



HP Database and Middleware Automation

Software Version: 10.30
Red Hat Enterprise Linux and SUSE Enterprise Linux

Administrator Guide

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

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2010-2015 Hewlett-Packard Development Company, L.P.

Trademark Notices

(missing or bad snippet)

Documentation Updates

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

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<https://softwaresupport.hp.com>

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

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

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

You will also receive updated or new editions if you subscribe to the appropriate product support service.

Contact your HP sales representative for details.

(missing or bad snippet)

Support

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

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

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

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

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

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

To find more information about access levels, go to:

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

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

Contents

Welcome	6
Audience	7
Document Map	8
Important Terms	9
Additional Resources	10
Chapter 1: Configuring Connector	11
Copying JAR Files	12
Configuring Connector	12
Chapter 2: Configure SSL on the HP DMA Server	14
About keytool	14
Generate a Private Key for the Server	15
Generate the Certificate Signing Request to Obtain Signed Server Certificates	16
Import the SSL Server Certificates	17
Configure the HP DMA Server to Use Your Certificate	18
Verify the SSL Connection	20
Chapter 3: Creating Targets	22
Creating Organizations	22
Adding Servers	23
Creating Custom Fields	24
Creating Smart Groups	25
Creating Policies	26
Using Discovery Workflows	27
Chapter 4: Installing Solution Packs	28
Installing Solution Packs	28
Versioning and Importing Solution Packs	30
Modifying a Solution Item	31
Roll Back a Solution Pack	31
Deleting a Solution Pack	32
Chapter 5: Configuring Email	33
Chapter 6: Special Configurations	34
Change the Default Port and Security Level	35
Use a Proxy Server with HP DMA	36
Default HP DMA Communications	37
Using an SA Satellite as a Proxy Server	38
How HP DMA Manages Proxy Communication	39
How to Set Up a Proxy Server	40
Configure the SA Core Gateway Properties	40
Specify the Server Automation Realm	41

Create and Configure the HP DMA Custom Fields	42
Specify a Renamed Windows Administrator User	44
Update the HP DMA APX	45
Create and Configure the HP DMA Custom Field	45
Run as a Windows Domain User	47
Configure Windows Domain User Using Custom Fields	47
Configure Windows Domain User Using Runtime Parameters	48
Change the Number of Active Connections	50
About This Help	51
Glossary	52

Welcome

This document describes the workflows used in HP Database and Middleware Automation (HP DMA).

Audience

This solution is designed for HP Database and Middleware Automation (HP DMA) administrators, who are responsible for all HP DMA administration tasks. They control the privileges and permissions available to each user role, and they decide which servers are managed by HP DMA. They may also be responsible for installing and updating HP DMA.

Document Map

The following table shows you how to navigate this guide:

Topic	Description
Configuring Connector	How to configure the Connector between HP DMA and HP Server Automation.
Configure SSL on the HP DMA Server	How to configure SSL on the HP DMA server.
Roles, Permissions, and Capabilities	How these mechanisms are used to achieve fine-grained role-based access control to HP DMA features, target servers, and automation content.
Creating Targets	How to manage the HP DMA target environment.
Installing Solution Packs	How to import a solution pack.
Configuring Email	How to specify the email settings.
Other Configurations	How to configure HP DMA for certain non-default scenarios.

Important Terms

Here are a few basic HP DMA terms that you will need to know:

- In HP DMA, a **workflow** executes a process —such as installing a software product or checking a database instance for compliance with a specific security benchmark.
- A workflow consists of a sequence of **steps**. Each step performs a very specific task. Steps can be shared among workflows.
- Steps can have input and output **parameters**, whose values will be unique to your environment.

If you provide correct values for the input parameters that each scenario requires, the workflow will be able to accomplish its objective. Output parameters from one step often serve as input parameters to another step.

- A **solution pack** contains a collection of related workflows and the steps, functions, and policies that implement each workflow.

More precisely, solution packs contain **workflow templates**. These are read-only versions of the workflows that cannot be deployed. To run a workflow included in a solution pack, you must first create a deployable copy of the workflow template and then customize that copy for your environment.

- A **deployment** associates a workflow with the targets (servers, instances, or databases) where the workflow will run. To run a workflow, you execute a specific deployment. A deployment is associated with one workflow; a workflow can have many deployments, each with its own targets and parameter settings.
- The umbrella term **automation items** is used to refer to those items to which role-based permissions can be assigned. Automation items include workflows, deployments, steps, and policies.

Organizations also have role-based permissions. Servers, instances, and databases inherit their role-based permissions from the organization in which the server resides.

- The **software repository** contains any files that a workflow might need to carry out its purpose (for example, software binaries or patch archives). If the files that a workflow requires are not in the software repository, they must be stored locally on each target server.

When you are using HP DMA with HP Server Automation (HP SA), the software repository is the HP SA Software Library.

- An **organization** is a logical grouping of servers. You can use organizations to separate development, staging, and production resources—or to separate logical business units. Because user security for running workflows is defined at the organization level, organizations should be composed with user security in mind.

Additional terms are defined in the [Glossary](#) on page 52.

Additional Resources

For additional information about using HP DMA, see the following documents:

Purpose	Document
To install HP DMA	<i>Database and Middleware Automation Installation Guide</i>
For help troubleshooting the HP DMA installation process	<i>Database and Middleware Automation Troubleshooting Guide</i>
To use the HP DMA web interface	<i>Database and Middleware Automation User Guide</i>
For simple instructions to run an HP DMA workflow	<i>Database and Middleware Automation Quick Start Tutorial</i>
For information about specific solution packs and workflows	See the HP DMA solution pack user guides

These documents are part of the HP DMA documentation library, which is available on the HP Software Support web site:

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

For additional information about using HP DMA APIs, see the following WebHelp:

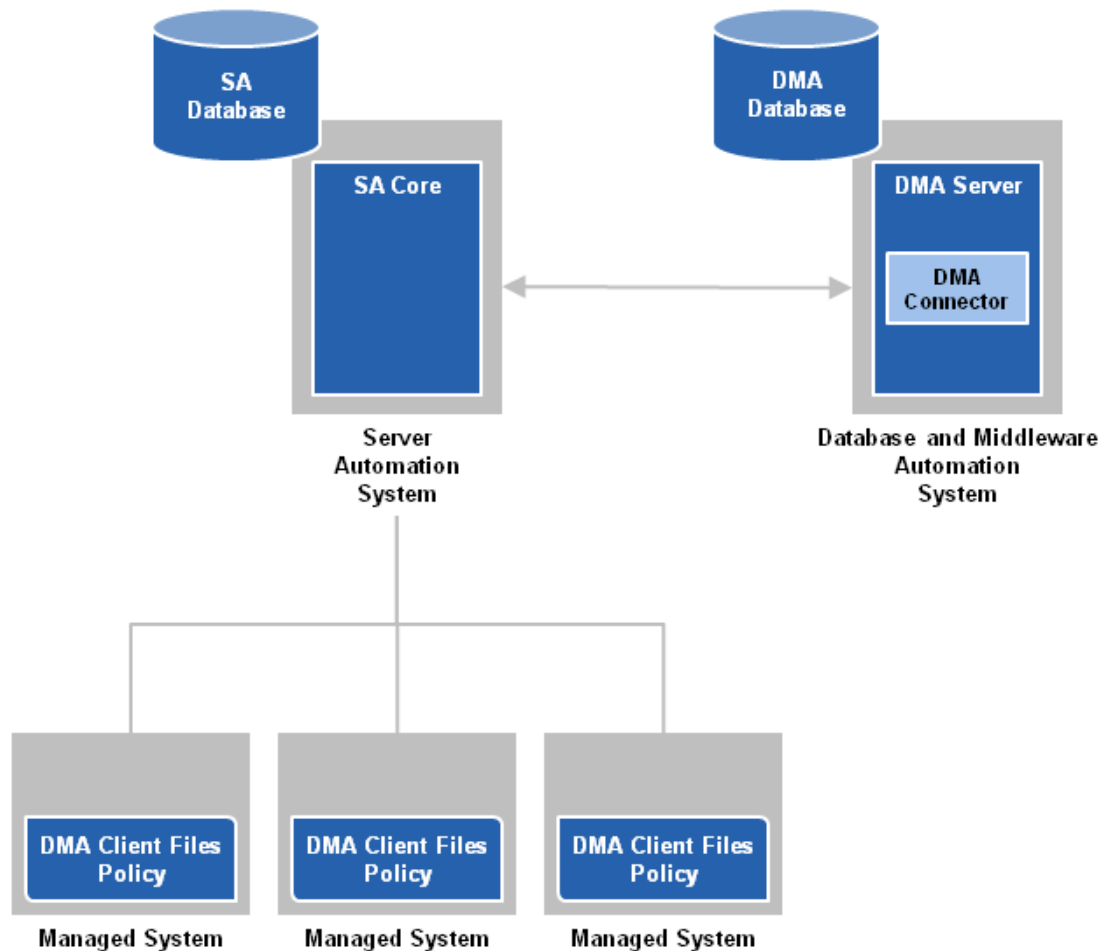
Purpose	Document
To use the HP DMA application programming interfaces (APIs)	<i>HP DMA API Reference WebHelp</i> is available on all HP DMA Servers at: <code>https://<DMA_SERVER>:8443/dma/api</code> Here, <DMA_SERVER> is the fully qualified host name of your HP DMA server.

Chapter 1: Configuring Connector

HP DMA includes a Connector component that enables it to communicate with HP Server Automation. You must configure the Connector before you can do the following:

- Run an HP DMA workflow against a target.
- Add managed servers.
- Configure roles.

The following example shows how HP DMA connects to HP Server Automation:



The Connector is added and initially configured when you install HP DMA (see [\[\[\[Undefined variable DMAVariables_SolnPack.Official_Install_Guide_Name\]\]\]](#)).

Caution: If you change the location or configuration of HP Server Automation, you may need to copy the JAR files and reconfigure the Connector.

If you switch the HP DMA Server to a different SA Core, the Connector needs to be reconfigured.

If the new SA Core is part of the same SA mesh, the same SA database is available. To complete the switch, follow the instructions in "HP DMA is Switched to Different SA Core" in the *HP DMA Troubleshooting Guide*.

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

Copying JAR Files

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

HP DMA provides a script to copy the JAR files from the intended SA Core so that HP 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 HP DMA server, run the following script command to copy the required JAR files from the SA server to the HP DMA server. For example (enter as a single line):

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

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

Configuring Connector

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

To configure the Connector:

1. Go to Setup > Connectors.
2. If a Connector already exists, click the tab that corresponds to the Connector for SA.
To add a new Connector, click the Add Connector button in the lower right corner.
3. Specify the information required.

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

hp Database & Middleware Automation

Home Automation Reports Environment Solutions **Setup**

Configuration Permissions Capabilities Roles **Connector**

Connector

SAsrvr001.mycompany.com

Server Automation Host: SAsrvr001.mycompany.com

Server Automation Username: dma_integration_user

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 HP DMA

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

4. Click the **Save** button.

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

5. Stop and restart your HP DMA server:

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

Chapter 2: Configure SSL on the HP DMA Server

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

1. [Generate a Private Key for the Server](#) on the next page
2. [Generate the Certificate Signing Request to Obtain Signed Server Certificates](#) on page 16
3. [Import the SSL Server Certificates](#) on page 17
4. [Configure the HP DMA Server to Use Your Certificate](#) on page 18
5. [Verify the SSL Connection](#) on page 20

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 HP DMA server.

For detailed instructions and an example of the `keytool` command that sets up the SAN, see "Use a Proxy Server with HP DMA" in the [\[\[\[Undefined variable DMAVariables_SolnPack.Official_Install_Guide_Name\]\]\]Use a Proxy Server with HP DMA](#).

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

About keytool

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

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

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

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

```
which keytool
```

Generate a Private Key for the Server

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

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

To generate a private key for the server:

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

```
/opt/hp/dma/server/jre/bin/keytool -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, 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 "Use a Proxy Server with HP DMA" in the [Use a Proxy Server with HP DMA](#).

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 HP DMA, set to <code>tomcat</code> .
<DMAserver>	Fully qualified host name of the server hosting the HP DMA server.
<orgunit>	The organizational unit (business unit) that owns this server.
<org>	The organization (company) that owns this server.
<Location>	The city in which this server physically resides.
<state>	The state or province in which this server physically resides.
<country>	The country in which this server physically resides.
<password>	The password for both the keystore and this private key.
<storefile>	Keystore file name. For example: <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>
```

Generate the Certificate Signing Request to Obtain Signed Server Certificates

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

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

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

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

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

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

For example:

```
/opt/hp/dma/server/jre/bin/keytool -certreq -v -alias 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.

Import the SSL Server Certificates

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

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

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

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

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

- Root certificate
- Primary intermediate certificate
- Secondary intermediate certificate

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

The variables used here refer to the following information:

Variable	Description	Examples
<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

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

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

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

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

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

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

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

For example:

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

You should see the following type of output:

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

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

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

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

Configure the HP DMA Server to Use Your Certificate

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

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

To configure the HP DMA server to use your certificate:

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

```
service dma stop
```

2. Open the following file in a text editor:

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

3. Identify the default SSL Connector element:

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

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

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

The variables used here represent the following information:

Variable	Description
<code><keyalias></code>	Unique alias for the server's private key (see Generate a Private Key for the Server on page 15).
<code><SSLport></code>	Port that will be used for: <ul style="list-style-type: none">• SSL communication between the HP DMA Server and the HP DMA clients• Accessing the HP DMA user interface
<code><storefile></code>	Keystore file name. For example: <code>/opt/hp/dma/server/.mykeystore</code>
<code><password></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 HP DMA Server by using the following command:

```
service dma start
```

Verify the SSL Connection

To verify your SSL connection, do the following:

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

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

4. For a test, execute an HP DMA deployment.

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

Warning: DMA Client is trusting all HTTPS Certificates

If it is in the output, go back to [Configure the HP DMA Server to Use Your Certificate](#) on page 18, make the change in the `dma.xml` file, and then execute the deployment again.

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

Note: You have completed configuring SSL on the HP DMA server.

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

Chapter 3: Creating Targets

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

The HP 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 HP 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.

Creating 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 HP 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 *HP 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 the **Save** button.

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 the **Save** button.

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 the **Delete** button.

Adding Servers

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

With HP 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 HP DMA organization and used as an HP DMA target.

Tip: See the *HP 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 *HP 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 the **Add servers** button.

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

The servers that you can see in the list depend on your permissions in HP 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 the **Add** button. 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.

Creating 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 HP 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 *HP DMA User Guide* and the *HP DMA API Reference WebHelp* (see [Additional Resources](#) on page 10).

To create a new Custom Field:

1. Go to Environment > Custom Fields.
2. Click the **New field** button.
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 the  (add) button. 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 modifications that you want to make.

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 the **Delete** button to confirm.

Creating 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 HP 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 HP DMA administrator, you can create, view, modify, and delete Smart Groups for any organization.

For additional information about Smart Groups, see the *HP DMA User Guide* and the *HP DMA API Reference WebHelp* (see [Additional Resources](#) on page 10).

To create a new Smart Group:

1. Go to Environment > Smart Groups.
2. Click the **New Group** button.
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 modifications that you want to make.

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 the **Delete** button to confirm.

Creating 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 HP 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 HP 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 *HP DMA User Guide* and the *HP DMA API Reference WebHelp* (see [Additional Resources](#) on page 10).

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 modifications that you want to make to the policy.

You can modify the Name, Attributes, and Role assignments for any policy that is not locked.

Policies that are included in HP 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 the **Delete** button to confirm.

Using Discovery Workflows

HP 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 *HP DMA User Guide*.

Chapter 4: Installing Solution Packs

A solution pack is a set of HP 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 HP 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 HP DMA.

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

Installing Solution Packs

The HP 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 (see [Support](#) on page 1).

To get the most recent HP DMA patch:

1. Go to the following web site: <https://softwaresupport.hp.com/>
2. Sign in using your HP Passport credentials (see [Support](#) on page 1 for more information).
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 HP DMA solution packs:

To access the HP DMA solution packs, mount the ISO file of the HP DMA10.30 (or patch) installation media.

The solution packs are located in the following folders:

- The `DMA_10.30.000.000_Server_and_Client` folder contains the Discovery and Promote solution packs.

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

- The `DMA_10.30.000.000_Database_Solution_Packs` folder contains all of the database solution packs (provisioning, advanced provisioning, patching, advanced patching, compliance, refresh, and release management).
- The `DMA_10.30.000.000_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://<HP 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 [How to Change the Default Port](#)).

2. Log in to the HP 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.

hp Database & Middleware Automation

Home Automation Reports Environment Solutions Setup

Installed History

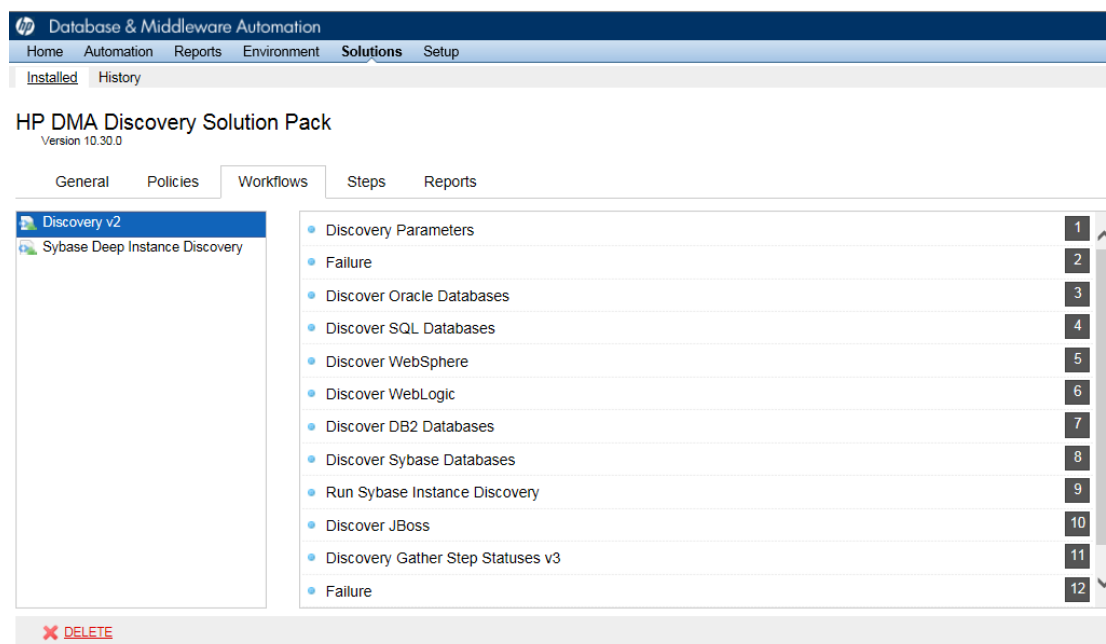
Installed Solutions

✓ Successfully imported HP DMA Discovery Solution Pack

SOLUTION PACKS	DETAILS
HP DMA Discovery Solution Pack Version 10.30.0	<ul style="list-style-type: none">• 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

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 HP 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 [Roll 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**.

Roll 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, HP 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:

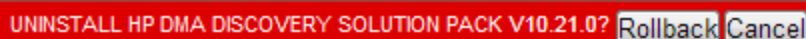
1. Go to the Solutions > History page.
2. Click the ROLLBACK link in the lower left corner.

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



DOWNGRADE HP DMA DISCOVERY SOLUTION PACK TO V10.20100.0? Rollback Cancel

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



UNINSTALL HP DMA DISCOVERY SOLUTION PACK V10.21.0? Rollback Cancel

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

Deleting a Solution Pack

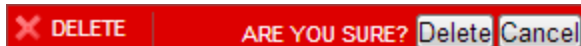
You can delete any solution pack that was previously installed. When you delete a solution pack, no attempt is made to restore any previous version of that solution pack.

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:



X DELETE ARE YOU SURE? Delete Cancel

4. Click the **Delete** button 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.

Chapter 5: Configuring Email

The email 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 the **Save** button.

Chapter 6: Special Configurations

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

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

[Use a Proxy Server with HP DMA](#) on page 36

[Specify a Renamed Windows Administrator User](#) on page 44

[Run as a Windows Domain User](#) on page 47

[Change the Number of Active Connections](#) on page 50

Change the Default Port and Security Level

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

To change the HP DMA port:

1. Stop HP DMA:

```
# service dma stop
```

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

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

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

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

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

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

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

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

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

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

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

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

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

8. Start HP DMA:

```
# service dma start
```

Use a Proxy Server with HP DMA

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

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

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

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

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

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

For additional information, see [Configure SSL on the HP DMA Server](#) "Configure SSL on the HP DMA Server" in the `[[[Undefined variable DMAVariables_SolnPack.Official_Install_Guide_Name]]]`.

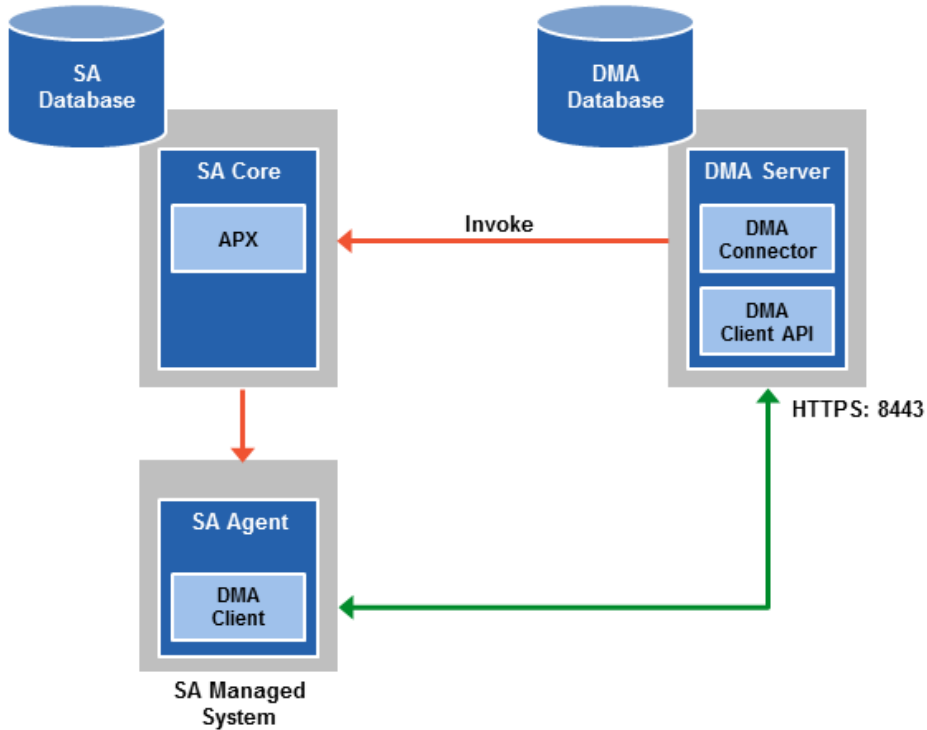
Note: The diagrams in this topic show simplified configurations of servers and communication paths. Real-world situations are much more complex with multiple SA Cores mapped to multiple SA Managed Servers. Multiple SA Satellites may also be configured.

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

Default HP DMA Communications

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

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

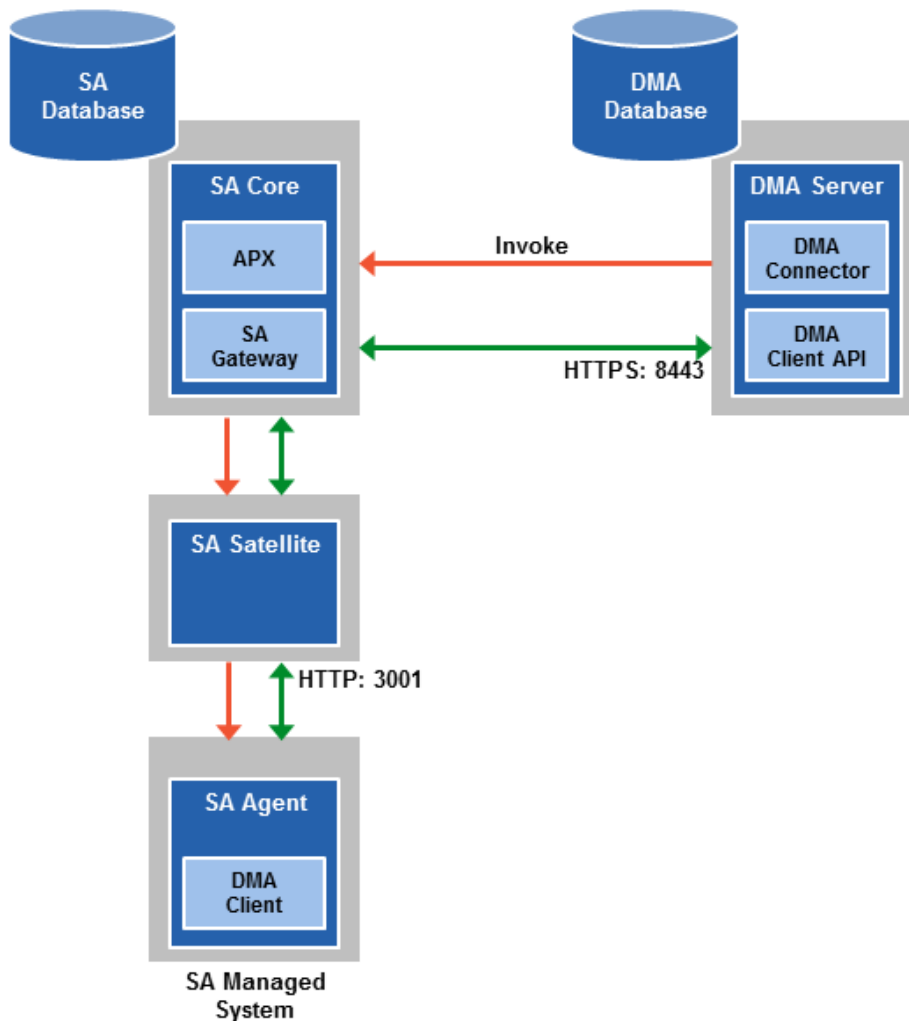


Using an SA Satellite as a Proxy Server

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

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

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



How HP DMA Manages Proxy Communication

HP DMA uses two Custom Fields to control proxy communication:

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

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

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

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

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

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

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

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

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

How to Set Up a Proxy Server

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

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

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

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

Configure the SA Core Gateway Properties

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

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

To add the new EgressFilter rule:

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

- a. Create or edit the gateway configuration file:

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

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

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

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

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

- c. Save the file.

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

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

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

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

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

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

Specify the Server Automation Realm

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

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

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

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

To specify the SA realm:

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

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

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

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

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

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

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

```
type="javax.sql.DataSource"  
url="jdbc:oracle:thin:@dma1.mycompany.com:1521:DMA"  
username="dma"/>  
</Context>
```

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

Create and Configure the HP DMA Custom Fields

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

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

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

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

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

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

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

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

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

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

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

- Set `west_proxy_address` to the full URL of the proxy, including the port, in this format:
`http://<proxy_hostname>:<proxy_port>`

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

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

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

My Organization

Properties Custom Fields Roles

Custom fields [NEW CUSTOM FIELD](#)

west_proxy_address:

west_proxy_in_use:

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

My Organization

Properties Custom Fields Roles

Custom fields [NEW CUSTOM FIELD](#)

west_proxy_address:

west_proxy_in_use:

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

Specify a Renamed Windows Administrator User

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

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

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

Instructions for making each of these changes are provided here.

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

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

Update the HP DMA APX

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

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

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

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

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

To update the HP DMA APX:

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

Create and Configure the HP DMA Custom Field

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

To create and configure the Custom Field:

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

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

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

agent_username_win with type Text

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

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

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

3. For each organization or server where you want to specify the Windows Administrator user name:
Go to Environment > Dashboard > <organization_name> (Optional: > <server_name>) to specify the Windows Administrator user name in the agent_username_win Custom Field.

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

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

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

Run as a Windows Domain User

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

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

Note: The specified domain user must:

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

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

Configure Windows Domain User Using Custom Fields

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

- domain_username_win
- domain_password_win

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

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

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

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

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

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

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

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

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

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

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

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

Note: If you have renamed the Windows Administrator account on your Windows target servers, you must also perform the procedures required to [Specify a Renamed Windows Administrator User](#) on page 44.

Configure Windows Domain User Using Runtime Parameters

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

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

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

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

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

Workflow	Step
MS SQL - Install Standalone SQL Instance	MS SQL - Advanced Parameters - Install Standalone
MS SQL - Install Clustered SQL Instance	MS SQL - Gather Advanced Parameters For Install Clustered SQL Instance

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

- 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 [Specify a Renamed Windows Administrator User](#) on page 44.

Change the Number of Active Connections

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

To change the number of active connections:

1. As root, stop the HP DMA server:
`$ service dma stop`
2. Open the following file in a text editor:
`/opt/hp/dma/server/tomcat/conf/Catalina/localhost/dma.xml`
3. Modify the following parameters:

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

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

4. Start the HP DMA server again:
`$ service dma start`

About This Help

[Legal Notices](#)

[Documentation Updates](#)

[Support](#)

Glossary

A

automation items

The umbrella term automation items is used to refer to those items to which role-based permissions can be assigned. Automation items include workflows, deployments, steps, and policies.

B

bridged execution

A bridged execution workflow includes some steps that run on certain targets and other steps that run on different targets. An example of a bridged execution workflow is Extract and Refresh Oracle Database via RMAN (in the Database Refresh solution pack). This workflow 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 workflow is useful when you want to clone a database - for example, to move it from a traditional IT infrastructure location into a private cloud. Bridged execution workflows are supported on HP DMA version 9.11 (and later).

C

capability

Capabilities are collections of related privileges. There are three capabilities defined in HP DMA. Login Access capability enables a user to log in to the web interface. This capability does not guarantee that this user can view any organizations or automation items—permissions are required to access those items. Workflow Creator capability enables a user to create new workflows and make copies of other

workflows. Administrator capability enables a user to perform any action and view all organizations. If you have Administrator capability, you do not need Workflow Creator capability. The Administrator can assign any of these capabilities to one or more roles registered roles.

connector

HP DMA includes a Connector component that enables it to communicate with HP Server Automation. You must configure the Connector before you can run an workflow against a target.

cross-platform

Cross-platform database refresh involves converting the data from one type of byte ordering to another. This is necessary, for example, if you want to load a database dump file on a little-endian Linux target that was created on a big-endian Solaris server.

custom field

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.

D

deployment

Deployments associate a workflow with a target environment in which a workflow runs. You can customize a deployment by specifying values for any workflow parameters that are designated - User Selected - in the workflow. You must save a deployment before you can run the workflow. You can re-use a saved deployment as many times as you like.

F

function

Functions are reusable pieces of code that can be included in automation steps. Any common routine or operation that multiple steps perform is a good candidate for a function. Functions can be tagged with keywords indicating the language in which they are written and the operating system with which they work. Functions are "injected" into the step code just prior to step execution.

I

input parameters

A workflow has a set of required parameters for which you must specify a value. The required parameters are a subset of all the parameters associated with that workflow. The remaining parameters are considered optional. You can specify a value for an optional parameter by first exposing it using the workflow editor and then specifying the value when you create a deployment.

M

mapping

An input parameter is said to be "mapped" when its value is linked to an output parameter from a previous step in the workflow or to a metadata field. Mapped parameters are not visible on the Deployment page. You can "unmap" a parameter by specifying - User Selected - in the workflow editor. This parameter will then become visible on the Deployment page.

O

organization

An organization is a logical grouping of servers. You can use organizations to

separate development, staging, and production resources - or to separate logical business units.

P

parameters

Parameters are pieces of information - such as a file system path or a user name - that a step requires to carry out its action. Values for parameters that are designated User Selected in the workflow can be specified in the deployment. Parameters that are marked Enter at Runtime in the deployment must be specified on the target system when the workflow runs.

policy

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

R

raw devices

In Sybase ASE version 15, you can create and mount database devices on raw bound devices. This enables Sybase ASE to use direct memory access from your address space to the physical sectors on the disk. This can improve performance by reducing memory copy operations from the user address space to the operating system kernel buffers.

role

Each HP DMA user has one or more roles. Roles are used to grant users permission to log in to and to access specific automation

items and organizations. Roles are defined in HP Server Automation. Before you can associate a role with an automation item or organization, however, you must register that role in HP DMA.

S

smart group

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 the groups is re-evaluated.

software repository

The software repository is where the workflow will look for any required files that are not found on the target server. If you are using HP DMA with HP Server Automation (SA), this repository is the SA Software Library.

solution pack

A solution pack contains one or more related workflow templates. These templates are read-only and cannot be deployed. To run one of the workflows included in a solution pack, you must first create a deployable copy of that template and then customize that copy for your environment. Solution packs are organized by function - for example: database patching or application server provisioning.

steps

Steps contains the actual code used to perform a unit of work detailed in a workflow.

T

target instance

In the context of MS SQL database refresh, the term "target instance" refers to the SQL

Server instance where the database that will be restored resides.

W

workflow

A workflow automates the process followed for an operational procedure. Workflows contain steps, which are linked together to form business logic for a common task. Workflows connect existing tasks in order to perform a new business process by building on existing best practices and processes.

workflow editor

The workflow editor is the tool that you use to assemble steps into workflows. You can map each input parameter to output parameters of previous steps or built-in metadata (such as the server name, instance name, or database name). You can also specify User Selected to expose a parameter in the deployment; this enables the person who creates the deployment to specify a value for that parameter.

workflow templates

A workflow template is a read-only workflow that cannot be deployed. To run one of the workflows included in a solution pack, you must first create a deployable copy of the workflow template and then customize that copy for your environment.