address or the SA Server host address.
<code>dbuser</code>	<code>dma</code>	DMA database username. Only needed if <code>remove_dma_db</code> is set to true.
<code>dbpass</code>	<code>&lt;dma_password&gt;</code>	DMA database password. Only needed if <code>remove_dma_db</code> is set to true.
<code>remove_dma_db</code>	<code>false</code>	Determines whether the DMA tables and data will be completely removed. Valid values are true and false.  <b>Tip:</b> Leaving the DMA tables and data intact can be useful in a development environment.

- d. Save the changes you made to the `remove-options.txt` file.



## 2. Run the script that automates the process to uninstall DMA:

### a. Start the script in the installation folder:

```
$ cd /<mnt_dir>/DMA_10.50.001.000_Install
$ ./dma_remove.sh <local_dir>/remove-options.txt
```

The script displays log information while running.

When prompted to continue the uninstallation script, respond yes.

If the DMA Oracle database is not on the DMA Server, specify the password for the Oracle root user when prompted..

### 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.hpswlab.s.adapps.hp.com
+DMA Pack           = dma-server-10.50.001.000-0.x86_64
+SA Host            = IWFVM00597.hpswlab.s.adapps.hp.com
+SID                = orcl
+DB User            = dma
+Data Tablespace Name = HPDMA_DATA
+Idx Tablespace Name = HPDMA_INDX
#####
<<<< The DMA DB will be removed now. >>>>
Dropping user
Dropping Tablespace
User and Tablespaces removed successfully
<<<< Stopping DMA and removing it now.. >>>>
Stopping 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/tomcat-juli.jar
waiting for processes to exit
waiting for processes to exitShutting down DMA service before
uninstalling DMA.
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
-----

```

## Verify the automated uninstallation of DMA

Perform the following steps to verify if the automated uninstallation is complete:

1. Verify that you received the "DMA server has been removed successfully.." message. If not, 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 DMA from the managed servers:
  - ["Uninstall"](#)
  - ["UninstallDMA from the Managed Servers" on page 62](#)
4. If the script removed the DMA database, your Oracle DBA can now delete the DMA user.
5. Your SA administrator can now clean up the DMA integrations with SA.

You have successfully uninstalled DMA!

## 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 10.50.001.000)**

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](mailto:hpe_dma_docs@hpe.com).

We appreciate your feedback!