



**Hewlett Packard**  
Enterprise

# **HPE Database and Middleware Automation**

Ultimate Edition

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

## **Administration Guide**

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

## Legal Notices

### Warranty

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

The information contained herein is subject to change without notice.

### Restricted Rights Legend

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

### Copyright Notice

© Copyright 2015 Hewlett Packard Enterprise Development LP

### Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

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

## Documentation Updates

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

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

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

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

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

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

## Support

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

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

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

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HPE support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

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

**<https://hpp12.passport.hp.com/hppcf/createuser.do>**

To find more information about access levels, go to:

**<https://softwaresupport.hp.com/web/softwaresupport/access-levels>**

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

## About this PDF Version of Online Help

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

# Contents

Administering .....	7
Enabling IPv6 .....	8
Configuring SSL on the HPE DMA Server .....	9
About the keytool utility .....	9
Generating a Private Key for the Server .....	9
Generating the Certificate Signing Request to Obtain Signed Server Certificates .....	10
Importing the SSL Server Certificates .....	11
Configuring the HPE DMA Server to Use Your Certificate .....	13
Verifying the SSL Connection .....	15
Configuring the Connector .....	15
Copying JAR Files .....	16
Configuring the Connector .....	16
Registering DMA Roles .....	18
Assigning HPE DMACapabilities .....	19
Adding Available Targets .....	20
Importing a Solution Pack .....	22
Targets .....	23
Organizations .....	24
Servers .....	25
Custom Fields .....	25
Smart Groups .....	27
Policies .....	28
Discovery .....	29
Solution Packs .....	30
Installing a Solution Pack .....	30
Versioning and Importing Solution Packs .....	32
Modifying a Solution Item .....	33
Rolling Back a Solution Pack .....	33
Deleting a Solution Pack .....	34
Configuring Email Settings .....	35
Hiding and Unhiding Workflows .....	35
Changing the Default Port and Security Level .....	39
Using a Proxy Server .....	40
Default HPE DMA Communications .....	41
Using an SA Satellite as a Proxy Server .....	42
How HPE DMA Manages Proxy Communication .....	43
Setting Up a Proxy Server .....	44
Configuring the SA Core Gateway Properties .....	44
Specifying the Server Automation Realm .....	45

Creating and Configuring the HPE DMA Custom Fields .....	46
Permission Settings .....	47
Specifying a Renamed Windows Administrator User .....	49
Updating the HPE DMA APX .....	50
Creating and Configuring the HPE DMA Custom Field .....	50
Running Workflows as a Windows Domain User .....	52
Configuring Windows Domain User Using Custom Fields .....	52
Configuring the Windows Domain User Using Runtime Parameters .....	53
Changing the Number of Active Connections .....	55
Configuring HADR using Oracle Database .....	55
HPE DMA HA Standard Architecture Solution .....	55
HPE DMA HA and DR Architecture Solution (Active-Passive) .....	56
HPE DMA HA and DR Architecture Solution (Active-Active Tomcat and Active-Passive Database) .....	58
HPE DMA Baseline Options .....	59
Configuring HADR using PostgreSQL Database .....	60
HPE DMA HA and DR Architecture Solution (Active-Passive) .....	61
How to Setup the HPE DMA Server on the Passive Standby Environment .....	62
How to Handle Failover for an Active Standby Environment .....	62
HPE DMA HA and DR Architecture Solution (Active-Active Tomcat and Active-Passive Database) .....	63
How to Setup the HPE DMA Server on the Active Standby Environment .....	63
How to Configure Failover when the Primary Database is Lost .....	64
Replicating Data .....	64
Example 1 – Both databases are active .....	64
Example 2 – Second database is only for reading .....	67
Bridged Execution Workflow .....	69
Running a Bridged Execution Workflow .....	69
Additional Considerations .....	69
Example .....	71
Workflow .....	72
Targetable Steps .....	73
Deployment .....	74
Run .....	74
Importing a File into the Software Repository .....	75
Maintenance .....	77
Resetting the HPE DMA Initial Admin password .....	77
Updating the Self-signed SSL Certificate .....	79
Updating Self-signed SSL Certificate on the HPE DMA Server .....	79
Send Documentation Feedback .....	82



# Administering

This section provides information to help you administer HPE DMA.

Topics	Description
<a href="#">"Configuring the Connector" on page 15</a>	Provides instructions to configure connector.
<a href="#">"Configuring SSL on the HPE DMA Server" on page 9</a>	Provides instructions to configure SSL.
<a href="#">"Targets" on page 23</a>	Provides instructions to configure and manage target environments.
<a href="#">"Solution Packs" on page 30</a>	Provides information on downloading and installing solution packs.
<a href="#">"Configuring Email Settings" on page 35</a>	Provides information on configuring email.
<a href="#">"Hiding and Unhiding Workflows" on page 35</a>	Provides information on hiding or unhiding workflows.
<a href="#">"Changing the Default Port and Security Level" on page 39</a>	Provides information on changing default port and security level.
<a href="#">"Using a Proxy Server" on page 40</a>	Provides information on using an HP SA Satellite as a proxy server.
<a href="#">"Setting Up a Proxy Server " on page 44</a>	Provides instructions on configuring a proxy server.
<a href="#">"Specifying a Renamed Windows Administrator User" on page 49</a>	Provides instructions to change Windows administrator user.
<a href="#">"Running Workflows as a Windows Domain User" on page 52</a>	Provides instructions to run workflows as a specific Windows domain user.
<a href="#">"Changing the Number of Active Connections" on page 55</a>	Provides instructions to change the number of active database connections.
<a href="#">"Configuring HADR using Oracle Database" on page 55</a>	Provides instructions to setup HPE DMA for HADR using Oracle database.
<a href="#">"Configuring HADR using PostgreSQL Database" on page 60</a>	Provides instructions to setup HPE DMA for HADR using PostgreSQL database.
<a href="#">"Replicating Data" on page 64</a>	Provides information on replicating data.
<a href="#">"Permission Settings" on page 47</a>	Describes permission settings to manage DMA.
<a href="#">"Bridged Execution Workflow" on page 69</a>	Provides information on running bridged workflows.
<a href="#">"Importing a File into the Software Repository" on page 75</a>	Provides instruction to import a file into the software repository.
<a href="#">"Maintenance" on page 77</a>	Provides information on maintaining HPE DMA capabilities.

# Enabling IPv6

Perform the following steps to enable Internet Protocol version 6 (IPv6) after installing DMA server (fresh install/upgrade):

1. Stop HPE 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. Modify the hostname for the `webServiceUrl` parameter to the hostname that resolves into an IPv6 address.
4. Save your changes to the `dma.xml` file and exit the text editor.
5. Start HPE DMA:  
`# service dma start`



# Configuring SSL on the HPE DMA Server

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

1. ["Generating a Private Key for the Server" below](#)
2. ["Generating the Certificate Signing Request to Obtain Signed Server Certificates" on the next page](#)
3. ["Importing the SSL Server Certificates" on page 11](#)
4. ["Configuring the HPE DMA Server to Use Your Certificate" on page 13](#)
5. ["Verifying the SSL Connection" on page 15](#)

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

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

**Caution:** If you are using an SA gateway infrastructure as a proxy network, you must have a subject alternate name (SAN) as part of your signed certificate:

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

For detailed instructions and an example of the `keytool` command that sets up the SAN, see ["Using a Proxy 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 the keytool utility

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

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

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

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

```
which keytool
```

## Generating a Private Key for the Server

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

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

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

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

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

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

The variables used here refer to the following information:

Variable	Description
<keyalias>	Unique alias for the server's private key. This will be used to associate the server certificate with its private key. For HPE DMA, set to <code>tomcat</code> .
<DMAserver>	Fully qualified host name of the server hosting the HPE DMA server.
<orgunit>	The organizational unit (business unit) that owns this server.
<org>	The organization (company) that owns this server.
<location>	The city in which this server physically resides.
<state>	The state or province in which this server physically resides.
<country>	The country in which this server physically resides.
<password>	The password for both the keystore and this private key.
<storefile>	Keystore file name. For example: <code>/opt/hp/dma/server/.mykeystore</code>
<numberdays>	The number of days that the key will be valid.

For example:

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

**Note:** You must use the same password for the `-keypass` and `-storepass` settings.

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

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

## Generating the Certificate Signing Request to Obtain Signed Server Certificates

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

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

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

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

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

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

For example:

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

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.

## Importing the SSL Server Certificates

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

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

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

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

**Note:** Your CA may provide any or all of these certificates:

- Root certificate
- Primary intermediate certificate
- Secondary intermediate certificate

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

The variables used here refer to the following information:

Variable	Description	Examples
<keyalias>	Unique alias for the server's private key. This will be used to associate the server certificate with its private key.	For root certificate: my-root-cert For primary intermediate certificate: my-cert-pri For secondary intermediate certificate: my-cert-sec
<CAcert>	File that contains the contents of the certificate.	For root certificate: CA-root-cert.cer For primary intermediate certificate: CA-cert-pri.cer For secondary intermediate certificate: CA-cert-sec.cer
<storefile>	Fully qualified keystore file name.	/opt/hp/dma/server/.mykeystore
<password>	The password for both the keystore and the private key.	mypassword

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

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

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

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

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

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

For example:

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

You should see the following type of output:

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

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

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

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

## Configuring the HPE DMA Server to Use Your Certificate

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

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

### To configure the HPE DMA server to use your certificate:

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

```
service dma stop
```

2. Open the following file in a text editor:

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

3. Identify the default SSL Connector element:

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

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

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

The variables used here represent the following information:

Variable	Description
<code>&lt;keyalias&gt;</code>	Unique alias for the server's private key (see <a href="#">"Generating a Private Key for the Server" on page 9</a> ).
<code>&lt;SSLport&gt;</code>	Port that will be used for: <ul style="list-style-type: none"> <li>• SSL communication between the HPE DMA Server and the HPE DMA clients</li> <li>• Accessing the HPE DMA user interface</li> </ul>
<code>&lt;storefile&gt;</code>	Keystore file name. For example: <code>/opt/hp/dma/server/.mykeystore</code>
<code>&lt;password&gt;</code>	The password for both the keystore and this private key.

For example:

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

6. Save the `server.xml` file.
7. Open the following file in a text editor:  
`/opt/hp/dma/server/tomcat/conf/Catalina/localhost/dma.xml`
8. Identify the following line:

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

9. Set the value to false.

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

If the line does not exist, add it.

10. Locate the following line:

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

For example:

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

11. Ensure that the `<DMAserver>` specified in the `webServiceUrl` value matches the `<DMAserver>` configured in the public certificate. They must both be IP addresses or both be host names.

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

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

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


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


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

## Verifying the SSL Connection

To verify your SSL connection, perform the following steps:

1. Log in to your HPE DMA server.
2. HTTPS protocol indicates that the HPE DMA Server is communicating with the HPE DMA Client using SSL.

3. The lock icon () in the address bar indicates that the HPE DMA Server is communicating with the HPE DMA Client using SSL.

If there is a problem with the website security certificate, you will see a shield icon () with a warning message.

4. For a test, execute an HPE DMA deployment.
5. When it finishes, navigate to the Automation > History page.
6. Select your deployment and then choose the Step Output tab in the bottom pane.
7. Verify that the deployment ended in SUCCESS—or at least did not have any errors indicating client-server communication issues.
8. Choose the Connector Output tab in the bottom pane.
9. Check that the following line is not in the output:

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

If it is in the output, go back to ["Configuring the HPE DMA Server to Use Your Certificate" on page 13](#), 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.

## Configuring the Connector

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

**Note:** You only do this once.

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

# Copying JAR Files

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

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

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

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

## To copy the required JAR files:

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

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

Here, <SA\_Server> is the fully qualified host name of the SA server to use as the SA Core.

# Configuring the Connector

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

## To configure the Connector:

1. Log in as dma\_initial\_admin.
2. Go to Setup > Connectors.
3. If a Connector already exists, click the tab that corresponds to the Connector for SA.

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

4. Specify the information required.

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

[Configuration](#)
[Permissions](#)
[Capabilities](#)
[Roles](#)
[Connector](#)

## Connector

SAsrvr001.mycompany.com

Server Automation Host:

Server Automation Username:

Server Automation Password:

The user specified here must be a valid SA user with the following permissions:



- List, Read, and Execute permission for the /DMA\_Client folder
- List permission for all parent folders of the /DMA\_Client folder
- Managed Servers and Groups
- Manage Software Policy (READ)

- READ access to all managed servers that will be added to HPE DMA

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

5. Click **Save**.

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

6. Stop and restart your HPE DMA server:

```
# service dma stop
# service dma start
```

# Registering DMA Roles


This topic shows you how to register HPE DMA roles.

HPE DMA obtains the complete set of available roles from Server Automation—including the groups that your SA administrator configured in [Setting 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.

Configuration Permissions Capabilities **Roles** Connectors

## Role Registration

✓ Role(s) saved successfully.

AVAILABLE		REGISTERED
 <b>Command Line Administrators</b> Command Line Administrators	   	 <b>DMA Admins</b> DMA Admins
 <b>Compliance Auditors</b> Compliance Auditors		 <b>DMA Workflow Creators</b> DMA Workflow Creators
 <b>Compliance Enforcers</b> Compliance Enforcers		 <b>DMA Workflow Runners</b> DMA Workflow Runners
 <b>Hypervisor Managers</b> Hypervisor Managers		
 <b>Opware System Administrators</b> Opware System Administrators		
 <b>OS Deployers</b> OS Deployers		
 <b>OS Policy Setters</b> OS Policy Setters		
 <b>Patch Deployers</b> Patch Deployers		
 <b>Patch Policy Setters</b> Patch Policy Setters		
 <b>Software Deployers</b> Software Deployers		

**Save** or **CANCEL**

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

# Assigning HPE DMACapabilities

This topic shows you how to assign HPE 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 HPE DMA.

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

# Adding Available Targets

This task must be performed by the HPE DMA Admin only.

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

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

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

## 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 *HPE DMA Administrator Guide*.

The screenshot shows the HPE DMA web interface. At the top, there are tabs for 'Dashboard', 'Smart Groups', and 'Custom Fields'. Below this is the 'Environment' section with a blue header and a 'Default' organization selected. A table with four columns is visible below the header. To the right of the table is a link labeled 'NEW ORGANIZATION'. Below the table, there is a 'Default' organization section with tabs for 'Properties', 'Custom Fields', and 'Roles'. The 'General' tab is active, showing a 'Name: Default' field. At the bottom, there is a 'DELETE' button with a red 'X' icon, and a row of buttons: 'Add servers', 'Save', and 'CANCEL'.

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

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

**Add servers to organization**

Search

- server1
- server2
- server3
- server4
- server5
- server6
- server7
- server8
- server9

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

Add

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

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.

Configuration Permissions Capabilities Roles Connector

**DMA Admins**

Deployments Workflows Steps Policies **Organizations**

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

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

Save or CANCEL

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

# Importing a Solution Pack

This task must be performed by the HPE DMA Admin only.

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

The following instructions assume that you have purchased a license for HPE DMA.

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

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

## To obtain the most recent HPE DMA patch:

1. Go to the following web site: <https://softwaresupport.hp.com/>
2. Sign in using your HP Passport credentials.
3. Your dashboard experience is based on your SAID. Under **My Products**, select database and middleware automation.
4. Look under **Software Patch** to determine whether a more recent patch is available.
5. If there is a more recent patch, do the following:
  - a. Click the link for the desired patch.
  - b. Under **Download Information**, click the link to download the patch installation media.

## To access the HPE DMA solution packs:

To access the HPE DMA solution packs, mount the ISO file of the HPE DMA10.40 (or patch) installation media.

The solution packs are located in the following folders:

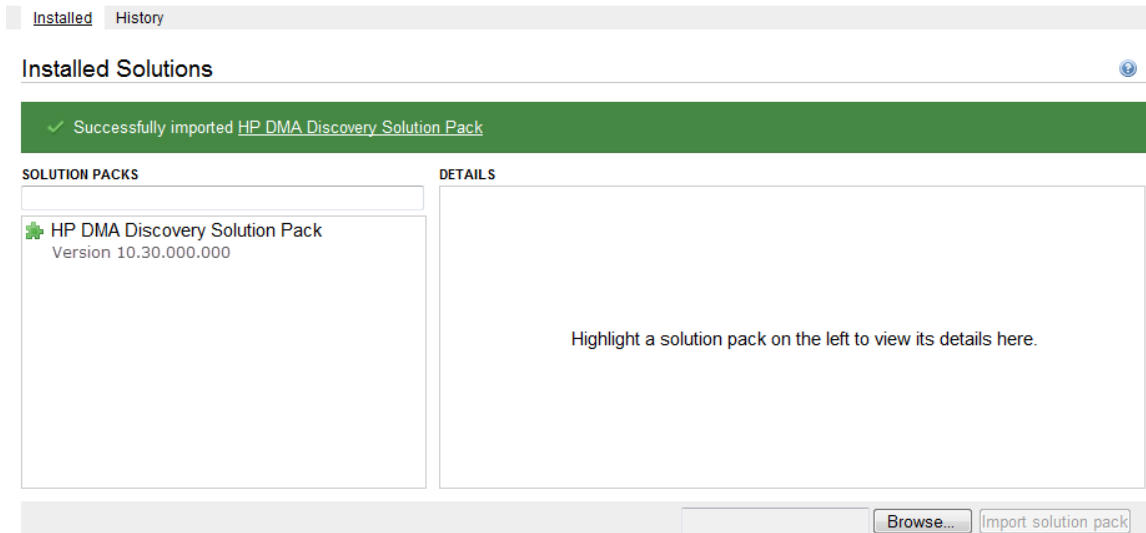
- The `DMA_10.40.000.000_Server_and_Client` folder contains the Discovery and Promote solution packs.  
The Discovery solution pack is not automatically installed with HPE DMA. You must import it if you want to use the discovery workflows.
- The `DMA_10.40.000.000_Database_Solution_Packs` folder contains all of the database solution packs (provisioning, advanced provisioning, patching, advanced patching, compliance, refresh, and release management).
- The `DMA_10.40.000.000_Middleware_Solution_Packs` folder contains all of the application server solution packs (provisioning, patching, configuration management, and release management).

## To import the solution pack:

1. On the system where you mounted the installation media, open a web browser, and go to the following URL:  
`http://<HPE_DMA_server>/dma/login`
2. Log in to the HPE DMA server using an account with Administrator capability.

- 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.



- Locate and select the ZIP file for the desired solution pack, and click **Open**.
- 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 HPE DMA is now ready to use. Refer to the *HPE DMA Administrator Guide* and the *HPE DMA User Guide* for additional information on using HPE DMA.

## Targets

One of the responsibilities of the HPE DMA administrator is to create and manage the HPE DMA target environment. Targets include servers, instances, and databases. Targets reside in organizations.

The HPE DMA Environment page contains two parts: the organization browser is on the top, and the object editor is on the bottom. To open the object editor, select an object (organization, server, instance, or database) in the organization browser.

In the object editor, users who have Read permission for an organization can view specific properties of the objects that reside in that organization. They can also test connectivity between HPE DMA and any database in the organization.

Users who have Write permission for the organization can modify some of these properties. They can also add objects to or delete objects from the organization.

# Organizations

An organization is a logical grouping of servers. Users who have Write permission for an organization can add servers to (or delete servers from) that organization. Because user security for running workflows is implemented at the organization level, organizations should be composed with user security in mind.

The Default organization is built-in to the HPE DMA software. All other organizations must be explicitly created.

Users who have Administrator capability or Write permission for an organization can add or delete servers, instances, and databases in that organization. See the *HPE DMA User Guide* for instructions.

**Note:** You must have Administrator capability to create an organization, modify the permissions for an organization, or delete an organization.

## To create an organization:

1. Go to Environment > Dashboard.
2. Click **New Organization**.
3. Specify a unique Name for the organization.
4. Click **Save**.

## To grant users permission to access a specific organization:

1. Go to Setup > Permissions.
2. Select the role whose permissions you want to modify.
3. Go to the Organizations tab.
4. For each organization listed:
  - Select Read if you want users with this role to be able to view information about this organization, including the servers it contains.
  - Select Write if you want users with this role to be able to modify this organization.
  - Select Deploy if you want users with this role to be able to deploy workflows to the servers in this organization.

Note: Always select Read when you select Write or Deploy.

5. Click **Save**.

Provided that you have Administrator capability, you can delete an organization that contains no servers. Only empty organizations can be deleted.

Servers cannot be moved from one organization to another. They must be deleted from one organization and then added to the other organization.

## To delete an organization:

1. Go to Environment > Dashboard.
2. Select the organization that you want to delete.
3. Click the DELETE link.
4. In response to the "Are you sure?" question, click **Delete**.



# Servers

Servers that will act as HPE DMA targets must have the ability to communicate with HPE DMA.

With Server Automation, servers must be managed by SA and have the DMA Client Files software policy. Any SA managed server with this policy can be added to an HPE DMA organization and used as an HPE DMA target.

**Tip:** See the *HPE DMA Installation Guide* for information about installing the DMA Client Files policy on a managed server.

Users who have Administrator capability or Write permission for an organization can add servers to or delete servers from an organization. They can also add or delete instances and databases. See the *HPE DMA User Guide* for additional information.

## To add servers to an organization:

1. Go to Environment > Dashboard.
2. Select the organization where you want to add the servers.
3. Click **Add servers**.

The “Add servers to organizations” dialog opens. It contains a list of the managed servers that can be used as HPE DMA targets and are not already included in an organization.

The servers that you can see in the list depend on your permissions in Server Automation.

You can use the Search filter to reduce the number of servers listed. The first 500 managed servers whose names contain the string specified in the Search box are listed. To filter the list of servers, specify text in this box, and then click **Search**.

4. Select the Server (or Servers) that you want to add.
5. Click **Add**. The “Add servers to organizations” dialog closes.

## To delete a server from an organization:

1. Go to Environment > Dashboard.
2. Select the organization where you want to delete the server.
3. Click the DELETE link.

Note that you must first delete any instances associated with the server before you will be allowed to delete the server.

4. In response to the “Are you sure?” question, click the **Delete** button.

# Custom Fields

Custom Fields are used to customize workflows or show information about the environment. Custom Fields can be used in workflow steps to automatically supply information that is specific to an organization, server, instance, or database.

For example, you can have a Custom Field that identifies a database as “Production” or “Test” and then use this field in workflows to choose between different behavior for the different types of databases.

When you define a Custom Field for any item in the environment (organization, server, instance, or database), all other items of that type will also have that Custom Field.



For example, if you create a Custom Field called Oracle Home for an instance target, all instance targets will have a Custom Field called Oracle Home—whether or not they actually represent Oracle instances. Except for the original item, the Custom Field will be blank (it will not have a value). Blank Custom Fields have no effect.

Custom Fields can be used by workflows, steps, deployments, and Smart Groups.

As the HPE DMA administrator, you can view, create, or delete any Custom Field. You can modify the options (list items) associated with a list type Custom Field.

For additional information about Custom Fields, see the *HPE DMA User Guide* and the *HPE DMA API Reference WebHelp*.

**To create a new Custom Field:**

1. Go to Environment > Custom Fields.
2. Click **New field**.
3. Specify the following information for your new Custom Field:
  - Name – a unique name for the Custom Field
  - Object – organization, server, instance, or database
  - Type – text, multi-line (contains one or more lines of text), or list
  - Options – items that will be available in the list (for list type fields only)  
To add a list item, type its name in the box, and click . For example:  
To delete a list item, click the  (delete) button.
4. Click **Save**.

**To modify an existing Custom Field:**

1. Go to Environment > Custom Fields.
2. Select the Custom Field that you want to modify.

3. Make the required modifications.

You can only modify Options (list items) associated with list type Custom Fields. You cannot modify the Name, Object, or Type of an existing Custom Field.

4. Click **Save**.

#### To delete a Custom Field:

1. Go to Environment > Custom Fields.
2. Select the Custom Field that you want to delete.

You cannot delete a Custom Field that is referenced by a workflow, step, deployment, or Smart Group.

3. Click the **DELETE** link.
4. Click **Delete** to confirm.

## Smart Groups

Smart Groups are dynamic groups of servers, instances, or databases defined by some criteria. They are used to specify targets for deployments. As information about an environment object changes, its membership in any Smart Groups is re-evaluated.

For example, say that a server has a Custom Field called `sshd_running` that is set to true. This server belongs to an SSH Group of servers. When `sshd_running` for this server changes to false, it is no longer included in the SSH Group.

Each Smart Group is assigned a role. An HPE DMA user can only create Smart Groups for roles assigned to that user. If the role grants the user both READ and DEPLOY permission for an organization, the servers, instances, or databases in that organization can be used in the Smart Group.

As the HPE DMA administrator, you can create, view, modify, and delete Smart Groups for any organization.

For additional information about Smart Groups, see the *HPE DMA User Guide* and the *HPE DMA API Reference WebHelp*.

#### To create a new Smart Group:

1. Go to Environment > Smart Groups.
2. Click **New Group**.
3. Specify the following information for your new Smart Group:
  - Name – a unique name for the Smart Group
  - Role – the role that will be able to view and use this Smart Group
  - Target Level – server, instance, or database
  - Criteria – the criteria that define the Smart Group

You must specify at least one criterion, and you can specify multiple criteria. The criteria will be combined using a logical AND—all criteria must be satisfied in order for the target to be included in the Smart Group.

Information about the specified Target Level object and its parents is available for forming the criteria. For example, if the Target Level is instance, information for organizations and servers is also

available in the drop-down.

4. Click **Save**.

#### To modify an existing Smart Group:

1. Go to Environment > Smart Groups.
2. Select the Smart Group that you want to modify.
3. Make the required modifications.

You can modify the Name, the Role, and the Criteria. You cannot modify the Target Level of an existing Smart Group.

4. Click **Save**.

#### To delete a Smart Group:

1. Go to Environment > Smart Groups.
2. Select the Smart Group that you want to delete.
3. Click the **DELETE** link.
4. Click **Delete** to confirm.

## Policies

Policies are reusable sets of attributes that can be used as parameter values in deployments. Deployments can reference policy attributes to change the automation behavior. Policies provide values for input parameters. They can contain fixed values or reference Custom Fields.

Policies enable HPE DMA to manage groups of hundreds or thousands of servers at a time without the need to configure each individual server.

Policies can have three different types of attributes:

- Text – a simple text value that users can view while deploying and running automation.
- Password – also a simple text value, but the value is masked (obfuscated) when displayed so that users cannot see the value.  
Note that any parameter whose name contains the string “password” is automatically masked throughout the HPE DMA user interface.
- List – a free-form text field that can contain comma-delimited lists of values or other large text data not suitable for a Text type attribute.

For additional information about policies, see the *HPE DMA User Guide* and the *HPE DMA API Reference WebHelp*.

**To create a new policy:**

1. Go to Automation > Policies.
2. Click **New Policy**.
3. Type a unique Name for your policy.
4. In the Attributes area, perform the following actions for each attribute that you want to add:
  - a. Specify a unique name (within this policy).
  - b. From the drop-down list, select this attribute's type: Text, List, or Password.
  - c. Click **Add**.
  - d. Specify the value of the attribute.
5. *Optional:* On the Roles tab, select the Read box for any users or user groups that you want to be able to use this policy to provide parameter values in a deployment. Select the Write box for any users or groups that you want to be able to modify this policy (add or remove attributes).
6. Click **Save**.

**To modify an existing policy:**

1. Go to Automation > Policies.
2. Select the policy that you want to modify.
3. Make the required modifications to the policy.  
 You can modify the Name, Attributes, and Role assignments for any policy that is not locked.  
 Policies that are included in HPE DMA solution packs are locked. You cannot modify a locked policy, but you can make a modifiable copy of that policy.
4. Click **Save**.

**To delete a policy:**

1. Go to Automation > Policies.
2. Select the policy that you want to delete.  
 You cannot delete a policy that is referenced by a deployment.
3. Click the **DELETE** link.
4. Click **Delete** to confirm.

## Discovery

HPE DMA provides special Discovery workflows that you can use to automatically discover instances and databases residing on your managed servers. You can run the Discovery workflows manually, or you can set up scheduled deployments to run them periodically.

For more information, including detailed instructions for using the Discovery workflows, see the *HPE DMA User Guide*.

# Solution Packs

A solution pack is a set of HPE DMA workflows, steps, functions, and policies that address a specific process or problem—such as database provisioning or application server patching. Solution packs are imported into HPE DMA and can be deployed in five to ten minutes. Each solution pack contains the following items:

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

For information about available solution packs, contact your HP Software sales representative.

To use the workflows in a solution pack, you must first import the solution pack into HPE DMA.

**Note:** Only users who have Administrator capability can install, roll back, or delete solution packs.

## Installing a Solution Pack

The HPE DMA solution packs is available as a downloadable link containing a zipped folder. You can download the most recent updates to those solution packs from HP Software Support Online.

**To obtain the most recent HPE DMA patch:**

1. Go to the following web site: <https://softwaresupport.hp.com/>
2. Sign in using your HP Passport credentials.
3. Your dashboard experience is based on your SAID. Under **My Products**, select database and middleware automation.
4. Look under **Software Patch** to determine whether a more recent patch is available.
5. If there is a more recent patch, do the following:
  - a. Click the link for the desired patch.
  - b. Under **Download Information**, click the link to download the patch installation media.

### To access the HPE DMA solution packs:

To access the HPE DMA solution packs, mount the ISO file of the HPE DMA10.40 (or patch) installation media.

The solution packs are located in the following folders:

- The `DMA_10.40.000.000_Server_and_Client` folder contains the Discovery and Promote solution packs.  
The Discovery solution pack is not automatically installed with HPE DMA. You must import it if you want to use the discovery workflows.
- The `DMA_10.40.000.000_Database_Solution_Packs` folder contains all of the database solution packs (provisioning, advanced provisioning, patching, advanced patching, compliance, refresh, and release management).
- The `DMA_10.40.000.000_Middleware_Solution_Packs` folder contains all of the application server solution packs (provisioning, patching, configuration management, and release management).

### To import the solution pack:

1. On the system where you downloaded the installation media, open a web browser, and go to the following URL:

`http://<HPE_DMA_server>/dma/login`

Port 8443 is the default port. You can change this if you prefer to use a different port (for more information, see ["Changing the Default Port and Security Level" on page 39](#)).

2. Log in to the HPE DMA server using an account with Administrator capability.
3. 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.

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

5. Click **Import solution pack**.

The solution pack is imported, and it now appears in the list of Installed Solutions.

**Tip:** To view basic information about the solution pack, hover your mouse over its name in the right pane.

Installed

History

Installed Solutions

✓ Successfully imported HP DMA Discovery Solution Pack

SOLUTION PACKS

HP DMA Discovery Solution Pack

Version 10.30.0

DETAILS

Name:

HP DMA Discovery Solution Pack

Version:

10.30.0

Targets:

25

Installed:

30 Jan, 2015

Description:

Discovers Oracle, Sybase and SQL Server databases on target servers. Also discovers WebSphere and WebLogic middleware applications on target servers. 44929

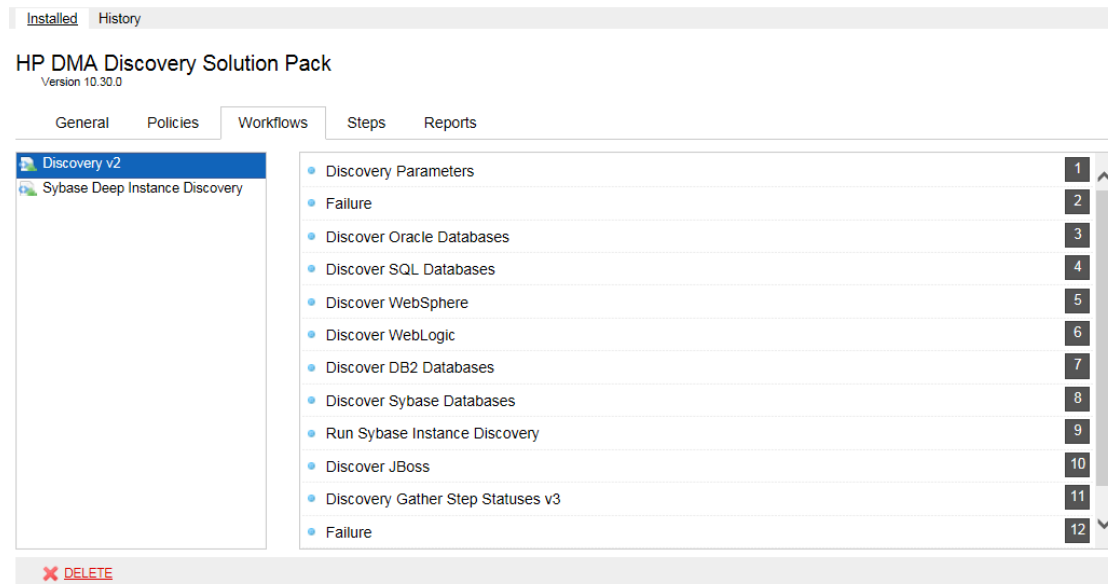
Browse...

Import solution pack

HPE Database and Middleware Automation (10.40)

Page 31 of 82

**Tip:** To view detailed information about the solution pack, click its name in the left pane. The General tab shows you information about the solution pack, including its installation history on this HPE DMA server. The Workflows tab lists the workflows included in this solution pack.



## Versioning and Importing Solution Packs

You may not import a solution pack with a lower version than your currently existing solution pack. To return to a previous solution pack, you must use the Rollback feature (see ["Rolling Back a Solution Pack" on the next page](#)).

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

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

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

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



## Modifying a Solution Item

You may need to modify the automation items included in an installed solution pack to fit your company's needs. Solution packs are fully-supported by HP, but modifications to solution pack contents are supported by the customer who implements the modifications.

It is a best practice to make a copy of any workflow, step, function, or policy that you wish to modify.

### To make a copy of a Solution Pack item:

1. Go to the Solutions > Installed page.
2. Select the solution pack that you want to work with.
3. Select the workflow, step, function, or policy tab.
4. Select the specific workflow, step, function, or policy that you want to modify.
5. Click **Copy**.
6. Specify a unique Name for the copy.
7. Modify the copy to suit your objective.
8. Click **Save**.

## Rolling Back a Solution Pack

You can roll a solution pack back to its previous state after an import or an upgrade. Roll back a solution pack import if you discover that you accidentally overwrote a version of the solution pack that you need or if you encounter any issues with a newly-imported solution pack. The most recently-installed solution pack is removed when you perform a rollback.

For example, if you import version 1, then you import version 2, and then you perform a rollback, all solution pack components are reset to version 1, regardless of any modifications you may have made to version 2.

You can only have one version of a specific solution pack on your system at any given time. If you want to modify an item included in an installed solution pack, you must make a copy of that item and give the copy a unique name (see ["Modifying a Solution Item" above](#)).

Note the following:

- If you roll back a solution pack that has only been imported once, the end result is the same as if you had deleted that solution pack. For example, if you initially import version 3, and then perform a rollback, HPE DMA removes version 3, because there is not another previously-existing version to which you can roll back.
- If you roll back a solution pack whose version is the only version installed on your system, the History list will display a "Remove" as the Operation.
- If an upgrade was performed on a solution pack after another solution pack was deleted, the rollback ignores the removed solution pack in the rollback sequence. Similarly, if the last action was to delete a solution pack, the rollback ignores the removed solution pack in the rollback sequence.

The rollback operation simply "undoes" the most recent solution pack import operation performed. It does not enable you to roll back a to a specific solution pack version.

**Note:** Functions are not rolled back when the solution packs that installed them are rolled back.

#### To roll back a solution pack:

1. Go to the Solutions > History page.
2. Click the ROLLBACK link in the lower left corner.

If a previous version of the solution pack is available, the following type of message appears:

DOWNGRADE HP DMA DISCOVERY SOLUTION PACK TO V10.01?

If no previous version of the solution pack is available, the following type of message appears:

UNINSTALL HP DMA DISCOVERY SOLUTION PACK V10.10?

3. Click **Rollback** to confirm the rollback.

## Deleting a Solution Pack

You can delete any solution pack that was previously installed. When you delete a solution pack, no attempt is made to restore any previous version of that solution pack.

If a component is shared with another solution pack that you are removing, once you remove the solution pack, that shared component remains in the system.

**Note:** Functions are not deleted when the solution packs that installed them are deleted.

#### To delete a specific solution pack:

1. Go to the Solutions > Installed Page.
2. Select the solution pack that you want to delete.
3. Click the DELETE link in the lower left corner. The following type of message appears:

ARE YOU SURE?

4. Click **Delete** to confirm the delete.

Deleting a Solution pack or performing a rollback both display as a Remove operation on the History page.

After you delete a solution pack, it is not available to use. If you later decide to install that solution pack again—either the same or a different version—the history of that solution pack is maintained, but you cannot roll back to the an earlier version.

#### Related Topics:

["Configuring the Connector" on page 15](#)

["Configuring SSL on the HPE DMA Server" on page 9](#)

["Solution Packs" on page 30](#)

["Configuring Email Settings" on the next page](#)

# Configuring Email Settings

The mail settings are used to send outgoing email messages when an email step is executed in a Workflow. There are two mail settings:

- **Server**—the SMTP Server that sends outgoing emails messages
- **Sender**—the “From” address, which is customizable to avoid possible issues with spam blockers

## To configure the mail settings:

1. Go to Setup > Configuration.
2. Click the Mail tab.
3. Specify the Server and Sender for your environment.
4. To test the settings, click the **Test** button, enter your email address, and click **OK**.  
If the settings are valid, you will receive an email message from the Sender specified.
5. Click **Save**.


# Hiding and Unhiding Workflows

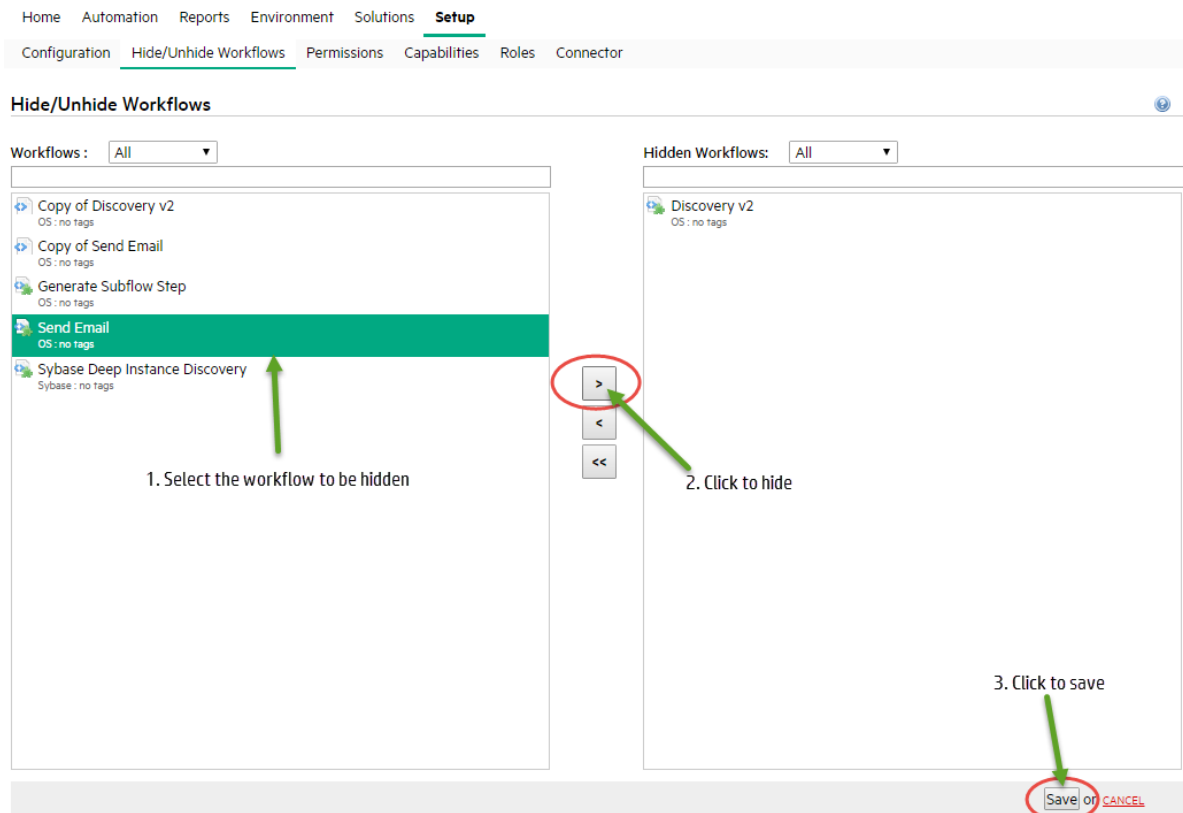
You can hide workflows, for example, deprecated workflows, from appearing in the DMA server user interface. These workflows will not be removed from the server. Any reference to hidden workflow in the server, will have the "HIDDEN" tag prefixed in the workflow name.

If a workflow with existing deployments is hidden, those deployments will not be hidden. These deployments can be modified and saved, but cannot be copied.

If a workflow is hidden, any deployment for hidden workflows cannot be created through DMA APIs.

## To hide a workflow as an administrator:

1. Login to DMA as admin or user with administrator privileges, if already not logged in.
2. Go to **Setup > Hide/Unhide Workflows** tab.
3. Filter the workflows by name or by the type of workflows under the Workflows box.
4. Select the workflow to be hidden from the Workflows list and click the hide icon  to hide the workflow.



5. Click **Save**.
6. Confirm **Yes** at the prompt to hide the selected workflow.
7. Repeat steps 3 through 6 to hide the required workflows.

**To hide a workflow as a workflow creator or administrator:**

1. Login to DMA, if already not logged in.
2. Go to **Automation > Workflows**.
3. Filter the workflows by name or by the type of workflows.
4. Click the workflow to be hidden. The selected workflow will be displayed.
5. Click **Hide** link at the bottom of the screen.

Home **Automation** Reports Environment Solutions Setup

Workflows Steps Functions Policies Deployments Run Console History

### Copy of Send Email

Documentation Workflow History Deployments Roles

Name: Copy of Send Email

Tags:

Type: OS

Target level: Server

Documentation:

**Usage instructions**

Detailed information on how this workflow operates.

**Dependencies**

List any system libraries or binaries that this workflow needs installed. Special privileges the user needs (ie. root, sudo) can also be listed here.

**Results verification**

List any steps that can be performed to check the outcome of the workflow.

**Notification plan**

Define who should be notified when the workflow succeeds and fails.

1. Click to hide


2. Click to save

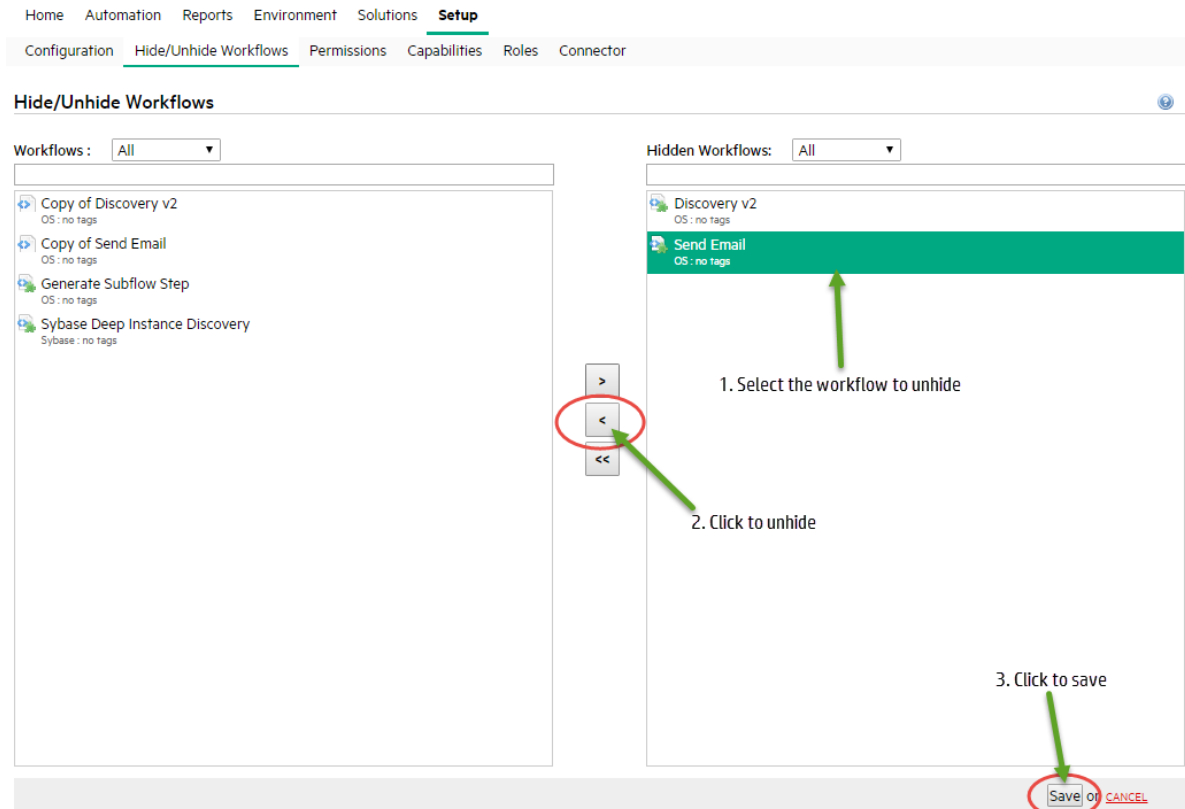
HELP EDIT

DELETE HIDE EXPORT EXTRACT POLICY DEPLOY RUN Copy Save CANCEL

6. Click **Save**.
7. Confirm **Yes** at the prompt to hide the selected workflow.
8. Repeat steps 3 through 7 to hide the required workflows.

#### To unhide a workflow:

1. Login to DMA as administrator or user with administrator privileges, if already not logged in.
2. Go to **Setup > Hide/Unhide Workflows** tab.
3. Filter the workflows by the name or by the type of workflows under the Hidden Workflows box.
4. Select the workflow to be hidden from the Workflows list and click the hide icon  to unhide the workflow.



5. Click **Save**.
6. Confirm **Yes** at the prompt to unhide the selected workflow.
7. Repeat steps 3 through 6 to unhide the required workflows.

# Changing the Default Port and Security Level

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

## To change the HPE DMA port:

1. Stop HPE DMA:

```
# service dma stop
```

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

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

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

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

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

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

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

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

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

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

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

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

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

8. Start HPE DMA:

```
# service dma start
```

# Using a Proxy Server

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

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

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

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

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

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

For additional information, see "[Configuring SSL on the HPE 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.

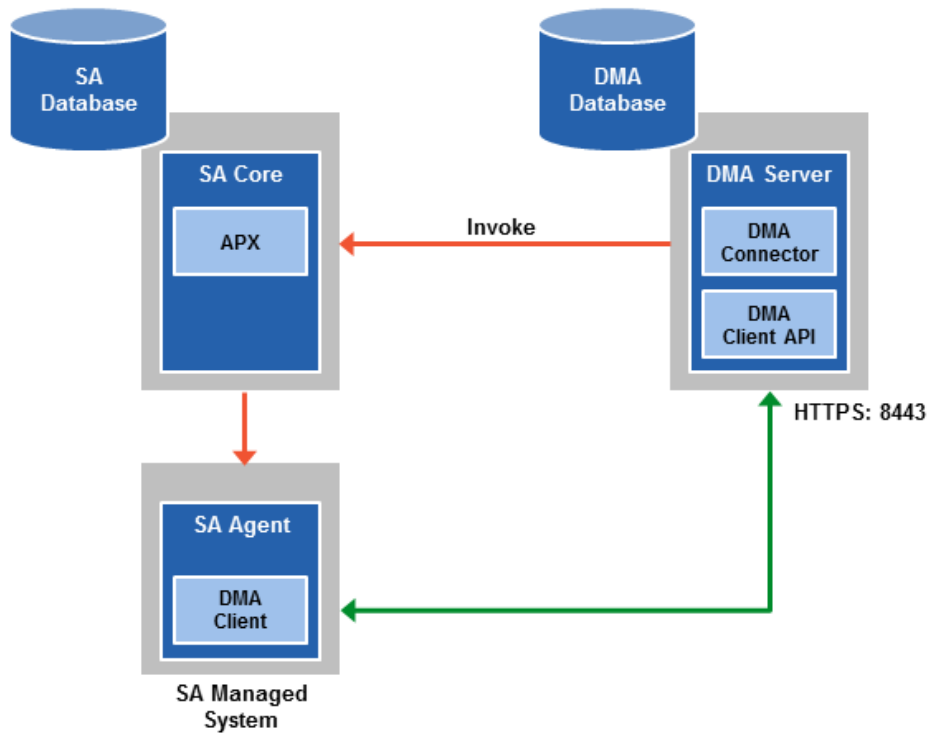
For more information, see *Using SA Gateway Network as a Proxy Network* document available on the HP Software Support web site: <https://softwaresupport.hp.com/>



## Default HPE DMA Communications

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

1. HPE 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.

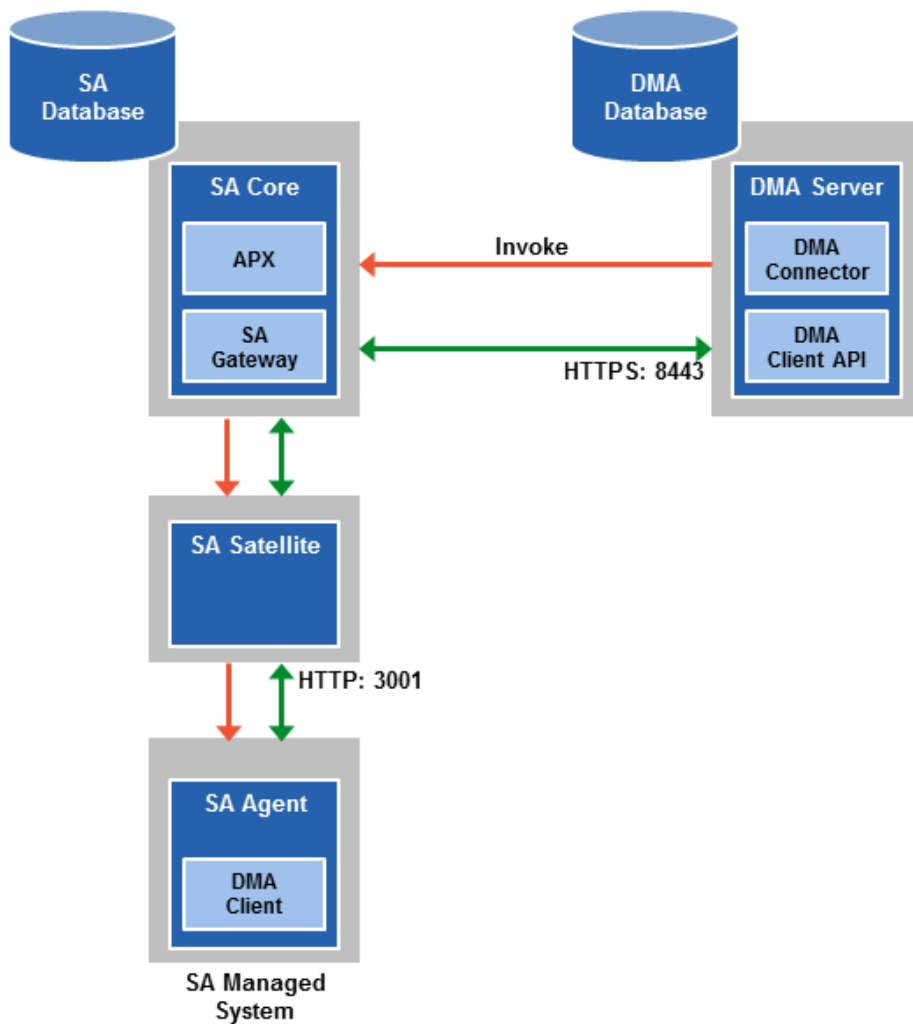


## Using an SA Satellite as a Proxy Server

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

1. HPE SA 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 HPE DMA Manages Proxy Communication

HPE 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 HPE 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 HPE DMA will communicate if `west_proxy_in_use` has values at both the organization level and the server level.

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

# Setting Up a Proxy Server

To set up a proxy server for HPE DMA, make the following changes to the HPE 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 HPE DMA to route traffic through the proxy server. This procedure is performed in the HPE DMA UI.

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

<https://softwaresupport.hp.com/>

## Configuring 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 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:<DMA Server>:<DMA Port>:*:*
```

Here `<DMA Server>` is the resolvable host name of your DMA Server and `<DMA Port>` 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.

## Specifying 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 HPE 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 HPE DMA server in the `webServiceUrl` parameter.

**Note:** To specify the SA realm while the HPE 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 HPE DMA server is connected to.

4. Specify the IP address of your HPE 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

## Creating and Configuring the HPE DMA Custom Fields

In the HPE 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 HPE 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 <a href="#">NEW CUSTOM FIELD</a>		
<code>west_proxy_address:</code> <input type="text" value="http://proxy.mycompany.com:3001"/>		
<code>west_proxy_in_use:</code> <input type="text" value="TRUE"/>		

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

### My Organization

Properties	Custom Fields	Roles
Custom fields <a href="#">NEW CUSTOM FIELD</a>		
<code>west_proxy_address:</code> <input type="text" value="SA_auto_select"/>		
<code>west_proxy_in_use:</code> <input type="text" value="TRUE"/>		

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

## Permission Settings

This section describes the permission settings to manage DMA (see [Roles, Capabilities, and Permissions](#)).

**Note:** Most SA administrative settings—including those that determine which users and groups can access which SA managed servers—are managed by the HP SA administrator outside of HPE DMA. For more information, refer to the *SA Administration Guide*.

HPE DMA provides finely grained role-based access so that you can carefully control the specific capabilities that individual users and user groups have within HPE DMA.

The following procedure shows you how to set the role-based access permissions. An overview is provided in [Roles, Capabilities, and Permissions](#).

**To grant access permissions to a user or user group:**

1. Go to Setup > Permissions.
2. Select the user or user group to whom you want to grant permissions.
3. Go to one of the tabs:

- Deployments
- Workflows
- Steps
- Policies
- Organizations

4. Select the pertinent boxes to grant Read, Write, Execute (applicable only to Deployments), and/or Deploy (applicable only to Organizations) permission to the selected user or group.

You can use the **ALL** links (for example, **READ ALL** or **WRITE ALL**) below the permissions box to grant the pertinent permission to all users and groups.

If an item has a “—” in one of the columns instead of a check box, that means that this permission is not applicable to that item. For example, you cannot grant Write permission to a read-only Step or Workflow.

5. Click **Save**.

**To grant a user or group permission to access a specific workflow:**

1. Go to Automation > Workflows.
2. From the list of available workflows, select the workflow that you want to work with.
3. Go to the Roles tab.
4. In the table, do the following things:
  - Select Read for user roles that you want to be able to view this workflow.
  - Select Write for user roles that you want to be able to modify the workflow.
5. Click the **Save** button in the lower right corner.

**Note:** Users with Administrator capability can set permissions for all workflows, deployments, steps, policies, and organizations from the Setup > Permissions page.



# Specifying 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 HPE DMA Automation Platform Extension (APX) to allow non-default Windows Administrator user names. See <a href="#">"Updating the HPE DMA APX"</a> .	On one SA Slice server	Only once
Create and configure a new HPE DMA Custom Field that will be used to specify the Windows Administrator user name at either the organization or server level. See <a href="#">"Creating and Configuring the HPE DMA Custom Field"</a> .	In HPE 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 *
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		

# Updating the HPE 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.
- OGSHP 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 Server Automation documentation library, which is available on the HPE Software Support web site:

<https://softwaresupport.hp.com/>

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.

## Creating and Configuring the HPE DMA Custom Field

The final change required is to create and configure an HPE 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, HPE 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 HPE 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 HPE DMA to run workflows on Windows targets as a specific Windows domain user, also see ["Running Workflows as a Windows Domain User" on the next page](#).

# Running Workflows 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 HPE DMA to discover information about the target environment.
- Enable the Secondary Logon Windows Service on the target windows server when the custom field **domain\_username\_win** is configured.

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

- ["Configuring Windows Domain User Using Custom Fields"](#)
- ["Configuring the Windows Domain User Using Runtime Parameters"](#)

## Configuring 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, HPE DMA will use the server value.

- 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 HPE 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 ["Specifying a Renamed Windows Administrator User" on page 49](#).

## Configuring the 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 HPE DMA.

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

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

- 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

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

- 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

- When you create a deployment from the copy of the workflow, set the parameter types to **Runtime Value**.
- 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 ["Specifying a Renamed Windows Administrator User" on page 49](#).

# Changing the Number of Active Connections

This topic shows you how to change the number of active database connections that HPE 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 HPE 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 HPE DMA server again:  

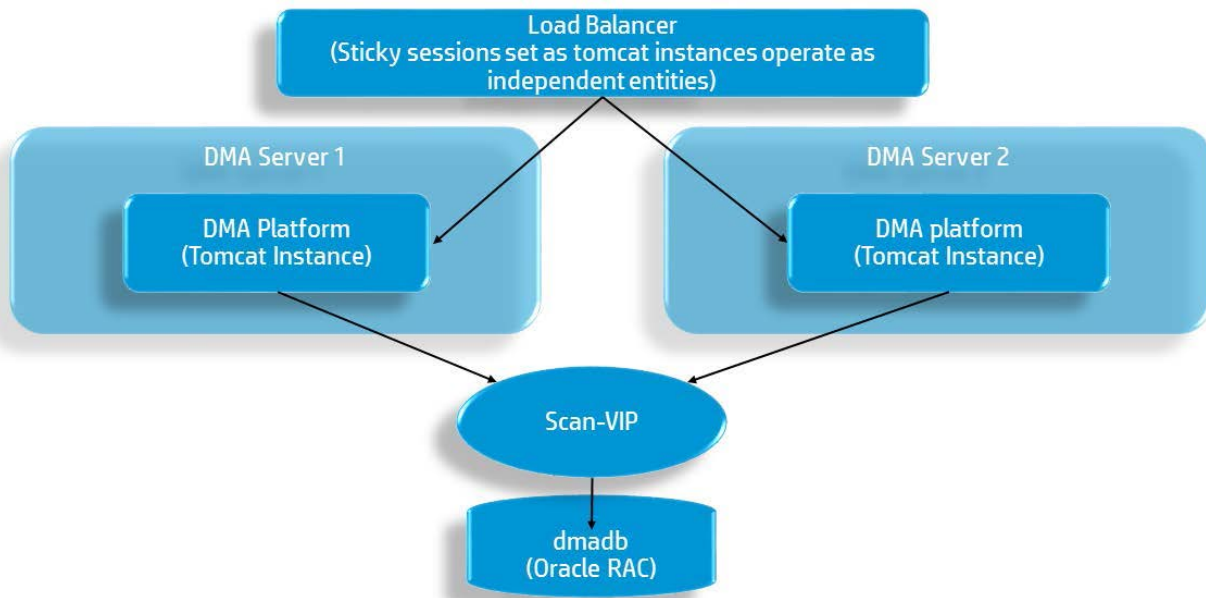
```
$ service dma start
```

## Configuring HADR using Oracle Database

This section provides examples of how to configure High Availability (HA) and Disaster Recover (DR) solutions with HP Database and Middleware Automation (HPE DMA).

### HPE DMA HA Standard Architecture Solution

This example is for HA architecture without DR:



### Running the Baseline command on Oracle RAC

To set up the Primary active environment, use these examples to modify the HPE DMA installation Baseline command:

1. Change your directory:  
`cd /opt/hp/dma/server/tomcat/webapps/dma/WEB-INF`
2. Run the Baseline command on the Primary node of Oracle RAC (as one line), for example:  
`sh dmaBaselineData.sh -cc -c -dbu dma -dbpw dma -dbp 1521 -dbs dmadb  
 -dbh dma-rac1.company.com -dmah dma-rac1.company.com  
 -jdbccs jdbc:oracle:thin:@scan-vip.company.com:1522/dmadb.servicename`
3. Run the Baseline command on all other nodes of Oracle RAC cluster (as one line), for example:  
`sh dmaBaselineData.sh -cc -dbu dma -dbpw dma -dbp 1521 -dbs dmadb  
 -dbh dma-rac(2/3/4...).company.com -dmah dma-rac(2/3/4...).company.com  
 -jdbccs jdbc:oracle:thin:@scan-vip.company.com:1522/dmadb.servicename`

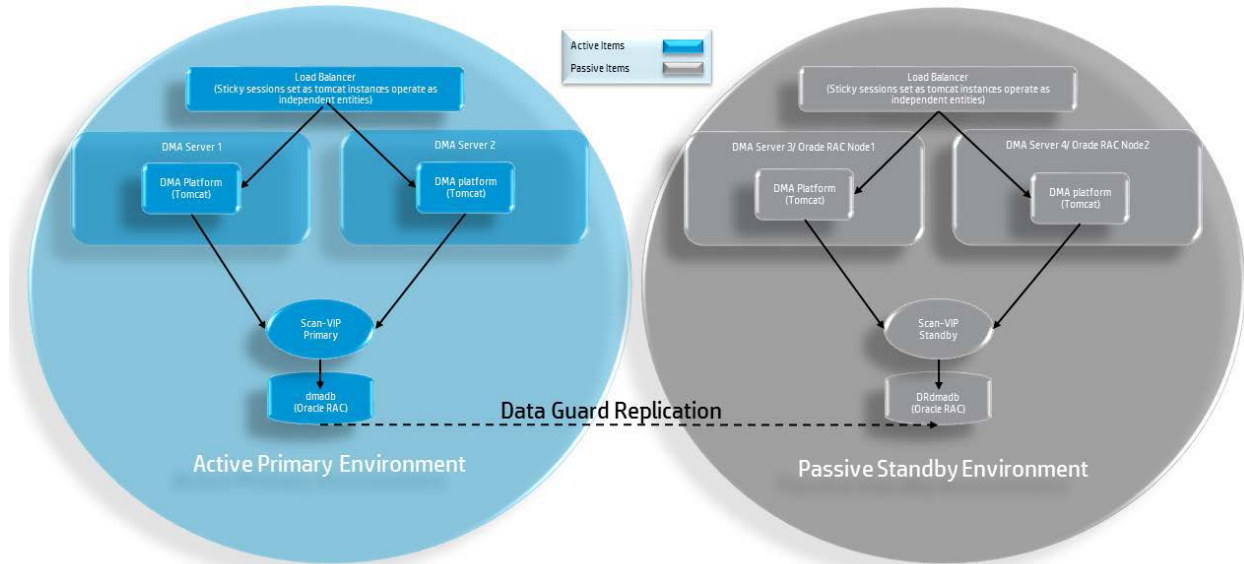
If desired, continue by following the instructions in either of these sections:

- HPE DMA HA and DR Architecture Solution (Active-Passive)
- HPE DMA HA and DR Architecture Solution (Active-Active Tomcat and Active-Passive Database)

## HPE DMA HA and DR Architecture Solution (Active-Passive)

This example is for HA architecture with DR (active-passive).





### Setting up the HPE DMA Server on the Standby Environment

After you have set up your primary active environment (see HPE DMA HA Standard Architecture Solution), perform these steps in the Passive Standby Environment (right side of the diagram) to set up the Active-Passive architecture:

**Note:** Do this after you run Baseline commands to set up your Primary active environment. You only need to modify the dma.xml files for the Standby environment.

1. Copy the dma.xml file from Primary node from Primary environment to the Standby nodes. The file is located here:  
`/opt/hp/dma/server/tomcat/conf/Catalina/localhost/dma.xml`
2. On each node, edit the webServiceUrl parameter and the jdbc/dma resource in the dma.xml file to match the Standby environment, for example:  

```
<Parameter name="com.hp.dma.core.webServiceUrl" value="https://dmaserver
(3/4):8443/dma" />
<Resource name="jdbc/dma" auth="container" type="javax.sql.DataSource"
maxActive="20" maxIdle="20" maxWait="20000" username="dma" password="{AES}
80c54c58279cb66cb879d432cd33be4fc53bc95a30d510dffdb55fd121be4d44"
driverClassName="oracle.jdbc.OracleDriver" url="jdbc:oracle:thin:@scan-standby-
vip.company.com:1522/DRmadb.servicename"
factory="com.hp.dma.util.DmaTomcatContextHandler" />
```

### Handling a Failover for an Active Standby Environment

In the event of a failover:

1. Cancel the workflows that were running when the failure occurred by running the following script on any of the Standby HPE DMA servers:

```
/opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/cancelWorkflow.sh
```

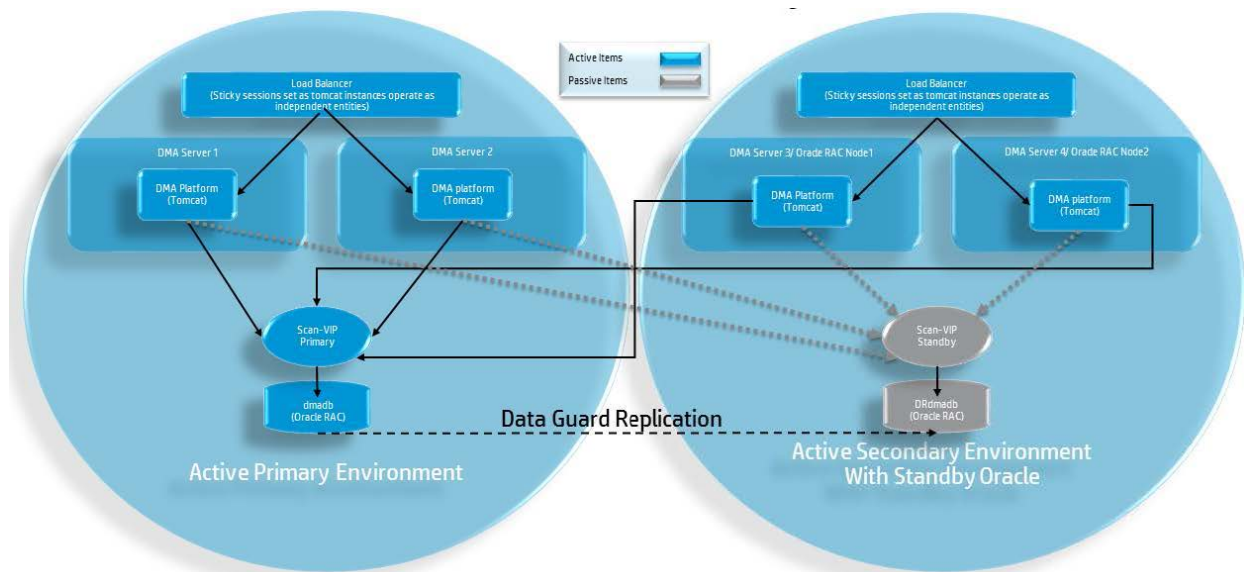
**Note:** The cancelWorkflow script will identify the workflows that need to be canceled.

2. Clean up any targets that may have had workflows running against them.

3. Restart the HPE DMA Service by running the following command on all Standby HPE DMA Servers:  
`service dma restart`
4. Change the SA slice or gateway of the Standby environment:
  - a. Log in to the HPE DMA user interface
  - b. Navigate to Setup > Connector
  - c. Specify the required connector information

## HPE DMA HA and DR Architecture Solution (Active-Active Tomcat and Active-Passive Database)

This example is for HA architecture with DR (Active-Active Tomcat and Active-Passive database).



### Setting up the HPE DMA Server on the Standby Environment

After you have set up your primary active environment (see HPE DMA HA Standard Architecture Solution), perform these steps in the Active Secondary Environment with Standby Oracle (right side of the diagram) to set up the Active-Active Tomcat and Active-Passive database architecture:

**Note:** Do this after you run Baseline commands to set up your Primary active environment. You only need to modify the dma.xml files.

1. Copy the dma.xml file from Primary node from Primary environment to the Standby nodes. The file is located here:  
`/opt/hp/dma/server/tomcat/conf/Catalina/localhost/dma.xml`
2. On each node, edit the webServiceUrl parameter in the dma.xml file to match the Standby environment, for example:  

```
<Parameter name="com.hp.dma.core.webServiceUrl" value="https://dmaserver
(3/4):8443/dma" />
```

### Handling a Failover when the Primary Database is Lost

If the primary DB is lost, perform a Failover Operations Active-Active:

1. Execute the Oracle Failover operation to change Standby to Primary Database.
2. Cancel the workflows that were running when the failure occurred by running the following script on any of the Standby HPE DMA servers:

```
/opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/cancelWorkflow.sh
```

**Note:** The cancelWorkflow script will identify the workflows that need to be canceled.

3. Clean up any targets that had workflows running against them.
4. On all HPE DMA Servers, edit the jdbc/dma resource in the dma.xml file, for example:
 

```
<Resource name="jdbc/dma" auth="container" type="javax.sql.DataSource"
maxActive="20" maxIdle="20" maxWait="20000" username="dma" password="{AES}
80c54c58279cb66cb879d432cd33be4fc53bc95a30d510dffdb55fd121be4d44"
driverClassName="oracle.jdbc.OracleDriver" url="jdbc:oracle:thin:@scan-standby-
vip.company.com:1522/DRdadb.servicename"
factory="com.hp.dma.util.DmaTomcatContextHandler" />
```
5. Restart the HPE DMA Service by running the following command on all HPE DMA Servers:
 

```
service dma restart
```

## Additional Resources

### HPE DMA Documentation

The HPE DMA Installation Guide contains complete instructions for installing HPE DMA and additional information about the Baseline command and the dma.xml file. It is available on the HP Software Product Manuals web site: <http://h20230.www2.hp.com/selfsolve/manuals>

## HPE DMA Baseline Options

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

Option	Example Argument Value	Description
-?, --help		Print this usage message.
-c, --create-tables		Create tables for database.
-cc, --create-context		Create a context file with the specified settings.
-context, --deployed-context-file <dma.xml>	dma.xml	Fully qualified path to the deployed context file to get database connection settings.
-dbh, --database-hostname <arg>	oracle.mycompany.com	The database host name for the Java Database Connectivity (JDBC) connection.
-dbp, --database-port <arg>	1521	The database port for the Java Database Connectivity (JDBC) connection.
-dbpw, --database-password <dbpasswordValue>	dbpassword	The password used to connect to the database.
-dbs, --database-sid <arg>	dma	The database SID for the Java Database Connectivity (JDBC) connection.

-dbts,--database-tablespace <arg>	/u01/app/oracle/ oradata/dma	The base directory for the database tablespace creation.
-dbtype,--database-type <arg>	oracle	(optional) The underlying database type. The default is oracle.
-dbu,--database-username <dbusernameValue>		The username used to connect to the database.
-dmah,--dma-hostname <dmahostnameValue>	dma.mycompany.com	Set the fully qualified host name of the HPE DMA server.  Note: If this value is not specified, the default is the server where the script is running.
-e,--erase		Erase existing data and add baseline data.  Caution: Do not do this unless instructed to by HP Support.

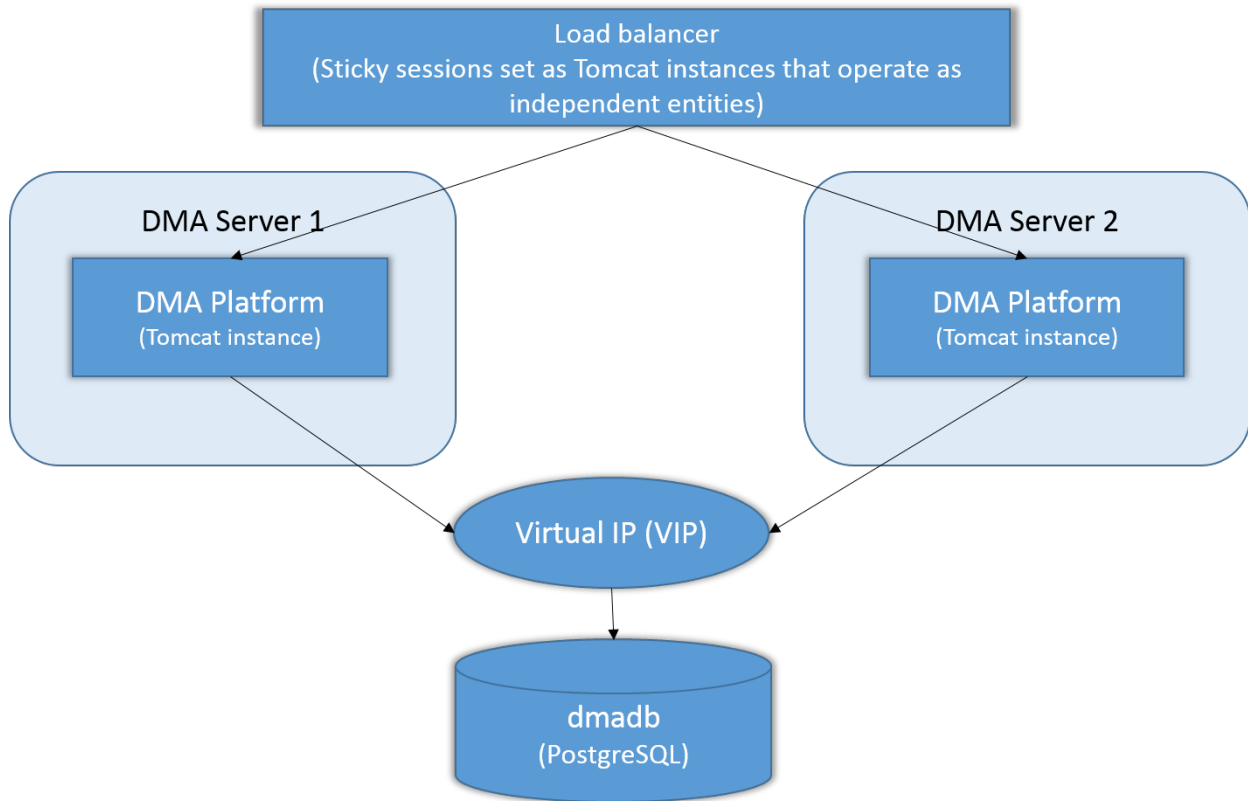
## Configuring HADR using PostgreSQL Database

This section includes the following topics:

- ["HPE DMA HA Standard Architecture Solution" below](#)
- ["HPE DMA HA and DR Architecture Solution \(Active-Passive\)" on the next page](#)
- ["HPE DMA HA and DR Architecture Solution \(Active-Active Tomcat and Active-Passive Database\)" on page 63](#)

## HPE DMA HA Standard Architecture Solution

This example is for HA architecture without DR:



## How to Run the Baseline Command on PostgreSQL

To set up the primary active environment, use these examples to modify the HPE DMA installation baseline command. How to use the baseline command is described in “Install the HPE DMA Server” section in the HPE DMA Installation Guide available at <http://h20230.www2.hp.com/selfsolve/manuals>. To see the full list of baseline options, see [HPE DMA Baseline Options](#).

1. Change your directory:

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

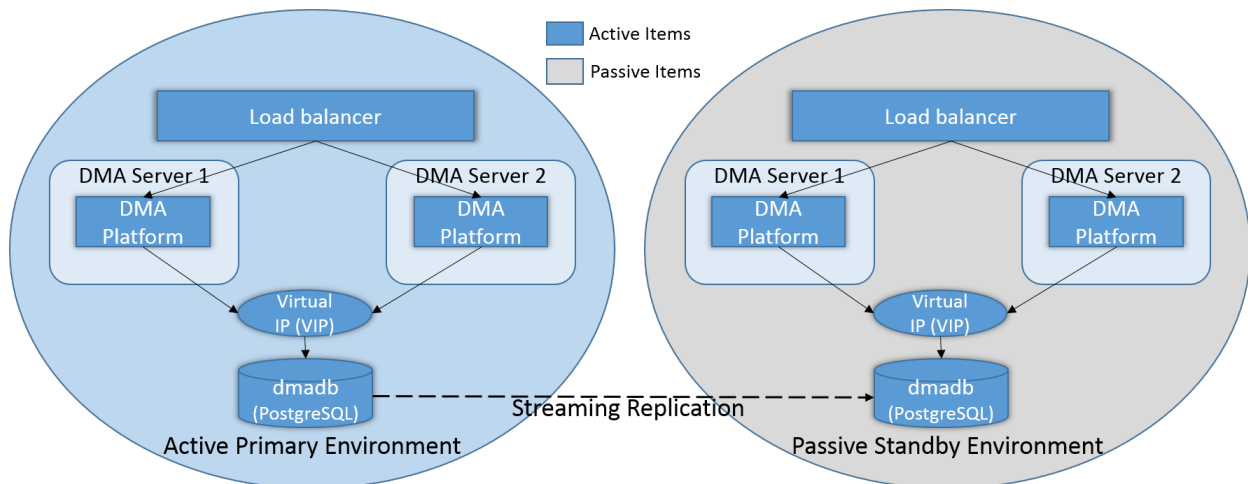
2. Run the baseline command on the primary node of PostgreSQL:

```
sh dmaBaselineData.sh --create-tables --database-type postgres --database-username postgres --database-password postgres --jdbc-connection-string jdbc:postgresql://<ipaddress>:5432/dma --dma-hostname <ipaddress>
```

The standby nodes are automatically synced as streaming replication continuously ships and applies Write-Ahead Logging (WAL) XLOG records.

## HPE DMA HA and DR Architecture Solution (Active-Passive)

This example is for HA architecture with DR (active-passive).



## How to Setup the HPE DMA Server on the Passive Standby Environment

After you have set up your primary active environment, perform these steps in the passive standby environment (right side of the diagram) to set up the active-passive architecture:

**Note:** Perform this after you run baseline commands to set up your primary active environment. You only need to modify the `dma.xml` files for the standby environment. For more information on the `dma.xml` file, see HPE DMA Installation Guide available at <http://h20230.www2.hp.com/selfsolve/manuals>.

1. Copy the `dma.xml` file from primary node from primary environment to the standby nodes. The file is located at:  
`/opt/hp/dma/server/tomcat/conf/Catalina/localhost/dma.xml`
2. On each node, edit the `webServiceUrl` parameter and the JDBC/DMA resource in the `dma.xml` file to match the Standby environment, for example, as highlighted in **bold**:

```
<Parameter name="com.hp.dma.core.webServiceUrl" value="https://dmaserver
(3/4):8443/dma"/>
<Resource name="jdbc/dma" auth="container" type="javax.sql.DataSource" maxActive="20"
maxIdle="20" maxWait="20000" username="dma" password="{AES}
80c54c58279cb66cb879d432cd33be4fc53bc95a30d510dffdb55fd121be4d44"
driverClassName="postgres.jdbc.PostgreSQLDriver" url="jdbc:postgresql:thin:@standby-
vip.company.com:1522/DRdmadb.servicename"
factory="com.hp.dma.util.DmaTomcatContextHandler"/>
```

## How to Handle Failover for an Active Standby Environment

In the event of a failover, perform the following:

1. Cancel the workflows that were running when the failure occurred by running the following script on any of the Standby HPE DMA servers:

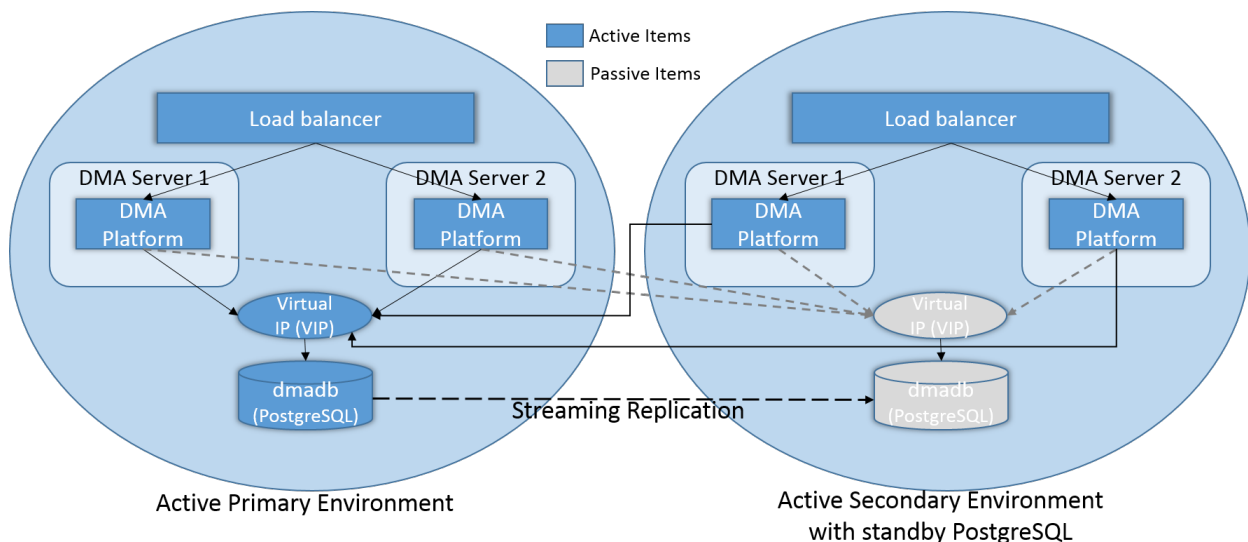
```
/opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/cancelWorkflow.sh
```

2. Clean up any targets that may have had workflows running against them.
3. Change the values for the following parameters in the dma.xml file:
  - testOnBorrow="true"
  - removeAbandoned="true"
  - timeBetweenEvictionRunsMillis="5000"
  - minEvictableIdleTimeMillis="5000"
  - minIdle="0"

The application attempts to reconnect to the datasource after restart of the database.

## HPE DMA HA and DR Architecture Solution (Active-Active Tomcat and Active-Passive Database)

This example is for HA architecture with DR (Active-Active Tomcat and Active-Passive database).



## How to Setup the HPE DMA Server on the Active Standby Environment

After you have set up your primary active environment, perform these steps in the active secondary environment with standby PostgreSQL to set up the Active-Active Tomcat and Active-Passive database architecture:

**Note:** Perform this after you run baseline commands to set up your primary active environment. You only need to modify the `dma.xml` files for the standby environment. For more information on the `dma.xml` file, see HPE DMA Installation Guide available at <http://h20230.www2.hp.com/selfsolve/manuals>.

1. Copy the `dma.xml` file from primary node from primary environment to the standby nodes. The file is located at:

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

2. On each node, edit the `webServiceUrl` parameter in the `dma.xml` file to match the standby environment:  
`<Parameter name="com.hp.dma.core.webServiceUrl" value="https://dmaserver(3/4):8443/dma" />`

## How to Configure Failover when the Primary Database is Lost

If the primary database is lost, perform a failover operation:

1. Promote the Standby database as the Active database by triggering `recovery.conf` file:
2. Cancel the workflows that were running when the failure occurred by running the following script on the Standby HPE DMA server:

```
/opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/cancelWorkflow.sh
```

3. Change the values for the following parameters in the `dma.xml` file:
  - `testOnBorrow="true"`
  - `removeAbandoned="true"`
  - `timeBetweenEvictionRunsMillis="5000"`
  - `minEvictableIdleTimeMillis="5000"`
  - `minIdle="0"`

The application attempts to reconnect to the datasource after restart of the database.

## Replicating Data

To help HP Database and Middleware Automation (HPE DMA) extend across broader geographical regions, you can build multiple HPE DMA servers and use Oracle Streams replication between those servers. This ensures that your HPE DMA solution packs, policies, and deployments – all HPE DMA automation items except your scheduler – are identical between the servers.

There are many ways to achieve Oracle replication. This section shows you two examples of setting up Oracle Streams using the Data Pump method of moving data. The first example uses two active HPE DMA databases, where replication must function in both directions. The second example assumes that the replicated database will only be used for read operations and to serve as a standby database for disaster recovery purposes.

### Example 1 - Both databases are active

In this example, both the source and destination databases are active, and replication must function in both directions.

#### Prerequisites

- Both databases have archive logging enabled.
- The Oracle Streams initiation parameters are set as follows:



- STREAMS\_POOL\_SIZE is set to 100M (if you are not using Automatic Memory Management or Automatic Shared Memory Management)
- SESSIONS and PROCESSES are increased by 50
- GLOBAL\_NAMES is set to true
- UNDO\_RETENTION is set to 3600
- The database links in the strmadmin schema for both databases are set up such that the source and destination databases connect to each other using the strmadmin login.
- The source database is already set up and is running as the HPE DMA server.
- The schema for the HPE DMA tables in the destination database has been built and is ready for tables to be imported.

### Step 1: Set up the streams administrator account to manage streams

Run these commands on both the source and destination databases – note that these are examples and should be changed to match your environment:

```
CREATE TABLESPACE streams_tbs DATAFILE '/u01/app/oradata/orcl/streams_tbs.dbf' SIZE
25M REUSE AUTOEXTEND ON MAXSIZE UNLIMITED;

CREATE USER strmadmin IDENTIFIED BY password DEFAULT TABLESPACE streams_tbs QUOTA
UNLIMITED ON streams_tbs;

GRANT DBA TO strmadmin;

BEGIN

DBMS_STREAMS_AUTH.GRANT_ADMIN_PRIVILEGE(

grantee => 'strmadmin',

grant_privileges => TRUE);

END;

/

CREATE DIRECTORY strmadmin.streams_dir AS '/u01/app/oracle/admin/streams'
```

### Step 2: Run this PL/SQL code

Run the following anonymous block of code from a SQLPLUS session connected as strmadmin on the source database. Replace the names of the source and destination servers, and modify the directory names, if necessary, for your environment.

```
DECLARE

tables DBMS_UTILITY.UNCL_ARRAY;

tab_count number := 1;

src_dir varchar(30) := ' strmadmin.streams_dir ';

dest_dir varchar(30) := ' strmadmin.streams_dir ';
```

```

src_db varchar(30) := 'dma.src';
dest_db varchar(30) := 'dma.dest';
cursor tables_cur is
select owner || '.' || table_name as table_name from dba_tables where table_name like
'DMA%'
and table_name not like '%QRTZ%';
BEGIN
for i in tables_cur
loop
tables(tab_count) := i.table_name;
execute immediate('alter table ' || i.table_name || ' add supplemental log data (all)
columns')
tab_count := tab_count + 1;
end loop;
dbms_streams_adm.maintain_tables(
table_names      => tables,
source_directory_object      => src_dir,
destination_directory_object => dest_dir,
source_database   => src_db,
destination_database   => dest_db,
capture_name      => 'capture_dma',
capture_queue_table      => 'streams_queue_qt_dma',
capture_queue_name      => 'streams_queue_dma',
apply_name        => 'apply_dma',
apply_queue_table  => 'streams_queue_qt_dma',
apply_queue_name   => 'streams_queue_dma',
bi_directional    => TRUE,
instantiation      => DBMS_STREAMS_ADM.INSTANTIATION_TABLE);
end;
/

```

### Step 3: Track progress

The block of code in Step 2 will take some time to complete, and the time will vary depending on the systems you are using. To track progress, run this query on the Destination database to see how many rules have been set up in Oracle Streams:

```
select count(*) from DBA_STREAMS_TABLE_RULES where table_name like 'DMA%';
```

When the code is complete, the count should be 264 rules.

#### Step 4: Initialize the quartz tables on the destination database

After you have configured Oracle Streams, you must connect to the destination database as the HPE DMA user that you have configured and run the following script to initialize the quartz tables that handle scheduling for HPE DMA.

```
@/opt/hp/dma/server/db_sql/dma-oracle/hpdma_schema-qrtz.sql
```

## Example 2 - Second database is only for reading

In this example, the destination database is used only for read operations and as a standby for disaster recovery purposes.

#### Prerequisites

- The source database has archive logging enabled.
- The Oracle Streams initiation parameters are set as follows:
  - STREAMS\_POOL\_SIZE is set to 100M (if you are not using Automatic Memory Management or Automatic Shared Memory Management)
  - SESSIONS and PROCESSES are increased by 50
  - GLOBAL\_NAMES is set to true
  - UNDO\_RETENTION is set to 3600
- The database links in the strmadmin schema for the source database are set up such that the source database connects to the destination database using strmadmin.
- The source database is already set up and is running as the HPE DMA server.
- The schema for the HPE DMA tables in the destination database has been built and is ready for tables to be imported.

#### Step 1: Set up the streams administrator account to manage streams

NOTE: Run these commands on both the source and destination databases.

```
CREATE TABLESPACE streams_tbs DATAFILE '/u01/app/oradata/orcl /streams_tbs.dbf' SIZE
25M REUSE AUTOEXTEND ON MAXSIZE UNLIMITED;

CREATE USER strmadmin IDENTIFIED BY password DEFAULT TABLESPACE streams_tbs QUOTA
UNLIMITED ON streams_tbs;

GRANT DBA TO strmadmin;

BEGIN

DBMS_STREAMS_AUTH.GRANT_ADMIN_PRIVILEGE(
```

```

grantee => 'strmadmin',
grant_privileges => TRUE);

END;

/

CREATE DIRECTORY strmadmin.streams_dir AS '/u01/app/oracle/admin/streams';

```

## Step 2: Run this PL/SQL code

Run the following anonymous block of code from a SQLPLUS session connected as strmadmin on the source database. Replace the names of the source and destination servers, and modify the directory names, if necessary, for your environment.

```

DECLARE
tables DBMS_UTILITY.UNCL_ARRAY;
tab_count number := 1;
src_dir varchar(30) := ' strmadmin.streams_dir ';
dest_dir varchar(30) := ' strmadmin.streams_dir ';
src_db varchar(30) := 'dma.src';
dest_db varchar(30) := 'dma.dest';
cursor tables_cur is
select owner || '.' || table_name as table_name from dba_tables where table_name like 'DMA%';
BEGIN
for i in tables_cur
loop
tables(tab_count) := i.table_name;
execute immediate('alter table ' || i.table_name || ' add supplemental log data (all)
columns')
tab_count := tab_count + 1;
end loop;
dbms_streams_adm.maintain_tables(
table_names => tables,
source_directory_object => src_dir,
destination_directory_object => dest_dir,
source_database => src_db,
destination_database => dest_db,

```

```

capture_name => 'capture_dma',
capture_queue_table => 'streams_queue_qt_dma',
capture_queue_name => 'streams_queue_dma',
apply_name => 'apply_dma',
apply_queue_table => 'streams_queue_qt_dma',
apply_queue_name => 'streams_queue_dma',
bi_directional => FALSE,
instantiation => DBMS_STREAMS_ADM.INSTANTIATION_TABLE);
end;
/

```

## Bridged Execution Workflow

When a traditional HPE DMA workflow runs, all of its steps are executed against a single target. If you specify multiple targets, a separate “run” of the entire workflow is executed on each target.

In a **bridged execution workflow**, different steps within that workflow can run on different targets.

## Running a Bridged Execution Workflow

The process of running a bridged execution workflow is the same as the process for a traditional workflow—until run time.

### To run a bridged execution workflow:

1. On the Automation → Workflows page, create a deployable copy of the bridged execution workflow.
2. On the Automation → Deployments page, create a new (or modify an existing) deployment.  
Specify any parameter values that you want to use. Be sure to select any targets that you might want to specify at run time.
3. On the Automation → Run page, select your deployment.  
Click the [SELECT](#) link to specify each target used by the workflow.
4. Click **Run workflow** to execute the workflow.

## Additional Considerations

An HPE DMA user will not see deployments for a bridged execution workflow unless that user has Read permission for the organization.

Deployments for bridged execution workflows are only visible to users who have Read permission for the organization where one (or more) of the specified targets resides.

For a bridged execution workflow, the target listed on the upper pane of the Console and History pages corresponds to the specified Primary Target. You can find information about a specific target in the output details for the pertinent step.

**Figure: Run Page Before Target Selection**

The screenshot shows the 'Run Workflow' page in the HPE Database and Middleware Automation interface. The top navigation bar includes 'Workflows', 'Steps', 'Functions', 'Policies', 'Deployments', 'Run', 'Console', and 'History'. The 'Run' tab is active.

The main heading is 'Run Workflow'. Below it is a 'Filter' input field. A list of workflows is displayed on the left, with 'Simplified Bridged Execution Workflow' selected. The workflow details are shown below:

**Database Refresh Example: Simplified Bridged Execution Workflow**

**Get Source and Destination Targets** 1

**Target Parameters**

Primary Target:  [SELECT](#)

Destination:  [SELECT](#)

Source:  [SELECT](#)

**Export Data from Source DB** 2

No parameters.

**Import Data into Destination DB** 3

No parameters.

**Success** 4

No parameters.

At the bottom, there are two buttons: 'Select targets' and 'Run workflow'.

**Figure: Run Page After Target Selection**

The screenshot shows the 'Run Workflow' interface. At the top, there are tabs: Workflows, Steps, Functions, Policies, Deployments, **Run**, Console, and History. Below the tabs is a 'Run Workflow' header with a 'Filter' input field. A list of workflows is shown on the left, with 'Simplified Bridged Execution Workflow' selected. The main content area displays the workflow steps:

- Get Source and Destination Targets** (Step 1):
  - Target Parameters**
    - Primary Target:  [SELECT](#)
    - Destination:  [SELECT](#)
    - Source:  [SELECT](#)
- Export Data from Source DB** (Step 2):
  - No parameters.
- Import Data into Destination DB** (Step 3):
  - No parameters.
- Success** (Step 4):
  - No parameters.

At the bottom right, there is a 'Run workflow' button.

## Example

An example of a bridged execution workflow is a database refresh workflow that extracts the contents of a database on one target (the Source) and creates a new database with the same contents on another target (the Destination).

This type of workflow is useful if you want to clone a database—for example, to move it from a traditional IT infrastructure location into a private cloud, or to populate a test database with real production data.

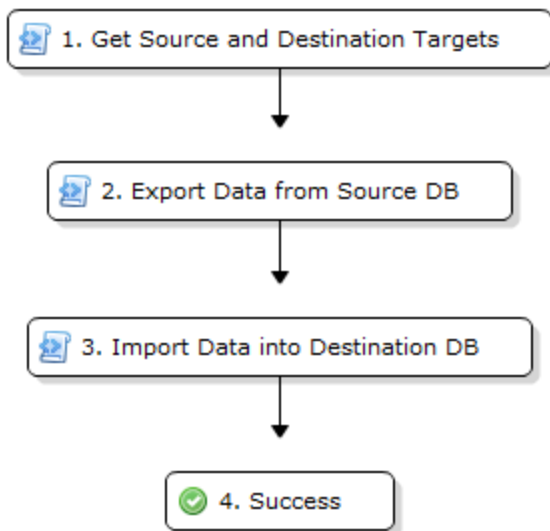
## Workflow

The workflow shown here is a very simplified example of a database refresh workflow. This workflow uses two targets:

- The Source target is the database instance where the contents of a specific database will be exported.
- The Destination target is the database instance where those contents will be imported.

**Note:** For the purpose of this simplified example, all other parameters have been removed.

All targets for a bridged execution workflow must have the same target level (Server, Instance, or Database) as the workflow itself. In this example, the target level is Instance.



A bridged execution workflow requires special settings both in the steps and in the workflow to facilitate the orderly selection of targets at run time. The following topics explain how bridged execution workflows affect each phase and artifact in the automation process.

## Obtaining Source and Destination Targets

The sole purpose of this step is to determine the targets for the subsequent steps. This step has two input parameters: Source and Destination.

Step	Name	Required Result	Next
1	<a href="#">Get Source and Destination Targets</a>		2
Destination: <input type="text" value="- User selected -"/>			
Source: <input type="text" value="- User selected -"/>			

Both input parameters must be set to - User selected - in the workflow.

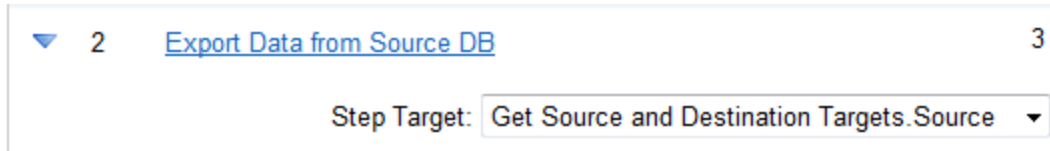
The step also has two output parameters with the same names: Source and Destination.



**Note:** It is important that the input and output parameters of this step have exactly the same names.

## Exporting Data from Source DB

The purpose of this step is to export the contents of the Source database. Its Step Target parameter is mapped to the Source output parameter of the first step.

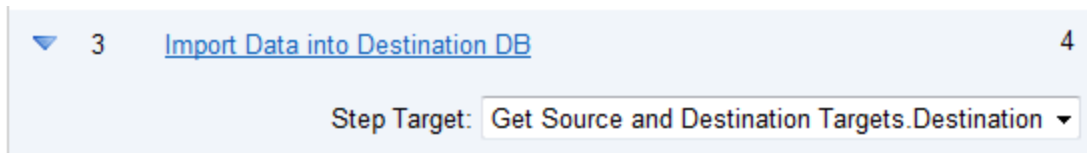


▼ 2 [Export Data from Source DB](#) 3

Step Target:

## Importing Data into Destination DB

The purpose of this step is to import the data that was exported in the previous step into the Destination database. Its Step Target parameter is mapped to the Destination output parameter of the first step.

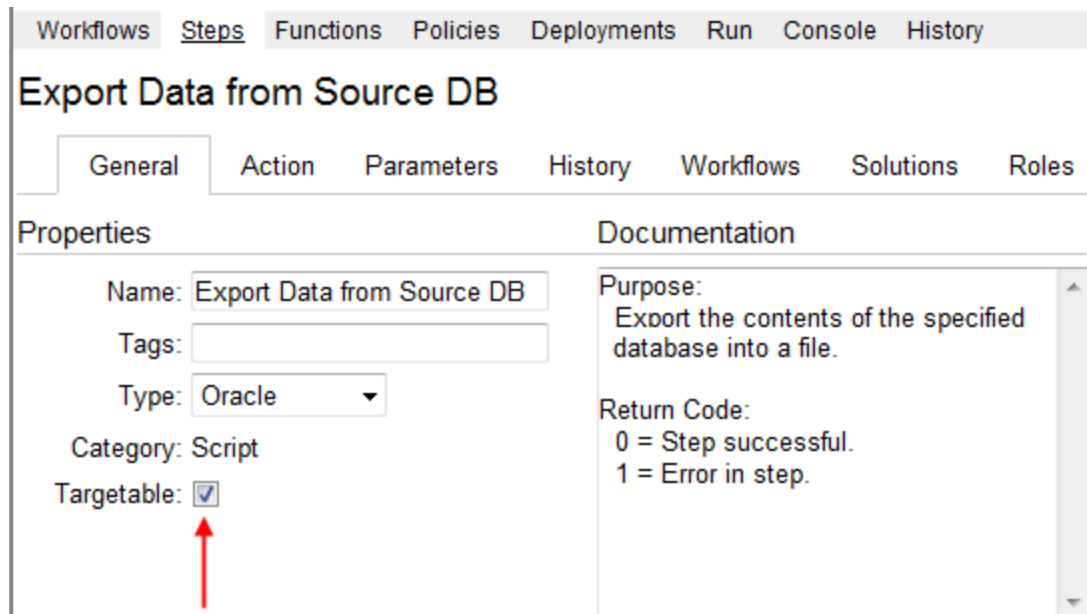


▼ 3 [Import Data into Destination DB](#) 4

Step Target:

## Targetable Steps

The Export Data from Source DB and Import Data into Destination DB steps are both “targetable” steps. This means that the target for each step is specified at run time.



Workflows Steps Functions Policies Deployments Run Console History

### Export Data from Source DB

General Action Parameters History Workflows Solutions Roles

**Properties**

Name:

Tags:

Type:

Category: Script

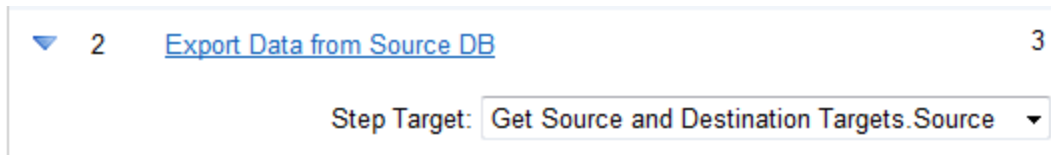
Targetable: ☒

**Documentation**

Purpose:  
Export the contents of the specified database into a file.

Return Code:  
0 = Step successful.  
1 = Error in step.

A targetable step has a special parameter called Step Target:



Step Target is only visible in the workflow editor. It does not appear on the Parameters tab in either the step or the deployment. Step Target must be mapped to an output parameter of a previous step.

**Best Practice:** As demonstrated in this example, the first step in a bridged execution workflow should gather the targets that subsequent steps will use. The Step Target parameter for each targetable step is then mapped to an output parameter of that first step.

## Deployment

The process of creating a deployment for a multi-target workflow is similar to the process for a traditional workflow with one salient difference. When you create (or modify) a deployment for a bridged execution workflow, the targets that you select on the Deployment page determine the list of available targets in the Select Target dialog on the Run page.

**Note:** The target parameters for the workflow (in this case, Source and Destination) do not appear on the Parameters tab in the deployment. This is because the targets must always be specified at run time in a bridged execution workflow. They cannot be specified in the deployment.

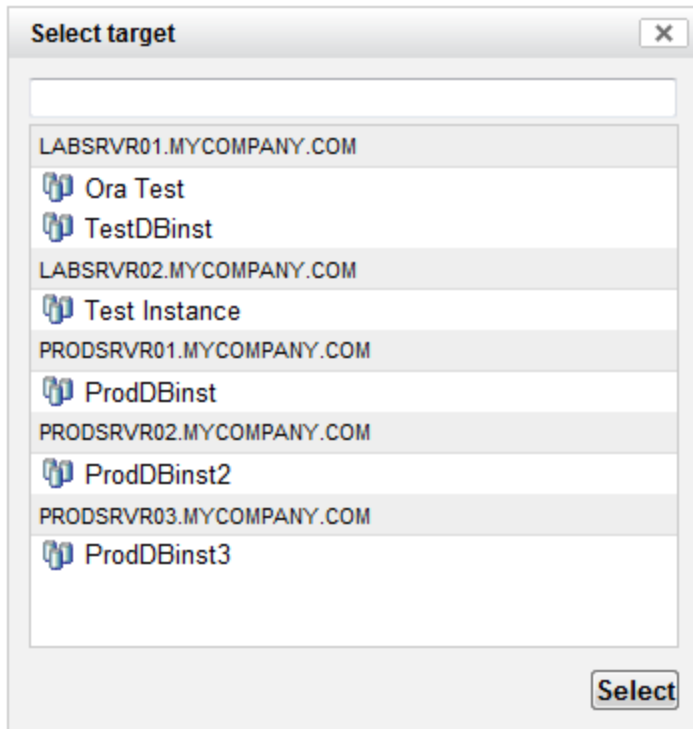
## Run

For a bridged execution workflow, the Run page looks different than it does for a traditional workflow.

Note the following:

- The SELECT links on the Run page enable you to specify each target required—in this case: Source, Destination, and Primary Target.

When you click a SELECT link, the Select Target dialog opens:



All available targets that you selected in the deployment are listed. You must select a single target from the list. If the list is long, you can filter it by typing characters in the text box at the top.

Select the target that you want to use, and click **Select**.

- The Primary Target is used by any steps in the workflow that are not targetable. In this particular workflow, there are no such steps.
- Until you select all the targets, the “Select targets” message is displayed in the lower right corner, and the Run workflow button is disabled.

After you select the targets, the Run Workflow button is enabled.

## Importing a File into the Software Repository

Many workflows are capable of downloading files from the software repository on the HPE DMA server to the target server (or servers) where the workflow is running. The following procedure shows you how to import a file into the software repository so that it can be downloaded and deployed by a workflow.

HPE DMA uses the HP Server Automation (SA) Software Library as its software repository.

**Tip:** Be sure to use unique file names for all files that you import into the software repository.

### To import a file into the SA Software Library:

1. Launch the SA Client from the Windows Start Menu.

By default, the HP Client is located in Start > All Programs > HP Software > HP Server Automation Client.

If the HP Client is not installed locally, follow the instructions under “Download and Install the HP SA Client Launcher” in the *HP Server Automation Single-Host Installation Guide*.

2. In the navigation pane in the SA Client, select Library > By Folder.

3. Select (or create) the folder where you want to store the file.
4. From the Actions menu, select **Import Software**.
5. In the Import Software dialog, click the **Browse** button to the right of the File(s) box.
6. In the Open dialog:
  - a. Select the file (or files) to import.
  - b. Specify the character encoding to be used from the Encoding drop-down list. The default encoding is English ASCII.
  - c. Click **Open**.The Import Software dialog reappears.
7. From the Type drop-down list, select **Unknown**.
8. If the folder where you want to store the files does not appear in the Folder box, follow these steps:
  - a. Click the **Browse** button to the right of the Folder box.
  - b. In the Select Folder window, select the import destination location, and click **Select**.The Import Software dialog reappears.
9. From the Platform drop-down list, select all the operating systems listed.
10. Click **Import**.

If one of the files that you are importing already exists in the folder that you specified, you will be prompted regarding how to handle the duplicate file. Press **F1** to view online help that explains the options.
11. Click **Close** after the import is completed.

# Maintenance

The following topics provide information to help you properly maintain your HPE DMA system.

- ["Resetting the HPE DMA Initial Admin password" below](#)  
Reset the password for the DMA Initial Admin (dma\_initial\_admin) account.
- ["Updating the Self-signed SSL Certificate" on page 79](#)  
Generate a new Self-Signed SSL Certificate and distribute your certificate to your managed servers.

## Resetting the HPE DMA Initial Admin password

For security reasons you may want to reset the password for the HPE DMA Initial Admin (dma\_initial\_admin) account.

HPE DMA provides a script to change the password for the HPE DMA Initial Admin (dma\_initial\_admin) account.

### To obtain online help:

Run the following command on the HPE 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 HPE 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 HPE 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.

# Updating the Self-signed SSL Certificate

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

- ["Updating Self-signed SSL Certificate on the HPE DMA Server"](#)
- [Updating Self-Signed SSL Certificate on the HPE DMA Client](#)

## Updating Self-signed SSL Certificate on the HPE DMA Server

To update the self-signed SSL certificate on the HPE DMA Server :

1. Stop HPE DMA:

```
# service dma stop
```

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

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

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

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

Specify the keystore password (the default is changeit).

The results will be similar to this:

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

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

tomcat, Oct 31, 2014, PrivateKeyEntry,
Certificate fingerprint (MD5): 99:35:B5:68:08:18:85:DB:51:96:FA:A4:41:A2:F3:AB
[root@IWFVM01939 bin:]#
```

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

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

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

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

Specify the keystore password (the default is changeit).

The results will be similar to this:

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

```
Enter keystore password:
```

```
[root@IWFVM01939 bin:~#
```

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

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

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

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

Specify the keystore password (the default is changeit).

The results will be similar to this:

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

```
Keystore type: JKS
```

```
Keystore provider: SUN
```

```
Your keystore contains 0 entries
```

```
[root@IWFVM01939 bin:~#
```

5. To generate the new self-signed SSL certificate, execute the following command (all on one line):

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

**Caution:** If you are using an SA gateway infrastructure as a proxy network, append `-ext SAN=ip:xx.xx.xxx.xxx` to the `keytool` command, replacing `xx.xx.xxx.xxx` with the desired IP address. For additional information, see ["Using a Proxy Server"](#).

The variables used here refer to the following information:

Variable	Description
<numberdays>	The number of days that the key will be valid.
<DMAserver>	Fully qualified host name of the server hosting the HPE DMA server.
<orgunit>	The organizational unit (business unit) that owns this server.
<org>	The organization (company) that owns this server.
<Location>	The city in which this server physically resides.
<state>	The state or province in which this server physically resides.
<country>	The country in which this server physically resides.



<code>&lt;keyalias&gt;</code>	Unique alias for the server's private key. This will be used to associate the server certificate with its private key. The default is tomcat.
<code>&lt;password&gt;</code>	The password for both the keystore and this private key.
<code>&lt;storefile&gt;</code>	Keystore file name. For example: /opt/hp/dma/server/.mykeystore

For example:

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

**Note:** You must use the same password for the `--keypass` and `--storepass` settings.

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

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

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

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

Specify the keystore password (the default is changeit).

The results will be similar to this:

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

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

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

- Start HPE DMA:
 

```
# service dma start
```
- Using the browser, log in to HPE DMA, as usual.

# Send Documentation Feedback

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

**Feedback on Administration Guide (Database and Middleware Automation 10.40)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to [hpe\\_dma\\_docs@hpe.com](mailto:hpe_dma_docs@hpe.com).

We appreciate your feedback!