

HP Database and Middleware Automation

For Red Hat Enterprise Linux and SUSE Enterprise Linux

Software Version: 10.21

Installation Guide

Document Release Date: October 2014

Software Release Date: July 2014



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2012-2014 Hewlett-Packard Development Company, L.P.

Trademark Notices

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

UNIX® is a registered trademark of The Open Group.

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

Documentation Updates

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

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to: <http://h20230.www2.hp.com/selfsolve/manuals>

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: <http://h20229.www2.hp.com/passport-registration.html>

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

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

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

Document Changes

Chapter	Version	Changes
Pre-Installation Requirements	10.01	Instructed user to check online for updated versions. Added a supported operating system.
How to Install HP DMA	10.01	Reorganized chapter to clarify what tasks are done by the SA administrator.
How to Upgrade HP DMA	10.01	Added instructions to upgrade from HP DMA 10.00 to 10.01.
How to Link HP DMA into HP Server Automation	10.01	Replaced the "How to Deactivate Outdated Versions of HP DMA" chapter with this chapter.
Special Configurations	10.01	Added new chapter.
Troubleshooting	10.01	Added new chapter.
Title Page Legal Notices	10.10	Updated version number, software release date, document release date, and copyright date range.
Pre-Installation Requirements	10.10	Added requirement to obtain an SSL Certificate.
How to Install HP DMA	10.10	Modified the instructions. Updated screen shots. Added instructions to configure SSL.
How to Upgrade HP DMA	10.10	Modified the instructions to upgrade from 10.01 (or 10.00) and to revert back to 10.01.
Special Configurations	10.10	Added additional configurations.
Troubleshooting	10.10	Added additional troubleshooting information.
APX Tool Configuration Error	10.10	Added new section of troubleshooting information.
Title Page Legal Notices	10.20	Updated version number, software release date, document release date, and copyright date range. Added SUSE platform.
Other Requirements	10.20	Added information that HP DMA and SA servers can be collocated.

Document Changes, continued

Chapter	Version	Changes
Supported Products and Platforms	10.20	Included support for HP Server Automation SAVA and Enterprise Edition. HP DMA can be installed on SUSE Enterprise Linux. Only supported on Oracle 11g R2.
Import the HP DMA APX How to Upgrade HP DMA Specify a Renamed Windows Administrator User HP Software Documentation	10.20	Added instructions to use the HP Live Network connector to update westAPX with the additional Update WestAPX for Windows User.
Steps to Create and Configure the Oracle Database Common Baseline Errors	10.20	The TNS listener needs to be started after database creation. If the TNS listener is not running, an error in the Oracle Server or Oracle SID Name will occur.
Start HP DMA	10.20	Described what happens when incorrect credentials are entered.
DMA Client Files Policy Error	10.20	Added troubleshooting information if the /DMA_Client directory does not exist or is not writable.
Other Requirements	10.20	Default SA port is 443.
Install the HP DMA Server	10.20	Clarified that the servers cannot be localhost.
Installation Media Contents	10.20	Updated contents of installation media.
Troubleshooting	10.20	Added information about turning on debug.
Pre-Installation Requirements	10.20	Oracle Database Enterprise or Standard Edition can be used as the backend database tool. HP DMA and SA can use the same Oracle installation and database, but each product needs to be configured in separate schemas.
Troubleshooting	10.20.100	Added troubleshooting information for login errors: Oracle database password changed The HP DMA database is not accessible
Special Configurations Troubleshooting	10.20.100	Reduced instructions for advanced DMA users to create and configure Custom Fields.
Use a Proxy Server with HP DMA	10.20.100	Reorganized section.
Run as a Windows Domain User	10.20.100	Added new capability to configure a Windows domain user using runtime parameters.
Entire guide	10.20.100	Updated HP DMA versions.
Title Page Legal Notices Entire guide	10.21	Updated version number, software release date, document release date, and copyright date range. Updated document template. Updated screen shots.
Troubleshooting	10.21	Added new section Run Time Errors to describe Workflow Aborts Using an Internal SSL Certificate.
How to Upgrade HP DMA Troubleshooting	10.21	Added instructions to copy the JAR files when the SA Core has been updated. Added a new troubleshooting section "The SA Core was Updated" under Login Errors .
Troubleshooting	10.21	Added new "HP DMA is Switched to Different SA Core" section to Login Errors . Added new "Reset the HP DMA Initial Admin Password" section to Password Security .
Performance Issues	10.21	Added new Troubleshooting information for performance issues.

Support

Visit the HP Software Support Online web site at: <http://www.hp.com/go/hpsoftwaresupport>

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

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

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts

- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

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

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

To find more information about access levels, go to:

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

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

Contents

Contents	5
Introduction	9
Audience	10
Document Map	11
Chapter 1: Pre-Installation Requirements	12
Installation Media Contents	13
Supported Products and Platforms	16
Sizing Recommendations	17
Create and Configure the Oracle Database	19
Steps to Create and Configure the Oracle Database	19
Obtain a Signed Server Certificate	21
Other Requirements	22
Chapter 2: How to Install HP DMA	24
Install the HP DMA Server	25
Configure SSL on the HP DMA Server	28
About keytool	28
Generate a Private Key for the Server	29
Generate the Certificate Signing Request to Obtain Signed Server Certificates	30
Import the SSL Server Certificates	31
Configure the HP DMA Server to Use Your Certificate	33
Verify the SSL Connection	36
Install the HP DMA Client for SA	37
Integrate HP DMA with HP Server Automation	38
SA Integration Requirements	39
Overview of the HP DMA and HP Server Automation Integration Process	39
Import the HP DMA APX	40
HP Live Network Connector Overview	40
SAVA Installation of the HP DMA APX	40
Enterprise SA Manual Import of the HP DMA APX	41

Install the DMA Client Files Policy	43
Set Up the SA Groups and Users	44
HP DMA User Groups	44
The HP DMA Connector User	46
Start HP DMA	47
Set Up HP DMA	49
Configure the Connector	50
Register HP DMA Roles	52
Assign HP DMA Capabilities	53
Add Available Targets	54
Import an HP DMA Solution Pack	57
Chapter 3: How to Uninstall HP DMA	60
Uninstall HP DMA from the HP DMA Server	60
Uninstall HP DMA from the Managed Servers	61
Chapter 4: How to Upgrade HP DMA	62
Chapter 5: How to Link HP DMA into HP Server Automation	66
Chapter 6: Special Configurations	68
Change the Default Port	69
Use a Proxy Server with HP DMA	70
Default HP DMA Communications	71
Using an SA Satellite as a Proxy Server	72
How HP DMA Manages Proxy Communication	73
How to Set Up a Proxy Server	74
Configure the SA Core Gateway Properties	74
Specify the Server Automation Realm	75
Create and Configure the HP DMA Custom Fields	77
Specify a Renamed Windows Administrator User	79
Update the HP DMA APX	80
Create and Configure the HP DMA Custom Field	80
Run as a Windows Domain User	82
Configure Windows Domain User Using Custom Fields	82

Configure Windows Domain User Using Runtime Parameters	84
Change the Number of Active Connections	86
Chapter 7: Troubleshooting	87
Debugging Tools	87
Troubleshooting Issues	89
Common Baseline Errors	91
Oracle Database User Was Not Created	91
Oracle Listener Is Not Running	92
Oracle Database Is Not Running	92
Error in the Oracle Server or Oracle SID Name	93
HP DMA Client Fails to Contact HP DMA Server	94
Did Not Run the Baseline Command as Root User	96
APX Tool Configuration Error	98
Not Pointing to Correct APX Tool Directory	98
DMA Client Files Policy Error	99
DMA_Client Directory Does Not Exist or Is Not Writable	99
Microsoft Patch Database Is Out of Date	100
Connector Errors	103
The SA Core Server Is Down	103
The JAR Files Are Not at the Required Locations	104
Login Errors	105
The SA Core Server Is Down	106
The SA Group Does Not have Login Access	106
HP DMA Started Before SA was Running	107
Oracle Database Password Changed	108
The HP DMA Database is Not Accessible	109
The SA Core was Updated	110
HP DMA is Switched to Different SA Core	111
No Servers Available to Add to HP DMA	113
The HP DMA Connector User Does Not Have Required Permissions	114
The HP DMA Connector User Cannot Find Any Servers	114

The Servers Are Already in Another HP DMA Organization	115
The HP DMA User Does Not Have Correct Permissions	115
The DMA Client Files Policy Is Not Attached and Remediated	116
Run Time Errors	117
Workflow Aborts Using an Internal SSL Certificate	117
Performance Issues	119
Intermittently Unable to Log In and System Freezes	119
Password Security	120
Reset the HP DMA Initial Admin password	120
Chapter 8: Reference Information	122
HP Software Documentation	123
HP DMA Baseline Options	125
About the SA Client	127
Workflow Execution Script	129

Introduction

This document shows you how to perform various installation tasks for HP Database and Middleware Automation (HP DMA) version 10.21:

- How to do a complete installation of HP DMA 10.21 from scratch: Install the HP DMA server, install the HP DMA Client for SA, integrate with HP Server Automation, and set up the initial HP DMA operating environment
- How to uninstall HP DMA
- How to upgrade from HP DMA version 10.20.100 (or 10.20, 10.10, 10.01) to version 10.21
- How to link HP DMA version 10.21 into HP Server Automation
- How to troubleshoot problems that can arise during installation and initial configuration of HP DMA

This guide also provides information about various [Special Configurations](#) that may be pertinent to your environment.

Audience

This guide is intended for system administrators who want to install or upgrade HP Database and Middleware Automation (HP DMA) version 10.21.

Document Map

The following table shows you how to navigate this guide:

Topic	Description
Pre-Installation Requirements	Information about the requirements to install HP DMA, including what is on the installation media, supported products and platforms, sizing requirements, how to set up the Oracle database, how to obtain a signed server certificate, and other requirements.
How to Install HP DMA	Detailed instructions for how to install HP DMA 10.21, including: <ul style="list-style-type: none">• How to install the HP DMA server• How to configure SSL on the HP DMA server• How to install the HP DMA Client for SA• How to integrate with HP Server Automation• How to start HP Database and Middleware Automation• How to do the initial set up of HP Database and Middleware Automation
How to Uninstall HP DMA	Instructions for how to uninstall HP DMA.
How to Upgrade HP DMA	Instructions for how to upgrade from HP DMA version 10.20.100 (or 10.20, 10.10, 10.01) to 10.21.
How to Link HP DMA into HP Server Automation	Instructions for how to disable outdated versions of HP DMA that came with HP Server Automation (SA) and redirect SA to call HP DMA 10.21 instead.
Special Configurations	How to configure HP DMA for certain non-default scenarios.
Troubleshooting	Tips for solving common problems.
Reference Information	Links to more information about HP DMA, HP Server Automation, reference information for the HP DMA baseline command, and information about the SA Client.

Chapter 1: Pre-Installation Requirements

You must meet the following requirements before you can install the HP DMA 10.21:

Topic	Description
Installation Media Contents	A description of the contents of the HP DMA 10.21 installation media that is required for the installation.
Supported Products and Platforms	A list of the required products, platforms, hardware, and software.
Sizing Recommendations	Information about the minimum recommended CPU count, RAM, and disk space for the HP DMA server and the HP DMA database server.
Create and Configure the Oracle Database	A description of how the Oracle Database needs to be configured before it can be used by HP DMA 10.21.
Obtain a Signed Server Certificate	Information about obtaining a server certificate signed by a trusted Certificate Authority.
Other Requirements	A list of all other pre-installation requirements for HP DMA 10.21.

Installation Media Contents

This topic describes the contents of the purchased HP DMA 10.21 installation media—DVD or ISO file. When you mount the media you will see the following folders and files:

Top level folder

readme.txt	Last minute corrections to instructions and information about files on the media
DMA_10.21_Open_Source_Licenses.zip	This file contains the license agreements for the Open Source software used by HP DMA.

DMA_10.21_Server_and_Client folder

dma-server-10.21-0.x86_64.rpm	The rpm file that will install the HP DMA 10.21 server.
dma-sa-client-10.21-0.x86_64.rpm	The rpm file that will install the HP DMA 10.21 client that enables HP DMA to integrate with HP Server Automation (SA).
Discovery.zip	Solution pack containing workflows that you can use to discover: <ul style="list-style-type: none">• Oracle, SQL Server, Sybase, and DB2 databases on target servers.• IBM WebSphere and Oracle Weblogic middleware applications on target servers.
Promote.zip	Solution pack containing workflows that you can use to promote HP DMA workflows (and related automation items) from a source HP DMA server to a destination HP DMA server.

DMA_10.21_Documentation

buildinfo.txt	Information about how the installation media was constructed
DMA_10.21_Installation_Guide.pdf	<i>HP DMA Installation Guide</i> —this document
DMA_10.21_Administrator_Guide.pdf	<i>HP DMA Administrator Guide</i>
DMA_10.21_User_Guide.pdf	<i>HP DMA User Guide</i>
DMA_10.21_Release_Notes.pdf	<i>HP DMA Release Notes</i>
DMA_10.21_Open_Source_Third_Party_Licenses.pdf	<i>HP DMA Open Source and Third-Party Software License Agreements</i>

DMA_10.21_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_10.21_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.
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 backing up, deploying, and restoring IBM WebSphere application servers and deploying and configuring Oracle WebLogic application servers.


Tip: Always check to see if there are more recent versions of the HP DMA documentation or solution packs available online. Due to frequent releases, it is possible that the files provided on the HP DMA 10.21 installation media have since been updated.

HP DMA solution pack documentation is only available online.

To get the most recent version of HP DMA documentation or solution packs:

1. Go to the following web site: [HP Software Support Online](#)
2. Go to the Self-Solve tab, and sign in using your HP Passport credentials (see [Support](#) on page 3 for more information).
3. On the Advanced Search page, specify the following search criteria:

Product:	Database and Middleware Automation
Version:	All Versions
Operating System:	All Operating Systems
Document Type:	Manuals and Patches

4. Click **Search**.
5. If there is a more recent version of documentation or you want a solution pack user guide (not included on the installation media), do the following:
 - a. Click the link for the manual that you want to view.
 - b. Click the  button or the manual name to open the manual in your browser.
6. If there is a more recent version of a solution pack, do the following:
 - a. Click the link for the solution pack.
 - b. Click the **DOWNLOAD PATCH** link, and download the ZIP file that contains the patch.
 - c. From the patch ZIP file, extract the ZIP file that contains the solution pack.

Note: This ZIP file may be included in a larger ZIP file that contains multiple solution packs.

Supported Products and Platforms

Operating System Requirements

HP DMA 10.21 can be installed on the following platforms:

- Red Hat Enterprise Linux versions 5.8 and 6.1 (or later) 64-bit
- SUSE Enterprise Linux version 11 (or later) 64-bit

Note: Although HP DMA will work on other Linux operating systems, HP will only support these certified versions.

Hardware Requirements

See the [Sizing Recommendations](#) on the next page.

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

Software Requirements

- HP Server Automation Virtual Appliance 10 (SAVA)—Standard Edition 10.0—or HP Server Automation Enterprise Edition version 10.0, 9.1x, or 9.06

Note: You must purchase this license separately.

- Oracle Database Enterprise or Standard Edition version 11g R2

Note: HP does not provide the Oracle Database license to run HP DMA.

Sizing Recommendations

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

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

HP DMA Deployment Modes

HP DMA supports the following deployment options:

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

Deployment sizing categories

Category	Number of HP 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 for HP DMA Components

Sizing recommendations for deploying the HP 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 what will be installed. These recommendations are based on dual core installation.

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

Sizing recommendations for deploying the HP 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 HP DMA database on a virtual machine you must ensure that the actual available CPUs and RAM for the HP DMA database virtual machine meets the same requirements.

Create and Configure the Oracle Database

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

You need a username and password for this Oracle database.

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

- Have your Oracle database administrator (DBA) create the Oracle Instance and the two tablespaces.
- Perform the [Steps to Create and Configure the Oracle Database](#) below.

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

Steps to Create and Configure the Oracle Database

This topic shows you how to create and configure an Oracle database that will be used by HP DMA 10.21.

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 do the following:

1. Have your DBA create an Oracle Database Enterprise or Standard Edition version 11g R2 database to be used by HP DMA. Make sure the Oracle Listener and database are up and running.
2. Connect to the Oracle database and create the hpdma_data and hpdma_indx tablespaces.

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 hpdma_data datafile '<DMA_data_file>' size  
<file_size>M autoextend on;
```

```
create tablespace hpdma_indx datafile '<DMA_indx_file>' size  
<file_size>M autoextend on;
```

```
exit;
```

3. 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](#).

4. Start the TNS listener after creating the database.

Obtain 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 HP 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 [Configure SSL on the HP DMA Server](#) on page 28 for more information.)

Other Requirements

HP Server Automation (SA)

HP Server Automation needs to be up and running.

The person who integrates HP 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

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

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

Ports

The following ports need to be available:

- HP DMA: 8443 is the default port, but HP DMA can be configured to use a different port if necessary.
- Oracle Database: The Oracle port needs to match how the database is configured—1521 is the default.
- SA: The SA port is 443.

Firewalls

The firewalls need to have the following ports open:

- Incoming on the port configured for HP DMA
- Outgoing on the ports configured for Oracle Database and SA

The firewalls need to allow SA managed servers running HP DMA workflows to access the HP DMA server on port 8443—or a proxy server can be used.

Tip: See [Use a Proxy Server with HP DMA](#) on page 70 for more information about how to set up a proxy server with HP DMA.

Privileges

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

Chapter 2: How to Install HP DMA

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

Topic	Description
Install the HP DMA Server	Step-by-step instructions about how to install the HP DMA 10.21 server.
Configure SSL on the HP DMA Server	Step-by-step instructions about how to configure SSL on the HP DMA 10.21 server.
Install the HP DMA Client for SA	Step-by-step instructions about how to install the HP DMA 10.21 client.
Integrate HP DMA with HP Server Automation	Step-by-step instructions about how to integrate HP DMA 10.21 with HP Server Automation. These steps should be performed by the SA administrator.
Start HP DMA	Directions to start HP DMA 10.21.
Set Up HP DMA	General information about how to use HP DMA 10.21 to set up the connector, roles, capabilities, and targets, and to import a solution pack.

Install the HP DMA Server

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

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—must be the same username that you used when you created your Oracle database in Steps to Create and Configure the Oracle Database
<database_password>	myOraclePassword	Oracle Database password—must be the same password that you used when you created your Oracle database in Steps to Create and Configure the Oracle Database
<DMA_server>	dma.mycompany.com	Fully qualified host name of the HP 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 Steps to Create and Configure the Oracle Database
<Oracle_Server>	oracle.mycompany.com	Fully qualified host name of the Oracle Database server—must be the same server that you used when you created your Oracle database in Steps to Create and Configure the Oracle Database Note: This cannot be localhost.
<jdbc_string>	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> Note: Other connection string syntax is possible. Consult your Oracle DBA for the company standard.
<SA_Server>	saserver.mycompany.com	Fully qualified host name of the HP Server Automation server

On your Red Hat Enterprise Linux HP DMA server (<DMA_server>) do the following:

1. Get the `dma-server-10.21-0.x86_64.rpm` file from the HP DMA 10.21 installation media under the `DMA_10.21_Server_and_Client` folder.
2. Run the following commands as root to install the HP DMA server:

```
$ cd DMA_10.21_Server_and_Client  
  
$ rpm -ivh dma-server-10.21-0.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 [HP DMA Baseline Options](#) on page 125.

This command does not baseline the connector. You will configure the connector later (see [Configure the Connector](#) on page 50).

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

Note: If you receive an error, see [Troubleshooting](#) on page 87.

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

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

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

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

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

Configure SSL on the HP DMA Server

To configure SSL on the HP 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 30
3. [Import the SSL Server Certificates](#) on page 31
4. [Configure the HP DMA Server to Use Your Certificate](#) on page 33
5. [Verify the SSL Connection](#) on page 36

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

Caution: If you are using an SA gateway infrastructure as a proxy network (see [Use a Proxy Server with HP DMA](#)), you must have a subject alternate name (SAN) as part of your signed certificate:

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

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 keytool

Many procedures in this section use the `keytool` utility, which is located in the following directory on the HP 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 HP 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 HP DMA server as the root user.
2. Execute the following command (all on one line):

```
/opt/hp/dma/server/jre/bin/keytool -genkey -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>
```

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.
<DMAserver>	Fully qualified host name of the server hosting the HP DMA server.
<orgunit>	The organizational unit (business unit) that owns this server.
<org>	The organization (company) that owns this server.
<location>	The city in which this server physically resides.
<state>	The state or province in which this server physically resides.
<country>	The country in which this server physically resides.
<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 -genkey -alias myserver -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 HP 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 HP 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 myserver  
-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.

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

Import 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, do the following:

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
<code><keyalias></code>	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
<code><CAcert></code>	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
<code><storefile></code>	Fully qualified keystore file name.	/opt/hp/dma/server/.mykeystore
<code><password></code>	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 myserver
-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>
```

Configure the HP 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 HP DMA Web Server
- Change the `trustAllCertificates` value in the `dma.xml` file to `false`

To configure the HP DMA server to use your certificate:

1. As root, stop the HP 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 Generate a Private Key for the Server on page 29).
<SSLport>	Port that will be used for: <ul style="list-style-type: none">■ SSL communication between the HP DMA Server and the HP DMA clients■ Accessing the HP 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 HP DMA Server by using the following command:

```
service dma start
```

Verify the SSL Connection

To verify your SSL connection, do the following:

1. Log in to your HP DMA server.
2. HTTPS protocol indicates that the HP DMA Server is communicating with the HP DMA Client using SSL.
3. The lock icon () in the address bar indicates that the HP DMA Server is communicating with the HP 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 HP 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 [Configure the HP DMA Server to Use Your Certificate](#) on page 33, 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 HP DMA server.

In the next stage you will install the HP DMA client for SA.

Install the HP DMA Client for SA

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

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

On the HP DMA server, get the `dma-sa-client-10.21-0.x86_64.rpm` file from the HP DMA 10.21 installation media under the `DMA_10.21_Server_and_Client` folder, and then run the following commands as root:

```
$ cd DMA_10.21_Server_and_Client
$ rpm -ivh dma-sa-client-10.21-0.x86_64.rpm
```

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

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

Integrate HP DMA with HP Server Automation

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

HP DMA uses HP Server Automation (SA) as an agent infrastructure. HP DMA integrates with SA to authenticate users, associate users with groups, and determine user privileges. HP DMA uses SA to acquire knowledge of servers and to send requests to execute workflows on servers. Before HP DMA can actually work, you have to perform a series of integration steps on your SA system as well as on your new HP 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 HP 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 HP 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 HP DMA with SA.
Overview of the HP DMA and HP Server Automation Integration Process	Overview of the steps to integrate with SA—to be performed by the SA administrator.
Import the HP DMA APX	Detailed instructions for the SA administrator to configure the SA Automation Platform Extension (APX) to be used by HP DMA.
Install the DMA Client Files Policy	Detailed instructions for the SA administrator to install and remediate the DMA Client Files policy.
Set Up the 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 HP DMA 10.21 with HP Server Automation (SA):

- Make sure that you have met all the general HP DMA installation requirements in [Pre-Installation Requirements](#) on page 12.
- You have already installed and configured the HP DMA server software. If you have not done so, see [Install the HP DMA Server](#) on page 25.
- You have already installed and configured the HP DMA Client for SA. If you have not done so, see [Install the HP DMA Client for SA](#) on page 37.
- The HP DMA server software and the HP DMA Client for SA software must be installed on the same system. This system will be referred to as the HP DMA server in the following instructions.

Overview of the HP DMA and HP Server Automation Integration Process

The SA administrator needs to perform the following general steps:

1. Install the HP 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 HP DMA targets.
4. Set up the SA groups that will have HP DMA access privileges.
5. Set up the SA user that HP 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 HP Server Automation server
<DMA_ server>	dma.mycompany.com	Fully qualified host name of the HP DMA server

Import the HP DMA APX

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

The HP DMA APX can be imported into HP Server Automation Virtual Appliance 10 (SAVA) or HP 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.

HP 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` HP LN Stream. SAVA uses the "Command-line Web Utilities Launcher" to configure LNc. Enterprise SA uses an installation of HP Live Network connector (LNc) as described in the LNc documentation (see [HP Software Documentation](#)).

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 HP 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 HP 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 HP Passport user name and password. (See [Support](#) on page 3 for more information about obtaining an HP Passport account.)

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 HP DMA APX

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

The SA user (`<SA_APX_User>`) who imports the HP 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 HP DMA APX.

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

On the HP DMA server, copy the HP 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 HP 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.

Install 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 HP 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 HP DMA packages and policy.

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

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

1. In the SA Client (see [About the SA Client](#) for more information), create a /DMA_Client folder.
2. As root on the HP 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 HP DMA target, attach and remediate the DMA Client Files policy.

Set Up the SA Groups and Users

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

HP DMA User Groups

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

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

To set up your HP DMA user groups:

1. On the SA server to which HP 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 HP DMA

In order to add servers to HP 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. (See [About the SA Client](#) for more information.)

3. Add at least one user to each group.

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

The HP DMA Connector User

An additional SA user, `<dma_connector_user>`, is required to configure the HP 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 HP 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 HP DMA connector user:

1. On the SA server to which HP 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 HP 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 HP DMA.

Start HP DMA

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

1. As root, start the HP DMA 10.21 server. For example:

```
$ service dma start
```

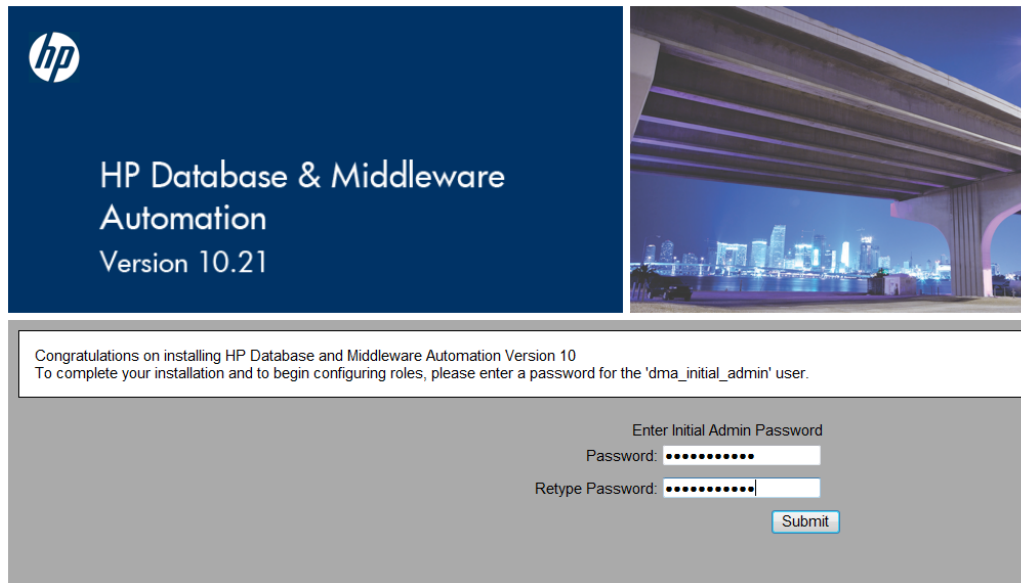
2. Use a web browser to connect to the HP DMA server:

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

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

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.

Note: Next you will perform the initial HP DMA setup using the HP DMA user interface.

Set Up HP DMA

This section shows you how to initially set up HP DMA.

Two different HP DMA administrators must configure the HP DMA operating environment.

1. The initial default administrator, `dma_initial_admin`, must perform the following steps:

Topic	Description
Configure the Connector	Step-by-step instructions about how to configure the HP DMA connector.
Register HP DMA Roles	Step-by-step instructions about how to register the HP DMA roles.
Assign HP DMA Capabilities	Step-by-step instructions about how to assign HP DMA capabilities.

2. Next, an HP DMA user whose role has Administrator capability—for example, the DMA Admins role—must perform the following steps:

Topic	Description
Add Available Targets	Step-by-step instructions about how to add targets to HP DMA.
Import an HP DMA Solution Pack	Step-by-step instructions about how to import an HP DMA solution pack.

Configure the Connector

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

Note: You only do this once.

While you are logged in as `dma_initial_admin`, do the following:

1. On the **Setup > Connector** page, click the **Add Connector** button in the lower right corner.
2. Specify a name for your connector, and then click **Enter**.
3. Specify the Server Automation Host, Server Automation Username, and Server Automation Password for your connector:

The Server Automation Username is the SA user that you created in [Set Up the SA Groups and Users](#)—for example, `dma_connector_user`.

hp Database & Middleware Automation

Home Automation Reports Environment Solutions **Setup**

Configuration Permissions Capabilities Roles **Connector**

Connector

MySAconnector

Server Automation Host: saserver.mycompany.com

Server Automation Username: dma_connector_user

Server Automation Password: ●●●●●●

Save or CANCEL

4. Click **Save**.

You will receive the following message:

✓ Successfully configured connector. Please restart DMA Server by entering 'service dma restart' at command-line.

Note: If you receive an error, see [Troubleshooting](#) on page 87.

5. As root, restart the HP DMA 10.21 server. For example:

```
$ service dma restart
```

6. Use a web browser to connect to the HP DMA server:

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

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

7. To log in, enter `dma_initial_admin` for the username, enter your password, and then click **Login**.

Register HP DMA Roles


This topic shows you how to register HP DMA roles.

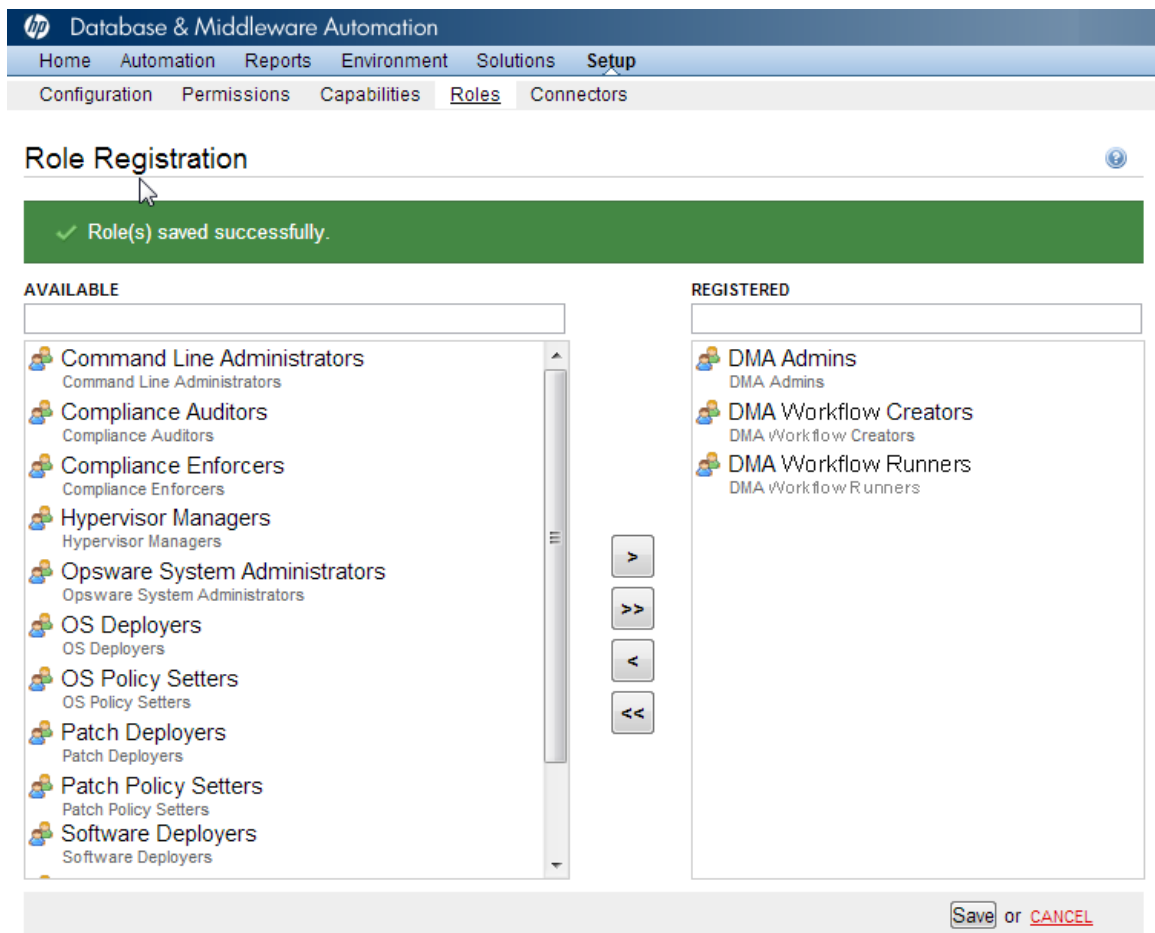
HP DMA obtains the complete set of available roles from HP Server Automation—including the groups that your SA administrator configured in [Set Up the SA Groups and Users](#).

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 an AVAILABLE user-group on the left and then click the  button. The selected role moves to the REGISTERED list on the right.



hp Database & Middleware Automation

Home Automation Reports Environment Solutions **Setup**

Configuration Permissions Capabilities **Roles** Connectors

Role Registration

✓ Role(s) saved successfully.

AVAILABLE

- Command Line Administrators
Command Line Administrators
- Compliance Auditors
Compliance Auditors
- Compliance Enforcers
Compliance Enforcers
- Hypervisor Managers
Hypervisor Managers
- Opware System Administrators
Opware System Administrators
- OS Deployers
OS Deployers
- OS Policy Setters
OS Policy Setters
- Patch Deployers
Patch Deployers
- Patch Policy Setters
Patch Policy Setters
- Software Deployers
Software Deployers

REGISTERED

- DMA Admins
DMA Admins
- DMA Workflow Creators
DMA Workflow Creators
- DMA Workflow Runners
DMA Workflow Runners

Save or CANCEL

3. Click the **Save** button to save your changes.

Assign HP DMA Capabilities

This topic shows you how to assign HP 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.

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 users whose roles have Administrator capability can import solution packs.

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

Note: This will log you out as the default initial administrator, `dma_initial_admin`.

Add Available Targets

This topic shows you how to make target servers available to HP DMA users.

Log in to HP DMA as a user with Administrator capability—for example, a user with the DMA Admins role.

Note: If you receive an error, see [Troubleshooting](#) on page 87.

To add servers:

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 *HP DMA Administrator Guide*.

The screenshot displays the HP Database & Middleware Automation interface. The top navigation bar includes 'Home', 'Automation', 'Reports', 'Environment', 'Solutions', and 'Setup'. Below this, a secondary navigation bar shows 'Dashboard', 'Smart Groups', and 'Custom Fields'. The main content area is titled 'Environment' and features a table with one row labeled 'Default'. To the right of the table is a 'NEW ORGANIZATION' link. Below the table, there is a 'Default' configuration section with tabs for 'Properties', 'Custom Fields', and 'Roles'. The 'General' tab is selected, showing a 'Name' field containing 'Default'. At the bottom of the page, there is a row of buttons: a red 'DELETE' button, an 'Add servers' button, a 'Save' button, and a 'CANCEL' button.

3. Click **Add servers** in the lower right corner. A new page will appear.

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



Note: If no servers are available to add to the organization, see [Troubleshooting](#) on page 87.

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

To grant user roles permission to access the servers:

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 HP Database & Middleware Automation interface. The top navigation bar includes 'Home', 'Automation', 'Reports', 'Environment', 'Solutions', and 'Setup'. Below this, there are tabs for 'Configuration', 'Permissions', 'Capabilities', 'Roles', and 'Connector'. The main heading is 'DMA Admins', with sub-tabs for 'Deployments', 'Workflows', 'Steps', 'Policies', and 'Organizations'. A search bar is present above a table. The table has columns for 'Organization', 'Read', 'Write', and 'Deploy'. The 'Default' organization row has checkmarks in the 'Read', 'Write', and 'Deploy' columns. 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"/>

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

Import an HP DMA Solution Pack

This topic shows you how to import solution packs. These instructions apply to any solution pack.

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

To access the solution pack:

The HP DMA 10.21 installation media provides solution packs in the following folders:

- `DMA_10.21_Server_and_Client` contains the Discovery solution pack (`Discovery.zip`).
- `DMA_10.21_Database_Solution_Packs` contains all of the database solution packs (provisioning, advanced provisioning, patching, advanced patching, compliance, refresh, and release management).
- `DMA_10.21_Middleware_Solution_Packs` contains all of the application server solution packs (provisioning, patching, configuration management, and release management).

Caution: Always check to see if there are more recent versions of the HP DMA solution packs available online. Due to frequent releases, it is possible that the solution packs provided on the HP DMA 10.21 installation media have since been updated.

To get the most recent version of a solution pack:

1. Go to the following web site: [HP Software Support Online](#)
2. Go to the Self-Solve tab, and sign in using your HP Passport credentials (see [Support](#) on page 3 for more information).
3. On the Advanced Search page, specify the following search criteria:

Product:	Database and Middleware Automation
Version:	All Versions
Operating System:	All Operating Systems
Document Type:	Patches

4. Click **Search**.
5. If there is a more recent version of the solution pack that you want to import, do the following:
 - a. Click the link for the solution pack that you want to import (for example: `discovery 10.21`).
 - b. Click the **DOWNLOAD PATCH** link, and download the ZIP file that contains the patch.

- c. From the patch ZIP file, extract the ZIP file that contains the solution pack.

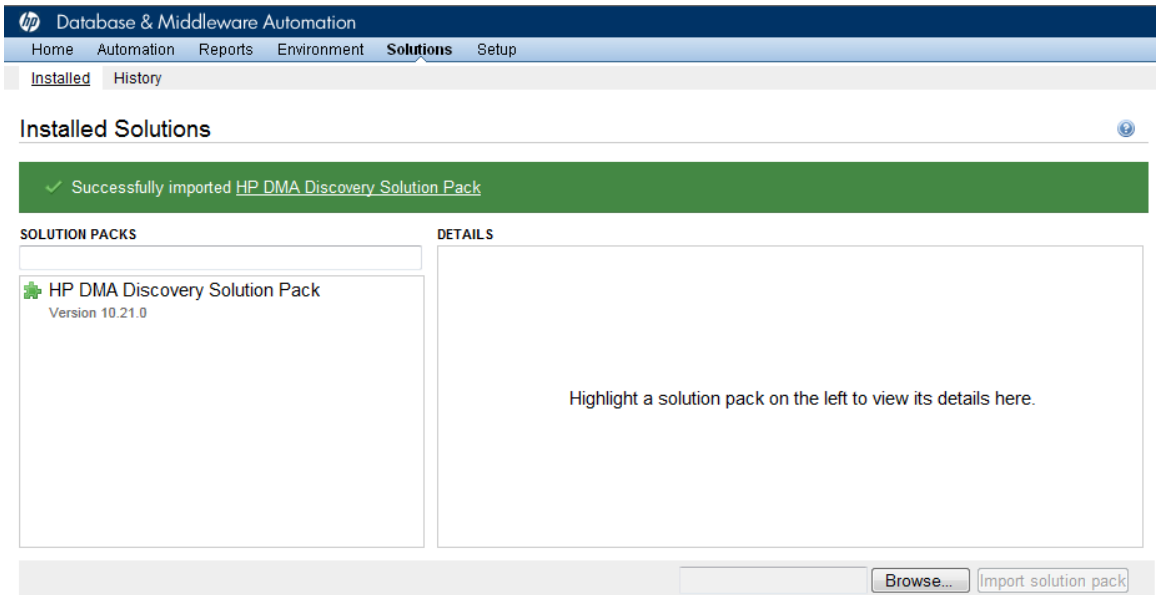
Note: This ZIP file may be included in a larger ZIP file that contains multiple solution packs.

To import the solution pack:

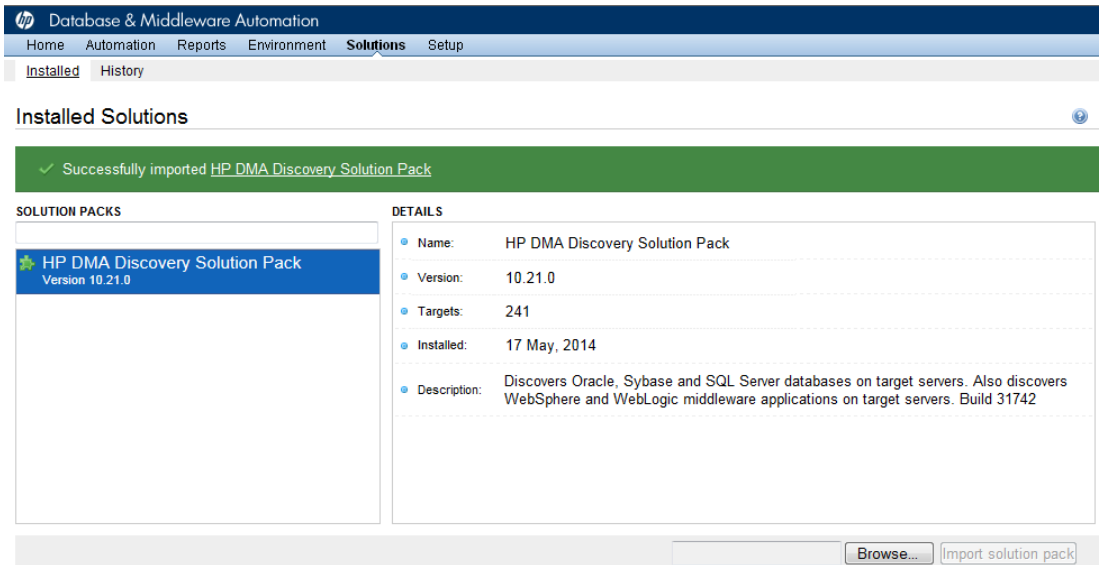
1. Log in to HP DMA as an HP DMA administrator (a user who has at least one role with Administrator capability).
2. On the Solutions > Installed tab, click the **Browse** button in the lower right corner. The Choose File dialog opens.

Note: This button and the dialog that subsequently opens may have different names depending on the browser that you are using.

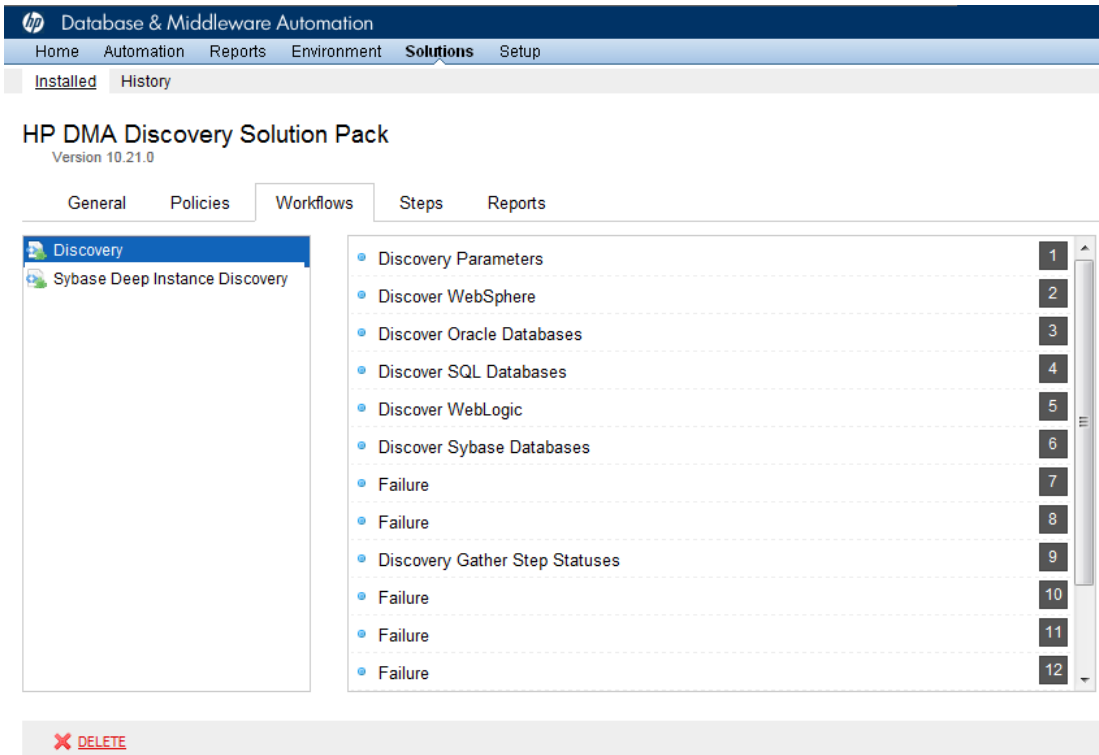
3. Locate and select the desired solution pack ZIP file—either from the HP DMA 10.21 installation media or from [HP Software Support Online](#)—then click **Open**.
4. Click **Import solution pack**.



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.



Note: This completes the initial set up process.

Your HP DMA is now ready to use. Refer to the *HP DMA Administrator Guide* and the *HP DMA User Guide* for additional information on using HP DMA.

Chapter 3: How to Uninstall HP DMA

This chapter shows you how to uninstall HP DMA 10.21 from the HP DMA Server and the HP DMA managed servers.

Uninstall HP DMA from the HP DMA Server

To uninstall HP DMA from the HP DMA Server, do the following:

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

```
$ service dma stop
```

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

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

You can locate the current version of HP 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 HP DMA is 10.21, your results will look like this:

```
dma-server-10.21-0.x86_64.rpm  
dma-sa-client-10.21-0.x86_64.rpm
```

3. Run the following commands as root to uninstall HP 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 HP DMA version from your query.

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

```
/opt/hp/dma/server
```

```
/var/opt/hp/dma/work/dma
```

```
/var/log/hp/dma
```

Uninstall HP DMA from the Managed Servers

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

1. In SA, detach the managed server from the DMA Client Files policy and then remediate the target.
2. To completely remove HP 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`

Chapter 4: How to Upgrade HP DMA

This chapter shows you how to upgrade from HP DMA version 10.20.100 (or 10.20, 10.10, 10.01) to 10.21.

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

Tip: To take advantage of the features and enhancements of the new HP DMA 10.21 workflows, after you have upgraded the HP DMA server you must import the HP DMA 10.21 solution pack, make a copy of the pertinent HP DMA 10.21 workflow, and then merge your customizations into it.

To upgrade to HP DMA 10.21:

The following steps must be performed 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 HP DMA 10.20.100.

2. Stop HP DMA:

```
$ service dma stop
```

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

3. Go to the HP DMA 10.21 installation media under the `DMA_10.21_Server_and_Client` folder.
4. On each HP DMA server to be upgraded do the following to upgrade the HP DMA server:

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

```
$ rpm --upgrade dma-server-10.21-0.x86_64.rpm
```

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

5. On one HP 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 HP 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 [HP DMA Baseline Options](#) on page 125.

Caution: When you run the baseline command exactly as given you will maintain your HP DMA database. If you use the `--erase` option you will lose your customized HP 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](#) on page 87.

6. Go to the HP DMA 10.21 installation media under the `DMA_10.21_Server_and_Client` folder.
7. On one HP DMA server per SA server, do the following to upgrade the HP 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-10.21-0.x86_64.rpm
```

8. Have your SA administrator reinstall the HP DMA APX on the SA core.

To do this, follow the instructions in [Import the HP DMA APX](#) on page 40. Note: The `/DMA_APX` folder will not be created since it already exists.

9. If you are also updating the SA core, rerun the script command to copy the required JAR files from the SA server to the HP DMA server. On your HP 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>
```

10. Have your SA administrator reinstall the DMA Client Files policy on the SA core.

To do this, follow the instructions in [Install the DMA Client Files Policy](#) on page 43:

- a. Use the same folder (/DMA_Client) as in step 1.
 - b. Do steps 2 and 3.
11. 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.

12. Restart all HP DMA servers using the following command:

```
$ service dma start
```


To revert an upgrade from the HP DMA Server:

Caution: You can only revert an upgrade if you created a backup of your database **BEFORE** you upgraded to version 10.21.

If you wish to revert the HP DMA 10.21 upgrade back to version 10.20.100 do the following:

1. Stop the HP DMA server, as root:

```
$ service dma stop
```

2. Restore the database from the backup.
3. Run the following command to revert back to HP DMA 10.20.100.

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

```
$ rpm --upgrade --oldpackage dma-server-10.20.100-0.x86_64.rpm
```

4. Upload and reinstall the HP DMA10.20.100 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 HP DMA 10.20.100.
7. Attach the DMA Client Files policy to all desired managed servers and then remediate again.
8. Restart the HP DMA server:

```
$ service dma start
```

Chapter 5: How to Link HP DMA into HP Server Automation

This chapter shows you how to disable outdated versions of HP DMA that came with HP Server Automation (SA) and redirect SA to call HP DMA 10.21 instead.

Note: When SA 9.1x was installed, HP DMA 9.1x was automatically installed with it. HP DMA 10.21 supersedes HP DMA 9.1x. To avoid confusion you may want to deactivate HP DMA 9.1x in your SA installation and link SA to the most recent version of HP DMA.

If you are using HP DMA 9.1x, it is possible to run HP DMA 9.1x and HP DMA 10.21 in parallel. Make sure to update your HP DMA 10.21 before deactivating HP DMA 9.1x.

You must perform these steps on the SA server.

To disable HP DMA 9.1x:

1. Disable HP DMA 9.1x by renaming the `dma.xml` file and the `META-INF` directory. For example:

```
$ mv /opt/opsware/da/conf/Catalina/localhost/dma.xml  
/opt/opsware/da/conf/Catalina/localhost/dma.xml.disabled
```

```
$ mv /opt/opsware/da/webapps/dma/META-INF /opt/opsware/da/webapps/dma/META-  
INF.disabled
```

2. Restart the Application Deployment Manager (ADM)—without restarting HP DMA:

```
$ /etc/init.d/opsware-sas restart da
```

To link SA to the most recent HP DMA—version 10.21:

1. Edit this file :

```
/etc/opt/opsware/httpsProxy/httpd.conf
```

2. Locate the following two lines in the `<VirtualHost *:4433>` grouping:

```
RewriteRule ^/dma/(.*)$ http://localhost:7080/dma/$1 [P,L]
```

```
ProxyPassReverse /dma/ http://localhost:7080/dma/
```

3. Change the two lines using the following example:

```
RewriteRule ^/dma/(.*)$ https://<DMA_Server>:8443/dma/$1 [P,L]
```

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

In these lines `<DMA_Server>` is the fully qualified host name of the HP DMA server, for example `dma.mycompany.com`.

4. Save the file.
5. Restart the `httpsProxy` as root:

```
% /etc/init.d/opsware-sas restart httpsProxy
```

6. You can now access your HP DMA server using the following URL:

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

Tip: To reactivate HP DMA 9.1x, reverse the steps above. Rename `dma.xml.disabled` back to `dma.xml`, rename `META-INF.disabled` back to `META-INF`, and change the two lines in `httpd.conf` back to their original state.

Chapter 6: Special Configurations

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

[Change the Default Port](#) on the next page

[Use a Proxy Server with HP DMA](#) on page 70

[Specify a Renamed Windows Administrator User](#) on page 79

[Run as a Windows Domain User](#) on page 82

[Change the Number of Active Connections](#) on page 86

Change the Default Port

HP DMA uses port 8443 by default. You can change this to another port if you prefer.

To change the HP DMA port:

1. Stop HP DMA:

```
# service dma stop
```

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

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

3. On line 84, change the port from 8443, to the port that you prefer:

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

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

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

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

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

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

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

8. Start HP DMA:

```
# service dma start
```

Use a Proxy Server with HP DMA

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

Caution: If the `trustAllCertificates` value in the `dma.xml` file is set to `false` (see [Configure SSL on the HP DMA Server](#)), you must have a subject alternate name (SAN) as part of your signed certificate:

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

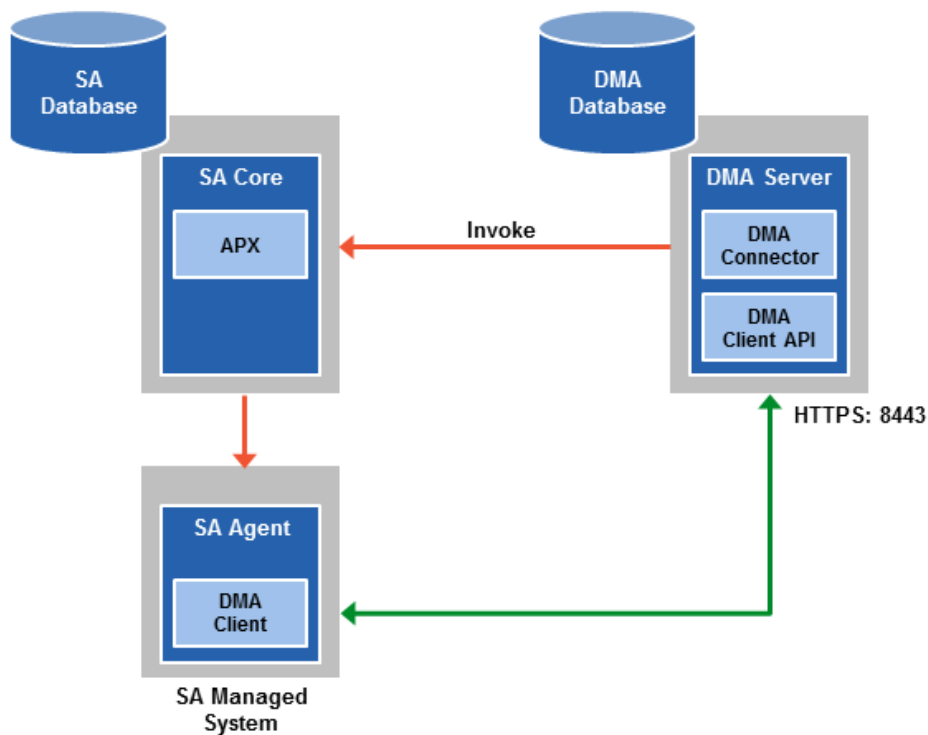
Note: The diagrams in this topic show simplified configurations of servers and communication paths. Real-world situations are much more complex with multiple SA Cores mapped to multiple SA Managed Servers. Multiple SA Satellites may also be configured.

For more information, see the technical white paper: *Configure HP DMA and SA to Use the SA Gateway Network as a Proxy Network*. This document is available on the HP Software Product Manuals web site: <http://h20230.www2.hp.com/selfsolve/manuals>

Default HP DMA Communications

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

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

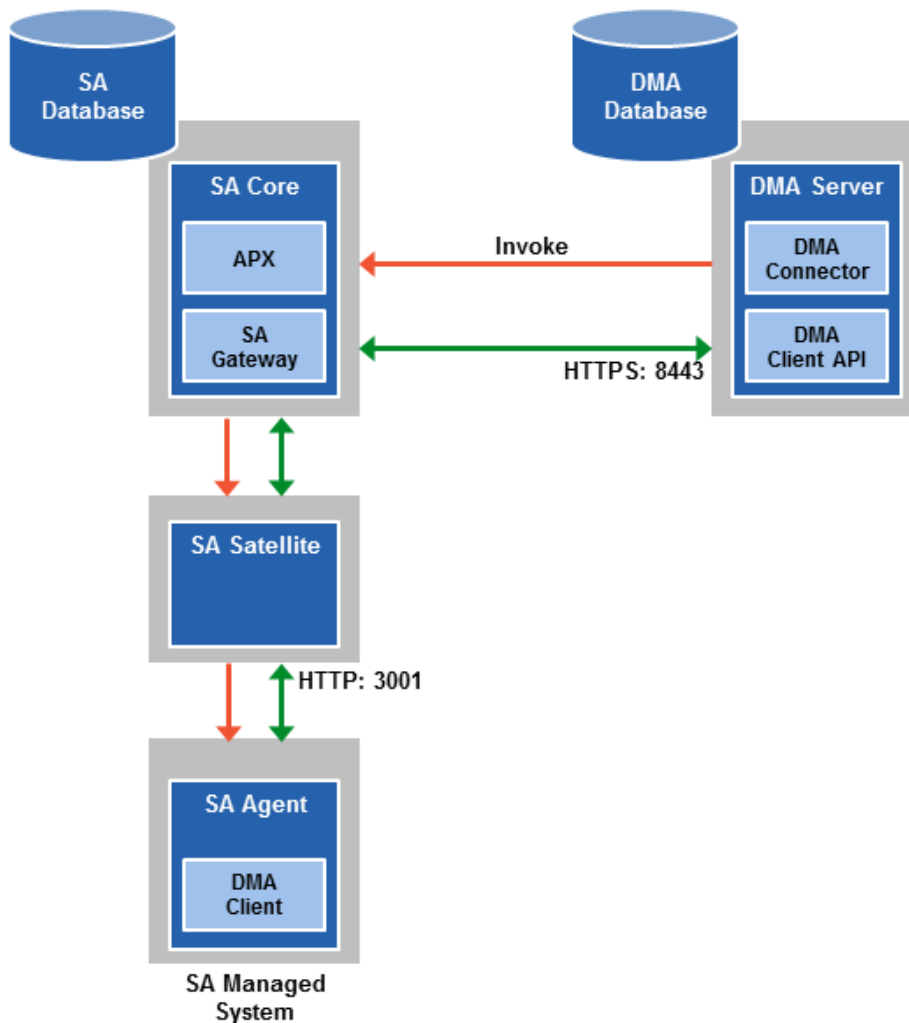


Using an SA Satellite as a Proxy Server

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

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

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



How HP DMA Manages Proxy Communication

HP DMA uses two Custom Fields to control proxy communication:

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

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

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

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

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

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

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

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

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

How to Set Up a Proxy Server

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

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

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

<http://h20230.www2.hp.com/selfsolve/manuals>

Configure the SA Core Gateway Properties

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

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

To add the new EgressFilter rule:

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

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

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

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

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

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

- c. Save the file.

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

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

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

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

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

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

Specify the Server Automation Realm

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

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

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

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

To specify the SA realm:

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

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

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

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

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

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

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

5. Save the `dma.xml` file.
6. Start the DMA service:

```
$ service dma start
```

Create and Configure the HP DMA Custom Fields

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- Set west_proxy_in_use to TRUE, FALSE, or blank.

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

My Organization

Properties Custom Fields Roles

Custom fields [NEW CUSTOM FIELD](#)

west_proxy_address:

west_proxy_in_use:

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

My Organization

Properties Custom Fields Roles

Custom fields [NEW CUSTOM FIELD](#)

west_proxy_address:

west_proxy_in_use:

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

Specify a Renamed Windows Administrator User

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

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

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

Instructions for making each of these changes are provided here.

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

Step Output	Step Errors	Step Header	Connector Output	Connector Errors *				
<table border="1"><thead><tr><th>Status</th><th>Output</th></tr></thead><tbody><tr><td>Server: target1.mycompany.com Created Time: 16:50:45 Client Exit Code: 1</td><td>Error from remote (3054): Handler pre-check failed Agent/Client system target1.mycompany.com is not responding The West APX execute was not successful</td></tr></tbody></table>					Status	Output	Server: target1.mycompany.com Created Time: 16:50:45 Client Exit Code: 1	Error from remote (3054): Handler pre-check failed Agent/Client system target1.mycompany.com is not responding The West APX execute was not successful
Status	Output							
Server: target1.mycompany.com Created Time: 16:50:45 Client Exit Code: 1	Error from remote (3054): Handler pre-check failed Agent/Client system target1.mycompany.com is not responding The West APX execute was not successful							

Update the HP DMA APX

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

Note: The following steps must be performed by an SA user (<SA_APX_User>) who belongs to a group with the following SA privileges:

- List, read, write, and execute permissions on the objects in the /DMA_APX folder.
- OGSH permission to Launch Global Shell.
- Manage Extensions (Read & Write) permission under Automation Platform Extension.
- List, Read, and Write permission on the /DMA_APX folder.

For more information about the SA permissions, see the HP Server Automation documentation library, which is available on the HP Software Product Manuals web site:

<http://h20230.www2.hp.com/selfsolve/manuals>

To update the HP DMA APX:

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

Create and Configure the HP DMA Custom Field

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

To create and configure the Custom Field:

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

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

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

agent_username_win with type Text

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

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

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

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

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

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

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

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

Run as a Windows Domain User

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

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

Note: The specified domain user must:

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

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

- [Configure Windows Domain User Using Custom Fields](#)
- [Configure Windows Domain User Using Runtime Parameters](#)

Configure Windows Domain User Using Custom Fields

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

- domain_username_win
- domain_password_win

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

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

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

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

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

- domain_username_win with type Text
- domain_password_win with type Password

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

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

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

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

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

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

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

Note: If you have renamed the Windows Administrator account on your Windows target servers, you must also perform the procedures required to [Specify a Renamed Windows Administrator User](#) on page 79.

Configure Windows Domain User Using Runtime Parameters

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

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

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

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

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

Workflow	Step
MS SQL - Install Standalone SQL Instance	MS SQL - Advanced Parameters - Install Standalone
MS SQL - Install Clustered SQL Instance	MS SQL - Gather Advanced Parameters For Install Clustered SQL Instance
MS SQL - Add Node to Cluster	MS SQL - Advanced Parameters - Add Node to Cluster
MS SQL - Upgrade Standalone SQL Instance	MS SQL - Advanced Parameters - Upgrade Standalone
MS SQL Create Database	MS SQL Advanced Parameters Create Database
MS SQL Drop Database	MS SQL Parameters Drop Database
MS SQL - Install Patch	MS SQL - Advanced Parameters - Install Patch
MS SQL Rollback Patch	MS SQL Gather Advanced Parameters for Rollback Patch
Backup and Restore MS SQL Database	Gather Advanced Parameters for MS SQL Database Backup and Restore
Backup MS SQL Database	Gather Advanced Parameters for MS SQL Database Backup
Restore MS SQL Database	Gather Advanced Parameters for MS SQL Database Restore

Workflow	Step
Run MS SQL Compliance Audit	Gather Advanced Parameters for MS SQL Compliance
DB Release for SQL Server	MS SQL - Parameters - DB Release for SQL Server
Discovery	Discover SQL Databases

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

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

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

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

Note: If you have renamed the Windows Administrator account on your Windows target servers, you must also perform the procedures required to [Specify a Renamed Windows Administrator User](#) on page 79.

Change the Number of Active Connections

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

To change the number of active connections:

1. As root, stop the HP DMA server:

```
$ service dma stop
```

2. Open the following file in a text editor:

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

3. Modify the following parameters:

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

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

4. Start the HP DMA server again:

```
$ service dma start
```

Chapter 7: Troubleshooting

This chapter provides information that will help you troubleshoot problems that can arise during the installation and initial configuration of HP Database and Middleware Automation (HP DMA) version 10.21.

Debugging Tools

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

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

0	No debug
1	Error debug
2	Warning debug
3	Success, information, and notice debug
4	Debug debug
5	Verbose debug
99	Maximum debug
- **west_verbose:** Determines whether additional debug logging is written to the HP DMA Client log. Valid values are TRUE and FALSE.

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

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

To create and configure the debug Custom Fields:

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

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


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

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

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

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

To obtain debug information:

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

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

To turn off debug:

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

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

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

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

Troubleshooting Issues

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

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

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

Problem	Installation Step	Probable Cause
<p>No Servers Available to Add to HP DMA</p>	<p>Add Available Targets</p>	<p>The HP DMA Connector User Does Not Have Required Permissions</p>
		<p>The HP DMA Connector User Cannot Find Any Servers</p>
		<p>The Servers Are Already in Another HP DMA Organization</p>
		<p>The HP DMA User Does Not Have Correct Permissions</p>
		<p>The DMA Client Files Policy Is Not Attached and Remediated</p>
<p>Run Time Errors</p>	<p>This error does not show up during the install process but when you run an HP DMA workflow.</p>	<p>Workflow Aborts Using an Internal SSL Certificate</p>
<p>Performance Issues</p>	<p>Performance issues do not show up during the install process but when you run HP DMA workflows.</p>	<p>Intermittently Unable to Log In and System Freezes</p>
<p>Password Security</p>	<p>This issue does not show up during the install process. Use these instructions to reset the HP DMA Initial Admin password.</p>	<p>Reset the HP DMA Initial Admin password</p>

Common Baseline Errors

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

- Not setting up Oracle Database as specified in [Create and Configure the Oracle Database](#) on page 19.
- The TNS listener is not running.
- Not specifying the correct values in the `dmaBaselineData` command.
- Not specifying the correct HP DMA server host name in the `dmaBaselineData` command.
- Not running the `dmaBaselineData` command with the correct permissions (root).

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

For additional information, see [Install the HP DMA Server](#) on page 25.

Oracle Database User Was Not Created

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

1. Log in to Oracle Database:

```
sqlplus / as sysdba
```

2. Run the following query:

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

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

If your HP DMA Oracle Database user name is not in the list, have your Oracle Database administrator (DBA) follow the instructions in [Create and Configure the Oracle Database](#) on page 19 to add the HP DMA Oracle Database user.

Oracle Listener Is Not Running

To verify that the Oracle Listener is running:

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

```
su - oracle
```

```
ps -ef | grep tns
```

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

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

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

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

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

Oracle Database Is Not Running

To verify that Oracle Database is running:

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

```
su - oracle
```

```
ps -ef | grep pmon
```

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

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

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

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

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

Error in the Oracle Server or Oracle SID Name

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

For example:

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

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

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

To solve this problem:

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

HP DMA Client Fails to Contact HP DMA Server

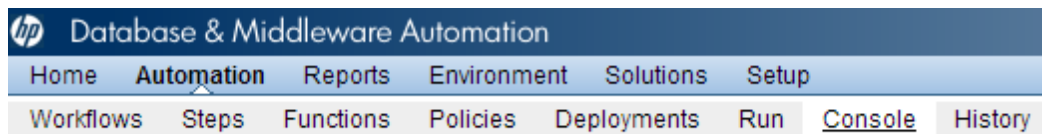
If the target server cannot communicate with the HP DMA server, a workflow will appear to be running when it really is not. There are several possible causes of this problem:

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

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

Symptoms

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



Console

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

Output

Discovery Parameters
Initiated

Nothing here

Never changes to Running

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

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

This log file is located here on the target server:

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

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

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

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

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

Solution

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

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

Perform these steps on the HP DMA server:

1. Stop the DMA service.

```
$ service dma stop
```

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

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

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

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

3. Start the DMA service.

```
$ service dma start
```

Note: You must also terminate the HP DMA Client process on the target server (see [Workflow Execution Script](#) on page 129).

Did Not Run the Baseline Command as Root User

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

For example:

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


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

```
log4j:ERROR setFile(null,true) call failed.
java.io.FileNotFoundException: /var/log/hp/dma/dma.log (Permission denied)
    at java.io.FileOutputStream.openAppend(Native Method)
    at java.io.FileOutputStream.<init>(Unknown Source)
    at java.io.FileOutputStream.<init>(Unknown Source)
    at org.apache.log4j.FileAppender.setFile(FileAppender.java:294)
    at org.apache.log4j.RollingFileAppender.setFile(RollingFileAppender.
java:207)
    at org.apache.log4j.FileAppender.activateOptions(FileAppender.java:1
65)
...
java.io.FileNotFoundException: /opt/hp/dma/server/tomcat/webapps/dma/WEB-INF
/./WEB-INF/./././././conf/Catalina/localhost/dma.xml (Permission denied)
    at java.io.FileOutputStream.open(Native Method)
    at java.io.FileOutputStream.<init>(Unknown Source)
    at java.io.FileOutputStream.<init>(Unknown Source)
    at com.hp.dma.cmdline.DMABaselineData.saveXMLFile(DMABaselineData.ja
va:713)
    at com.hp.dma.cmdline.DMABaselineData.main(DMABaselineData.java:837)
30 Jan 2005 10:43:43,463 ERROR CmdlineExceptionHandler - Exception
java.lang.Throwable: java.io.FileNotFoundException: /opt/hp/dma/server/tomca
t/webapps/dma/WEB-INF/./WEB-INF/./././././conf/Catalina/localhost/dma.xml (P
ermission denied
...

```

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

APX Tool Configuration Error

You may receive an error that you do not have a valid APX file or directory when you perform the [Import the HP DMA APX](#) step.

Not Pointing to Correct APX Tool Directory

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

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

If you have this problem, verify the location of the APX tool and rerun the `apxtool` command (see [Import the HP DMA APX](#)).

DMA Client Files Policy Error

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

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

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

For additional information, see [Install the DMA Client Files Policy](#) on page 43.

DMA_Client Directory Does Not Exist or Is Not Writable

Symptoms

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

```
...
# sh ./dma_upload.sh -host sa2.mycompany.com -user myusername -password mypassword -keyFile /opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/PublicKey -folderName /DMA_Client
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
Dload  Upload  Total  Spent    Left  Speed
100 2780k 100 2780k    0     0  120M      0 --:--:-- --:--:-- --:--:-- 14
2M
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
Dload  Upload  Total  Spent    Left  Speed
100 1712k 100 1712k    0     0  127M      0 --:--:-- --:--:-- --:--:-- 15
1M
CORBA BAD_PARAM 0 No; nested exception is:
org.omg.CORBA.BAD_PARAM:  vmcid: 0x0  minor code: 0  completed: No
...
```

Solution

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

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

```
...  
# sh ./dma_upload.sh -host sa2.mycompany.com -user myusername -password mypassword -keyFile /opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/PublicKey -folderName /DMA_Client  
% Total      % Received % Xferd  Average Speed   Time    Time       Time  Current  
Dload Upload  Total   Spent    Left  Speed  
100 2780k 100 2780k    0     0  137M      0  --:--:--  --:--:--  --:--:-- 15  
0M  
% Total      % Received % Xferd  Average Speed   Time    Time       Time  Current  
Dload Upload  Total   Spent    Left  Speed  
100 1712k 100 1712k    0     0  121M      0  --:--:--  --:--:--  --:--:-- 13  
9M  
Policy associations for DMA completed.  
...
```

Microsoft Patch Database Is Out of Date

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

Symptoms

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

```
The request to retrieve information from the Agent failed for an  
unknown reason, please contact your HP Server Automation  
Administrator.Execution error: Traceback (most recent call last):  
File ".\base\wayfuncs.py",line 136, in evaluator  
File "", line 3058, in ?  
  
...  
  
File ".\nt_hotfix_handler.py", line 539, in installedList  
File ".\nt\nt_hotfix_handler.py", line 521, in filterMbsa20ResultByInstalled  
OrRecommended  
OpwareError:  
  
...  
  
params: {'handler':'nt_hotfix_handler','results':'AGENT_ERROR_PATCH_DATABASE_  
CERTIFICATE_ERROR'}  
request: UNKNOWN  
tb_change: []  
  
...
```

Solution

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

You should verify that you are using the current Microsoft links and files. The ones listed here were correct as of the publication of this guide.

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

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

- a. Update Products from Vendor:

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

- b. Update Product List from File:

Download the `wuredist.cab` file manually at <http://update.microsoft.com/redist/wuredist.cab> and then click the Update Product List from File button to update the `wuredist.cab` file that you just downloaded.

3. Update the Security Update Catalog (`wsusscn2.cab`) with one of the following methods:

- a. Update Products from Vendor:

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

- b. Update Product List from File:

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

This updates the catalog of available patches.

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

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

b. Import from File:

Download the installer files manually from:

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

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

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

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

6. Clean up any Windows 2012 servers that indicate that the DMA Client Files policy is installed but are actually in a corrupt state.
7. Install the DMA Client Files policy on the Windows 2012 servers and remediate. For more information, see [Install the DMA Client Files Policy](#).

Examine the contents of the Job Status log for the  Succeeded status.

8. To update your repository with the same patching tools, copy the files that were downloaded in steps 3 and 5 to the Windows patching utilities directory on your SA Core (for example: /root/wintools or /root/winutils).

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

<http://h20230.www2.hp.com/selfsolve/manuals>

Connector Errors

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

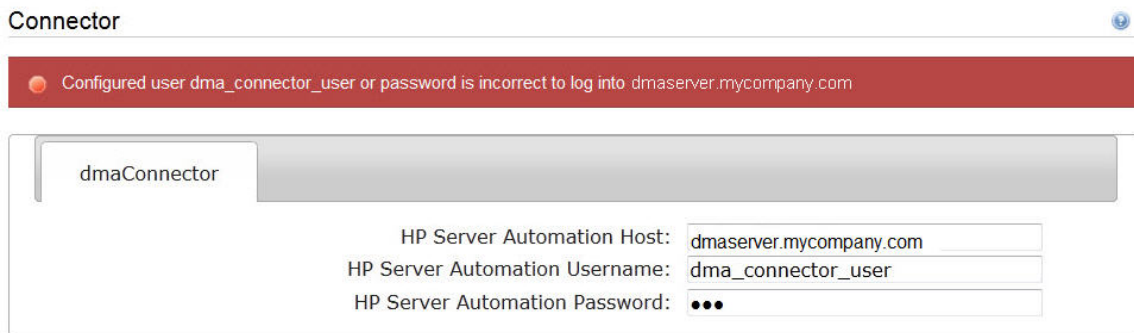
- The SA Core server is down.
- The JAR files are not at the required locations.

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

For additional information, see [Configure the Connector](#) on page 50.

The SA Core Server Is Down

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



Connector

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

dmaConnector

HP Server Automation Host: dmaserver.mycompany.com

HP Server Automation Username: dma_connector_user

HP Server Automation Password: ●●●

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

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

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

The JAR Files Are Not at the Required Locations

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

Connector ?

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

lupulin

HP Server Automation Host:

HP Server Automation Username:

HP Server Automation Password:

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

```
2005-01-30 16:37:54,626 INFO [main] PersistenceService:137 - Setting oracle
.net.tns.admin
2005-01-30 16:37:57,037 INFO [main] WorkflowStarter:107 - abortIfNotStarted
= true
2005-01-30 16:37:57,489 ERROR [main] StartupListener:114 - Unable to connect
to Server Automation because opswclient.jar and twistclient.jar have not been
copied to /opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/lib
2005-01-30 16:37:57,489 INFO [main] StartupListener:115 - Failure:
java.lang.NoClassDefFoundError: com/opsware/client/TokenFinder
...
2005-01-30 16:37:57,491 ERROR [main] StartupListener:49 - Exception on start
up
java.lang.RuntimeException: Unable to start DMA due to Connector failure
```

To fix this problem, run the script command to copy the required JAR files to the correct locations as described in [Install the HP DMA Server](#) on page 25.

Login Errors

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

- Credentials are incorrect or do not allow login.
- **Error:** Failed to connect with the configured database.

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

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

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

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

The SA Core Server Is Down

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

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

...

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

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

The SA Group Does Not have Login Access

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

```
...

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

...
```

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

See [Set Up the SA Groups and Users](#) on page 44 for more information.

HP DMA Started Before SA was Running

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

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

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

1. Stop the DMA service.

```
$ service dma stop
```

2. Start the DMA service.

```
$ service dma start
```

Oracle Database Password Changed

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

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

```
2014-03-03 12:18:14,436 INFO [localhost-startStop-1] PersistenceService:143
- Setting oracle.net.tns.admin
2014-03-03 12:18:15,412 ERROR [localhost-startStop-1] StartupListener:63 - E
xception on startup
org.hibernate.HibernateException: Connection cannot be null when 'hibernate.
dialect' not set
at org.hibernate.service.jdbc.dialect.internal.DialectFactoryImpl.determineD
ialect(DialectFactoryImpl.java:97)
at org.hibernate.service.jdbc.dialect.internal.DialectFactoryImpl.buildDiale
ct(DialectFactoryImpl.java:67)
at org.hibernate.engine.jdbc.internal.JdbcServicesImpl.configure(JdbcService
sImpl.java:170)
...
at java.util.concurrent.Executors$RunnableAdapter.call(Unknown Source)
at java.util.concurrent.FutureTask.run(Unknown Source)
at java.util.concurrent.ThreadPoolExecutor.runWorker(Unknown Source)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(Unknown Source)
at java.lang.Thread.run(Unknown Source)
```

If your Oracle password changed, perform the following:

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

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

Use either the short command:

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

Or the long command:

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

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

2. Restart the DMA service:

```
$ service dma restart
```

The HP DMA Database is Not Accessible

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

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

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

3. Verify the following:
 - You are pointing to the correct system—this might be incorrect in `/etc/hosts` or DNS.
 - You have the correct database user.
 - You have the correct Oracle SID.
 - You have the correct port number.

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

4. Stop the DMA service:

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

```
$ service dma restart
```

The SA Core was Updated

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

To solve this problem perform the following steps:

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

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

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

2. Restart the DMA service:

```
$ service dma restart
```

HP DMA is Switched to Different SA Core

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





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

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

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

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

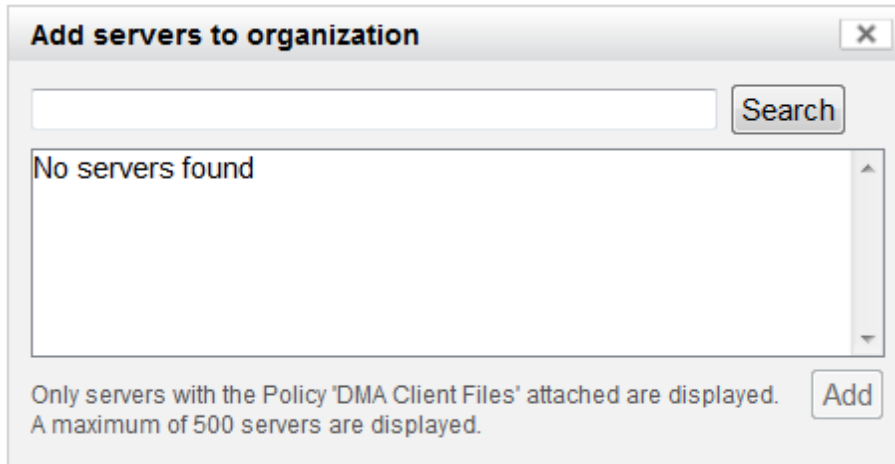
To solve this problem perform the following steps while logged in to the HP DMA server as the default initial HP DMA administrator (`dma_initial_admin`):

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

- c. Remove any of the capabilities and then click **Save**.
- d. Add the capability that you removed and then click **Save** again.

No Servers Available to Add to HP DMA

If no servers are available in the [Add Available Targets](#) step, you will see the following error when you try to add servers to an organization:



There are several situations that may cause this problem:

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

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

The HP DMA Connector User Does Not Have Required Permissions

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

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

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

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

For more information, see [Set Up the SA Groups and Users](#).

The HP DMA Connector User Cannot Find Any Servers

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

```
...  
2013-03-15 14:59:57,377 INFO [http-8080-1] DmaPolicyCacher.getDMASoftwarePol  
icyRef:306  
DMA Software Policy ref is DMA Client Files (SoftwarePolicyRef:1230001)  
...  
2013-03-15 14:59:57,634 INFO [http-8080-1] DmaPolicyCacher.findServers:107  
User can't read any servers or no servers have policy DMA Client Files  
...
```

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

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

For more information, see [Install the DMA Client Files Policy](#) and [Set Up the SA Groups and Users](#).

The Servers Are Already in Another HP DMA Organization

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

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

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

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

The HP DMA User Does Not Have Correct Permissions

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

To determine whether this is the case:

1. Log in to HP DMA as a different user, preferably one with Administrator capability.
2. Have this user try to add targets (see [Add Available Targets](#)).

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

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

For more information, see [Set Up the SA Groups and Users](#).

The DMA Client Files Policy Is Not Attached and Remediated

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

To determine whether this is the case, have your SA administrator check that the DMA Client Files policy is attached and remediated on all servers that need to be available to HP DMA, as described in [Install the DMA Client Files Policy](#).

Run Time Errors

If an HP DMA workflow aborts when you run it, it may be caused by using an internal SSL certificate.

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

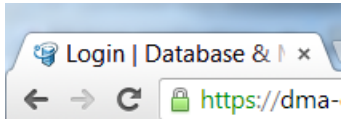
Workflow Aborts Using an Internal SSL Certificate

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

Symptoms

If you have this problem you will observe the following:

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



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

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

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

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

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

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

Solution

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

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

Performance Issues

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

Intermittently Unable to Log In and System Freezes

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

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

You can resolve this by changing the HP DMA configuration:

1. Stop HP DMA:

```
# service dma stop
```

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

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

3. Add the following lines to the file:

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

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

5. Start HP DMA:

```
# service dma start
```

Password Security

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

Reset the HP DMA Initial Admin password

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

To obtain online help:

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

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

Here, `-help` is optional.

Method 1: To reset the password Interactively

Perform these steps on the HP DMA server:

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

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

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

Method 2: To reset the password on the command line

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

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

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

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

Results

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

```
Successfully updated the dma_initial_admin password.
```

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

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

Chapter 8: Reference Information

This chapter contains the following information:

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

HP Software Documentation

HP Database and Middleware Automation Documentation

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

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

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

<http://h20230.www2.hp.com/selfsolve/manuals>

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

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

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

HP Server Automation Documentation

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

<http://h20230.www2.hp.com/selfsolve/manuals>

HP Live Network connector Documentation

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

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

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

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

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

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

Note: You must sign in to HP Live Network using your HP Passport credentials. (See [Support](#) on page 3 for more information about obtaining an HP Passport account.)

HP DMA Baseline Options

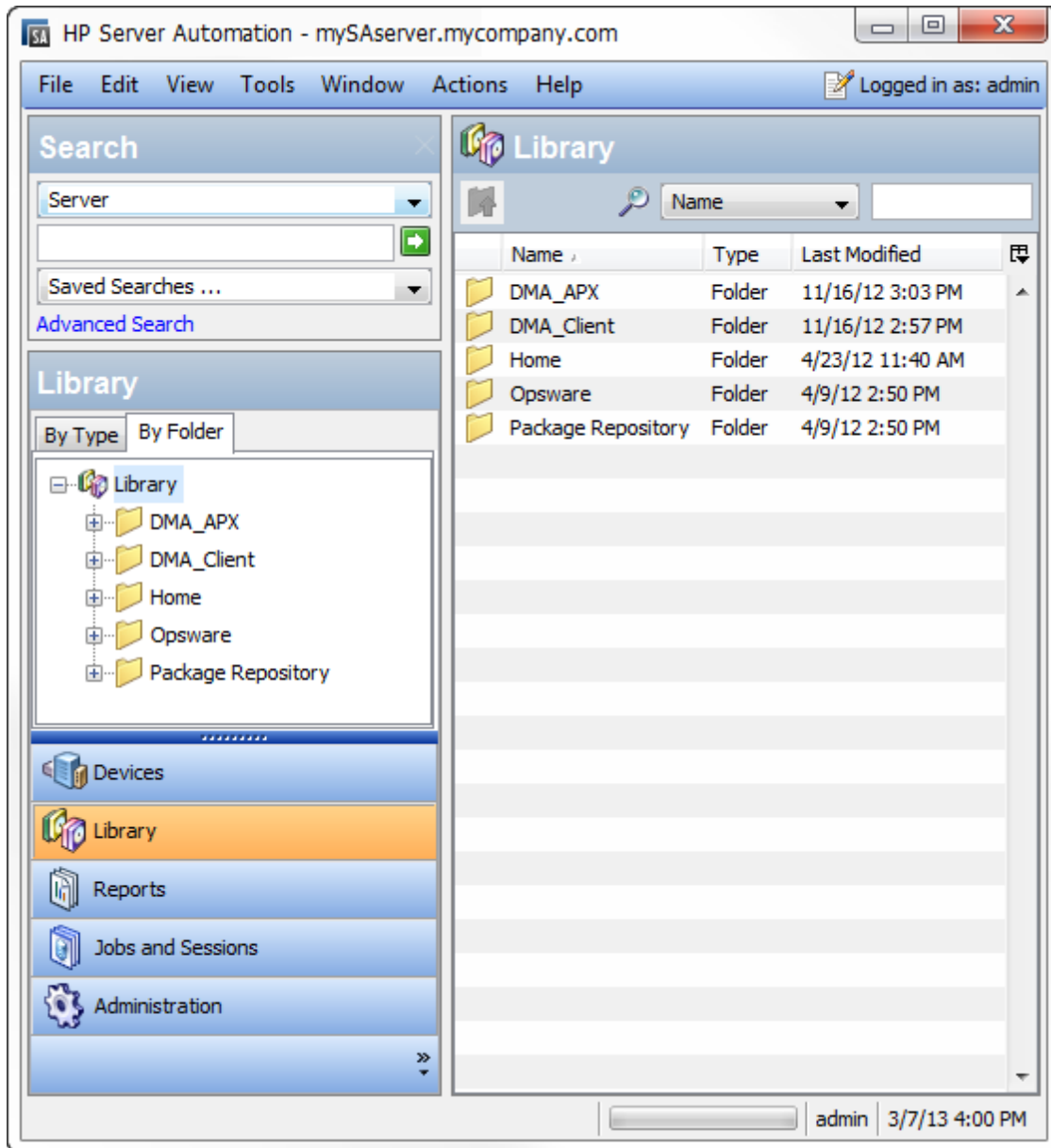
The following table gives a complete list of all the `dmaBaselineData.sh` options:

Option	Example Argument Value	Description
<code>-?,--help</code>		Print this usage message.
<code>-c,--create-tables</code>		Create tables for database.
<code>-cc,--create-context</code>		Create a context file with the specified settings.
<code>-context,--deployed-context-file <dma.xml></code>	<code>dma.xml</code>	Fully qualified path to the deployed context file to get database connection settings.
<code>-dbh,--database-hostname <arg></code>	<code>oracle.mycompany.com</code>	The database host name for the Java Database Connectivity (JDBC) connection.
<code>-dbp,--database-port <arg></code>	<code>1521</code>	The database port for the Java Database Connectivity (JDBC) connection.
<code>-dbpw,--database-password <dbpasswordValue></code>	<code>dbpassword</code>	The password used to connect to the database.
<code>-dbs,--database-sid <arg></code>	<code>dma</code>	The database SID for the Java Database Connectivity (JDBC) connection.
<code>-dbts,--database-tablespace <arg></code>	<code>/u01/app/oracle/oradata/dma</code>	The base directory for the database tablespace creation.
<code>-dbtype,--database-type <arg></code>	<code>oracle</code>	(optional) The underlying database type. The default is oracle.
<code>-dbu,--database-username <dbusernameValue></code>		The username used to connect to the database.
<code>-dmah,--dma-hostname <dmahostnameValue></code>	<code>dma.mycompany.com</code>	Set the fully qualified host name of the HP DMA server. Note: If this value is not specified, the default is the server where the script is running.

Option	Example Argument Value	Description
-e,--erase		Erase existing data and add baseline data. Caution: Do not do this unless instructed to by HP Support.
-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. Note: Other connection string syntax is possible. Consult your Oracle DBA for the company standard.
-okeys,--overwrite-keys		Overwrite public and private key in the database if they exist Caution: Do not do this unless instructed to by HP Support.
-privkey,--private-key-file <privateKeyFilename>		File containing the private key.
-pubkey,--public-key-file <publicKeyFilename>		File containing the public key.
-sahostname,--server-automation-hostname <sahostnameValue>	saserver.mycompany.com	The fully qualified host name of the SA server.
-sapassword,--server-automation-password <sapasswordValue>		The password used to connect to SA.
-sausername,--server-automation-username <sausernameValue>		The username used to connect to the SA.
-sqlfile,--baseline-sqlfile <baselineSQLfile>		The baseline file containing SQL insert statements
-t,--test		Test the underlying database connection.

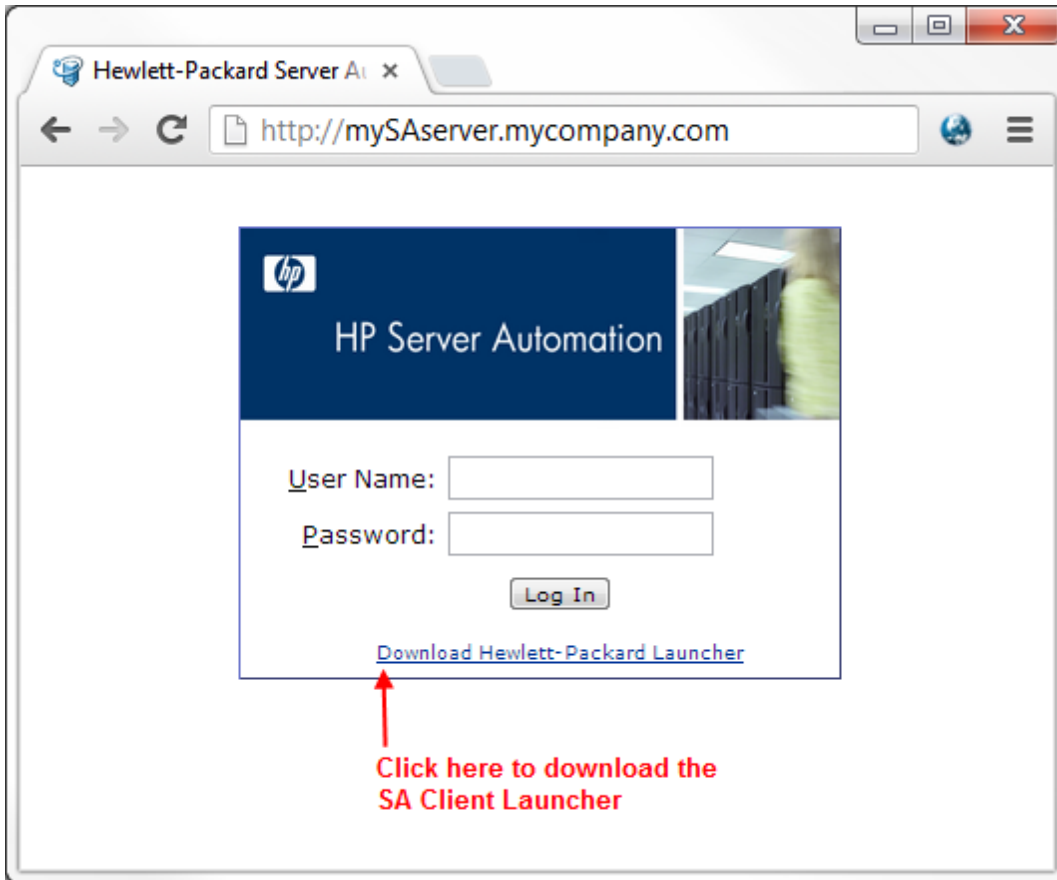
About the SA Client

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



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

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



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

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

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

<http://h20230.www2.hp.com/selfsolve/manuals>

Workflow Execution Script

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

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

WEST is installed on each target server when you attach and remediate the DMA Client Files software policy on that target (see [Install the DMA Client Files Policy](#) on page 43).

Under certain circumstances, you may need to manually terminate WEST on a target server. This would be necessary, for example, if the HP DMA server name was specified incorrectly when the `dmaBaselineData` command was executed, and a workflow execution was subsequently attempted (see [HP DMA Client Fails to Contact HP DMA Server](#) on page 94).

To terminate WEST on UNIX targets:

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

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

2. Kill that process.

To terminate WEST on Windows targets:

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

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

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

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

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

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