Database and Middleware Automation

Software Version: 10.50.001.000

Linux, Solaris, AIX, and HP-UX

Administration Guide

Document Release Date: May 2017

Software Release Date: May 2017

Hewlett Packard Enterprise

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

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

Documentation Updates

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

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

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

Support

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

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

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

HPE Software Solutions Now accesses the HPSW Solution and Integration Portal website. This site enables you to explore HPE Product Solutions to meet your business needs, includes a full list of Integrations between HPE Products, as well as a listing of ITIL Processes. The URL for this website is https://softwaresupport.hpe.com/km/KM01702731.

About this PDF Version of Online Help

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

Contents

Administer

This section provides information to help you administer DMA.

Enabling IPv6

Perform the following steps to enable Internet Protocol version 6 (IPv6) after installing or upgrading the DMA server:

1. Stop 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. Modify the hostname for the `webServiceUrl` parameter to the hostname that resolves into an IPv6 address.

4. Save your changes to the `server.xml` file and exit the text editor.

5. Start DMA:

   ```
   # service dma start
   ```

Create targets

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

The DMA **Environment** page contains two parts: the organization browser at the top, and the object editor at 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 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. Organizations should be composed with user security in mind because user security for running workflows is implemented at the organization level.

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

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

Create an organization

Perform the following steps to create an organization:

1. Go to **Environment** > **Dashboard**.
2. Click **New Organization**.

3. Specify a unique Name for the organization.
4. Click **Save**.

Grant permission to access an organization

Perform the following steps 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**.

Delete an organization

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.

Perform the following steps 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 DMA targets must have the ability to communicate with 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 DMA organization and used as an DMA target.

> **Tip:** For more information about installing the DMA Client Files policy on a managed server, see the Install the DMA Client Files policy topic in the *DMA Integration Guide*.

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.

Add servers to an organization

Perform the following steps 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 box opens. It contains a list of the managed servers that can be used as DMA targets and are not included in an organization.

   The servers that you can see in the list depend on the permissions you have 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 box closes.

Delete servers from an organization

Perform the following steps 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 alowed 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 they actually represent Oracle instances or not. 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 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.

Creating a new custom field

Perform the following steps 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**.

Modify an existing custom field

Perform the following steps to modify an existing custom field:

1. Go to **Environment** > **Custom Field**s.
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**.

Deleting a custom field

Perform the following steps 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 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 DMA administrator, you can create, view, modify, and delete Smart Groups for any organization.

Create a new Smart Group

Perform the following steps 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 the AND logical expression. All the 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**.

Modify a Smart Group

Perform the following steps to modify an exisiting 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**.

Delete a Smart Group

Perform the following steps 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 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 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.

Create a new policy

Perform following the steps to create a new Smart Group:

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**.

Modify a policy

Perform the following steps 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 DMA solution packs are locked. You cannot modify a locked policy, but you can make a modifiable copy of that policy.
4. Click **Save**.

Delete a policy

Perform the following steps 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

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 about using the Discovery workflows, see the *Workflow for Discovery Guide*.

Manage solution packs

This section describes the following tasks that you can perform to manage the solution packs that you have imported.

Modify a solution item

You may have to modify the automation items included in an installed solution pack to fit your company's needs. Solution packs are fully-supported by HPE, 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 want to modify.

To make a copy of a solution pack item, do the following:

1. Go to the **Solutions** > **Installed** page.
2. Select the solution pack that you want to modify.
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 in either of the following situations:

- if you discover that you accidentally overwrote a version of the solution pack that you need
- 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 "Modify a solution item" on the previous page.

> **Note:** 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 the solution pack. For example, if you initially import version 3, and then perform a rollback, 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 displays **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 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.

Perform the following steps 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 message appears:

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

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

Delete 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.

Perform the following steps to delete a 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 message appears:

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.

Configure email settings

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

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

Perform the following steps to configure the email 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 **Test**, 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**.

Hide and unhide workflows

You can hide workflows such as 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.

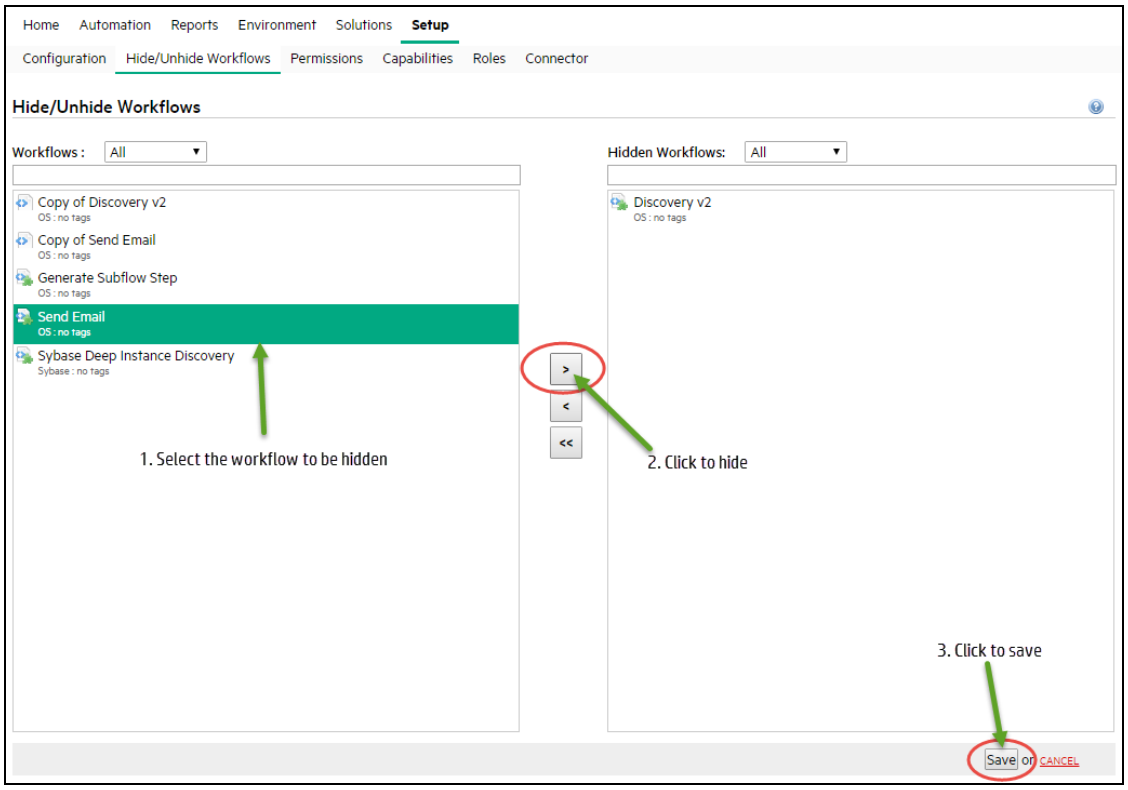
If a workflow with existing deployments is hidden, those deployments will not be hidden. These deployments can be modified and saved, but cannot be copied.

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

Hide a workflow

Perform the following steps to hide a workflow:

1. Login to DMA as admin or user with administrator privileges.
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 list of workflows and click  to hide the workflow.

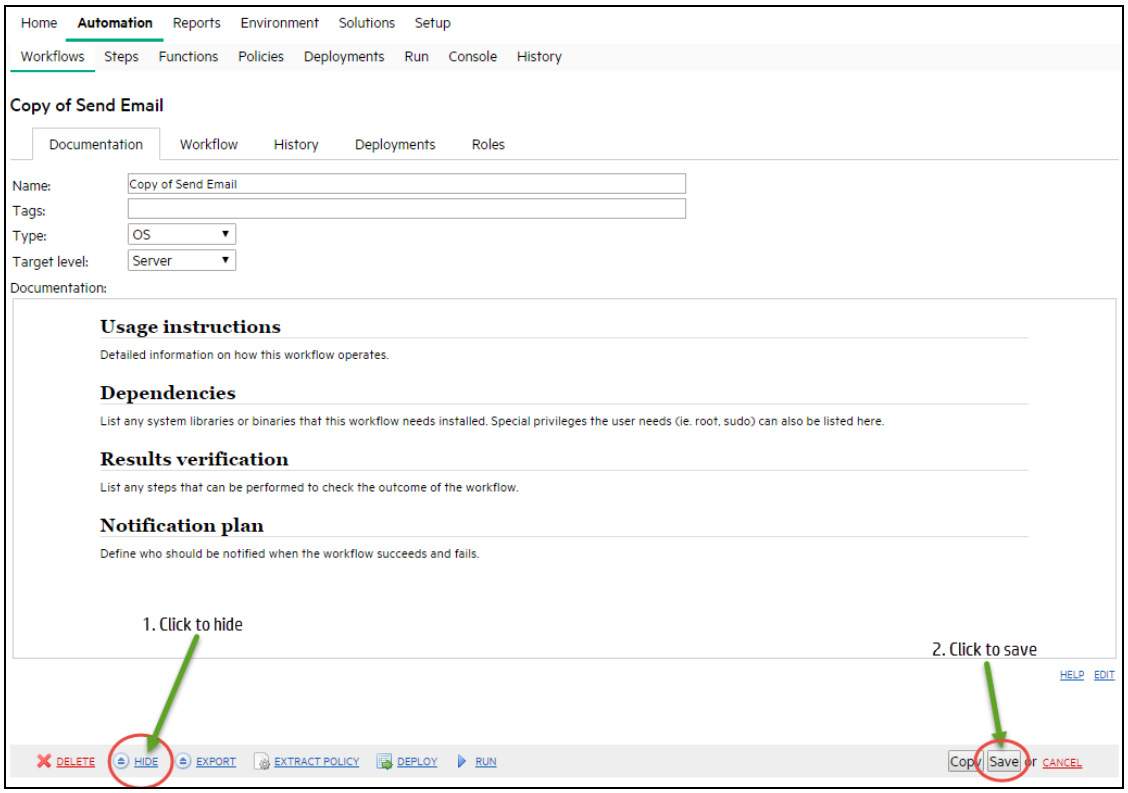


5. Click **Save**.
6. Confirm **Yes** to hide the selected workflow.
7. Repeat steps 3 through 6 to hide the required workflows.

Hide a workflow as a workflow creator or administrator

Perform the following steps to hide a workflow as the 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.



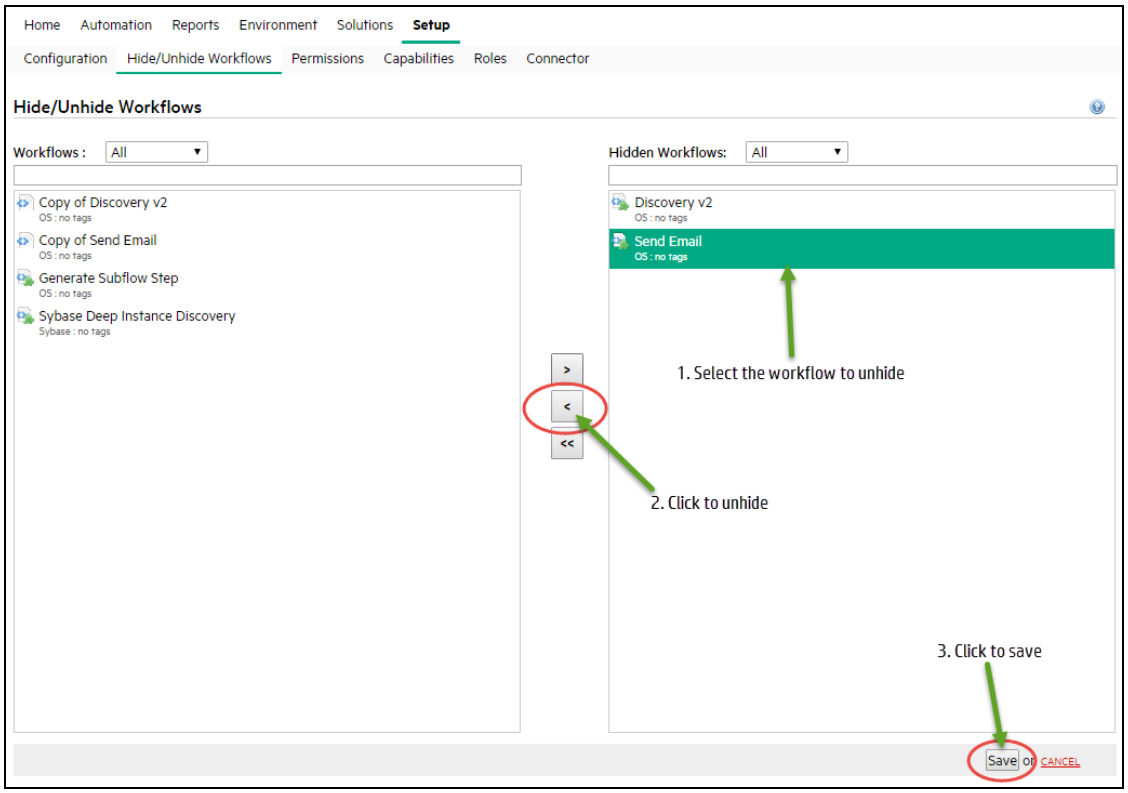
6. Click **Save**.
7. Confirm **Yes** to hide the selected workflow.
8. Repeat steps 3 through 7 to hide the required workflows.

Unhide a workflow

Perform the following steps to unhide a workflow:

1. Login to DMA as administrator or user with administrator privileges.
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 list of workflows list and click 

to unhide the workflow.



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

Change the default port and security level

DMA uses port 8443 and HTTPS protocol by default. You can change this to another port (for example, 8080) and the protocol from secure to non-secure (for example, HTTP). Perform the following steps to change the port:

1. Stop 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 following:

   ```
   <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 following:

   ```
   <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. 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"/>
   ```

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

6. Start DMA:

   ```
   # service dma start
   ```

Use a proxy server

A proxy server can be used to provide additional security for 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 `server.xml` file is set to false, you must have a Subject Alternative Name (SAN) as part of your signed certificate:

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

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 the Configure SSL on the DMA Server topic in the *Installation Guide*.

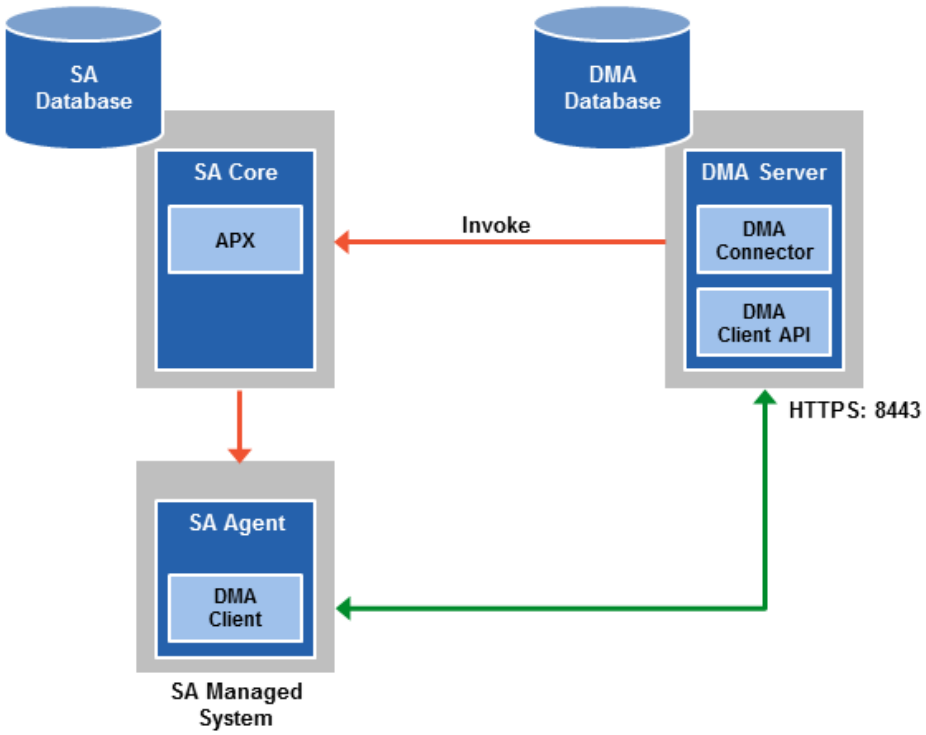
Note: The diagrams in this topic show simplified configurations of servers and communication paths. Real-world situations are much more complex with multiple SA Cores mapped to multiple SA Managed Servers. Multiple SA Satellites may also be configured.

For more information, see the Using SA Gateway Network as a Proxy Network topic in the *Installation Guide*.

Default DMA communications

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

1. 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.

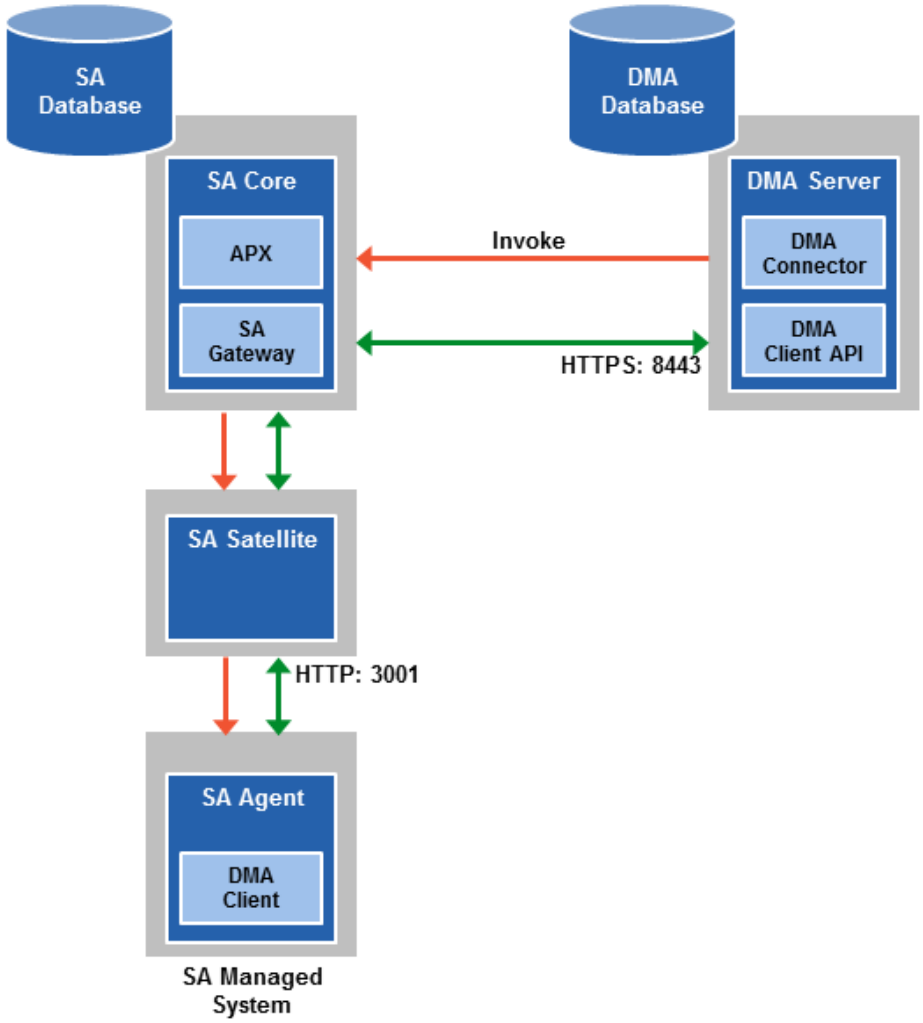


Use an SA Satellite as a proxy server

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

1. 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.


SA Database
DMA Database
SA Core
APX
SA Gateway
Invoke
HTTPS: 8443
DMA Server
DMA Connector
DMA Client API
SA Satellite
HTTP: 3001
SA Agent
DMA Client
SA Managed System

How DMA manages proxy communication

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 DMA whether a proxy server will be used. Valid values are:

TRUE	Use the proxy specified in the `west_proxy_address`
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 a 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.

Proxy precedence

The following table shows how 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

Proxy Precedence	Server value is TRUE	Server value is FALSE	Server value is not set
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

Set up a proxy server

To set up a proxy server for DMA, make the following changes to the 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 `server.xml` configuration file.
3. Create and configure the two **Custom Fields** that instruct DMA to route traffic through the proxy server. This procedure is performed in the DMA UI.

Instructions for making each of these changes are provided here. For more information about the SA Satellite and SA Gateway, see the SA gateways and SA Satellites topics in the Server Automation Getting Started Guide.

Configuring the SA Core Gateway properties

On the SA Core, add a new Egress Filter 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.

Add a new Egress Filter 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 executing 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.

   > **Note:** If the SA Core is multi-sliced, repeat step 1 through step 3 for every slice of SA core that is connected to the DMA server.

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 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 DMA server in the `webServiceUrl` parameter.

To specify the SA realm while the DMA Server is being installed, perform the following steps after baselining is completed:

1. Stop the DMA service

   ```
   service dma stop
   ```

2. Open the `/opt/hp/dma/server/tomcat/conf/server.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 DMA server is connected to.
4. Specify the IP address of your DMA server in the `webServiceUrl` parameter:

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

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

   ```
   ....
   <?xml version="1.0" encoding="UTF-8"?>
   <Valve className="org.apache.catalina.valves.AccessLogValve" directory="${dma.log.dir}"
   pattern="%h %l %u %t "%r" %s %b" prefix="localhost_access_log." resolveHosts="false"
   suffix=".txt"/>
    <Context allowLinking="true" path="/dma" privileged="true" swallowOutput="true"
   useHttpOnly="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." resolveHosts="false"
   suffix=".log"/>
   <Parameter name="com.hp.dma.core.webServiceUrl"
   value="https://hostname.domainname.com:8443/dma"/>
   <Parameter name="com.hp.dma.conn.trustAllCertificates" value="true"/>
   <Parameter name="com.hp.dma.util.AsymmetricEncryptionUtil.FIPSEnabled" value="true"/>
   <Resource aes256="KEK" auth="container" driverClassName="oracle.jdbc.OracleDriver"
   factory="com.hp.dma.util.DmaTomcatContextHandler"
   maxActive="20" maxIdle="20" maxWait="20000" name="jdbc/dma" password="{AES}
   5503ab207080df2ba21c3f299082947511713d35b7b1c65ca6816e5312bc302b"
   type="javax.sql.DataSource" url="jdbc:oracle:thin:@hostname.domainname.com:1521:orca"
   username="dmauser"/>
   ```

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

   ```
   $ service dma start
   ```

   > **Note:** If the value of custom field *SA_REALM* for a given target server is not the same as the SA realm that has the Egress filter configured ("Add a new Egress Filter rule" on page 34) in `/etc/opt/opsware/opswgw-cgws1-<REALM_NAME>/opswgw.custom`, blank out the value for the custom field.

Version 10.50.0001.000 onwards you don't need to specify the SA realm while installing DMA for any new servers added in an SA realm. This functionality is available only to servers added after installing or upgrading to DMA 10.50.001.000.

Create and configure the DMA custom fields

In the 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" on page 32.

To create and configure the custom fields to use proxy communication, perform the following steps:

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" on page 32:
   - Go to **Environment** > **Dashboard** > <*organization_name*> (*Optional:* > <*server_name*>)

     > **Note:** This must be performed by an 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.

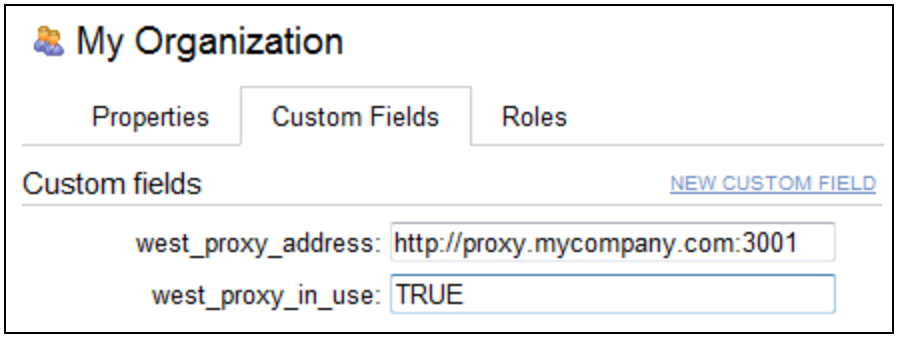
   - Set `west_proxy_address` to the full URL of the proxy, including the port, in the format:

     `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



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

> **Note:** You can easily adjust how the proxy server is 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.

Set the access permissions

This section describes the permission settings to manage DMA, see the Roles, Capabilities, and Permissions topic in the *Planning Guide*.

> **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 DMA. For more information, refer to the *SA Administration Guide*.

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

The following procedure shows you how to set the role-based access permissions. An overview is provided in the Roles, Capabilities, and Permissions topic in the *Planning Guide*.

Grant access permissions to a user or a user group

Perform the following steps to grant permissions to a user or user group:

1. Go to **Setup** > **Permissions**.
2. Select the user or user group to which you want to grant permissions.
3. Go to one of the following 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**.

Grant access permission to a specific workflow

Perform the following steps to grant access permissions to 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.

Specify renamed Windows Administrator user

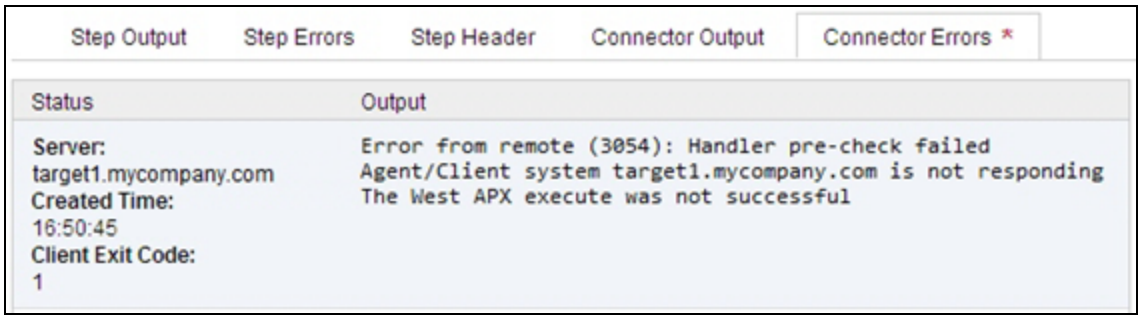
This topic shows you how to make changes necessary to accommodate Windows targets where the Windows Administrator user has been renamed.

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 DMA Automation Platform Extension (APX) to allow non-default Windows Administrator user names. See "Update DMA APX".	On one SA Slice server	Only once
Create and configure a new DMA **Custom Field** that is used to specify the Windows Administrator user name at either the organization or server level. See "Create and configure the DMA Custom Field".	In DMA	Once per relevant organization or server

Instructions for making each of these changes are provided in thise section.

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:



Update 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 Permissions topic in the SA Administration Guide.

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 DMA Custom Field

The final change required is to create and configure an DMA **Custom Field** called `agent_username_win` that contains the Windows Administrator user name for each Windows target server. To create and configure the Custom Field, do the following:

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 by running the following command:

   `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, 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**, DMA uses 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 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 DMA to run workflows on Windows targets as a specific Windows domain user, also see "Run workflows as a Windows domain user" on page 44.

Run 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, you must .Net 3.5 to run a workflow 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 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 the 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 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 a **Custom Field** when the organization or server is open in the **Environment** page by running either of the following commands:

   - `domain_username_win` with type Text
   - `domain_password_win` with type Password

   > **Tip:** If each Windows server requires a different Windows domain user, you must specify this user name for each server.
   >
   > If many Windows servers in the same organization use the same Windows domain user, 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, DMA uses 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 Field**s.

   > **Note:** This must be performed by an 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 specify the renamed Windows Administrator user. For instructions to specify the renamed user, see "Specify renamed Windows Administrator user" on page 41.

Configure 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 in DMA.

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

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

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

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

2. When you make a copy of the workflow, expand the step, and then set the Windows domain user

parameters to **- User selected -**.

> **Note:** The pertinent parameters are based on the solution type:
>
> | | |
> |---|---|
> | Provisioning | Installer Account
Installer Password |
> | Patching, refresh, compliance, and release management | Instance Account
Instance Password |
> | Discovery | SQL Instance Account
SQL Instance Password |

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

> **Note:** If you have renamed the Windows Administrator account on your Windows target servers, you must specify the renamed Windows Administrator user. For instructions to specify the renamed user, see "Specify renamed Windows Administrator user" on page 41.

Change the number of active connections

This topic shows you how to change the number of active database connections that 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. Perform the following steps to change the number of active connections:

1. As the root user, stop the DMA server:

   ```
   $ service dma stop
   ```

2. Open the following file in a text editor:

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

3. Modify the following parameters:

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

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

4. Start the DMA server again:

   ```
   $ service dma start
   ```

Enable FIPS

When you install DMA for the first time, Federal Information Processing Standards 140-2 Level 1 (FIPS) is enabled by default. When you upgrade DMA from a previous version to 10.50.001.000, you must enable FIPS to be FIPS compliant.

Perform the following steps, to enable or disable FIPS, post installation:

1. Stop the DMA server.
2. Change the value of com.hp.dma.FIPSEnabled in server.xml as following:
   - To enable FIPS, com.hp.dma.util.AsymmetricEncryptionUtil.FIPSEnabled=true
   - To disable FIPS, com.hp.dma.util.AsymmetricEncryptionUtil.FIPSEnabled=false
3. Run the `dmaBaseline.sh` as the following example:

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

   $ sh ./dmaBaselineData.sh

   –context /opt/hp/dma/server/tomcat/conf/server.xml

   --overwrite-keys
4. Run `dma_upload.sh` script as the following example:

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

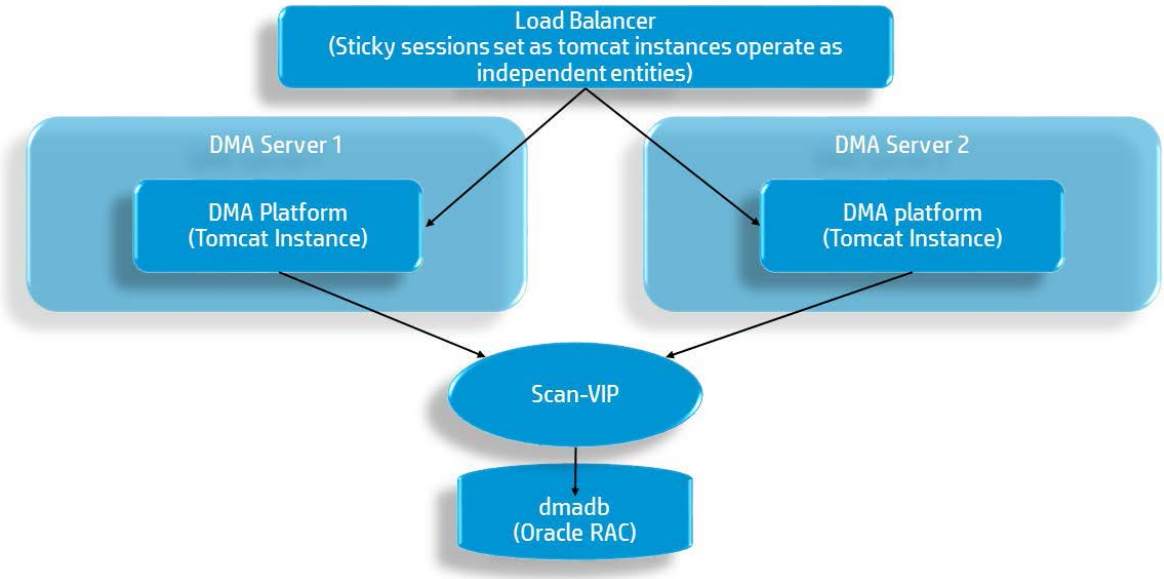
   ```
   $ sh ./dma_upload.sh -host <SA_Server> -user <SA_Policy_User>
    -password <SA_Policy_Password>
    -keyFile /opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/publicKey
    -folderName /DMA_Client
   ```
5. Remediate all the target servers.
6. Start the DMA server.

Configure 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 (DMA).

DMA HA standard architecture solution

The following is an example of HA architecture without DR:



Run the Baseline command on Oracle RAC

To set up the Primary active environment, use these examples to modify the 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:

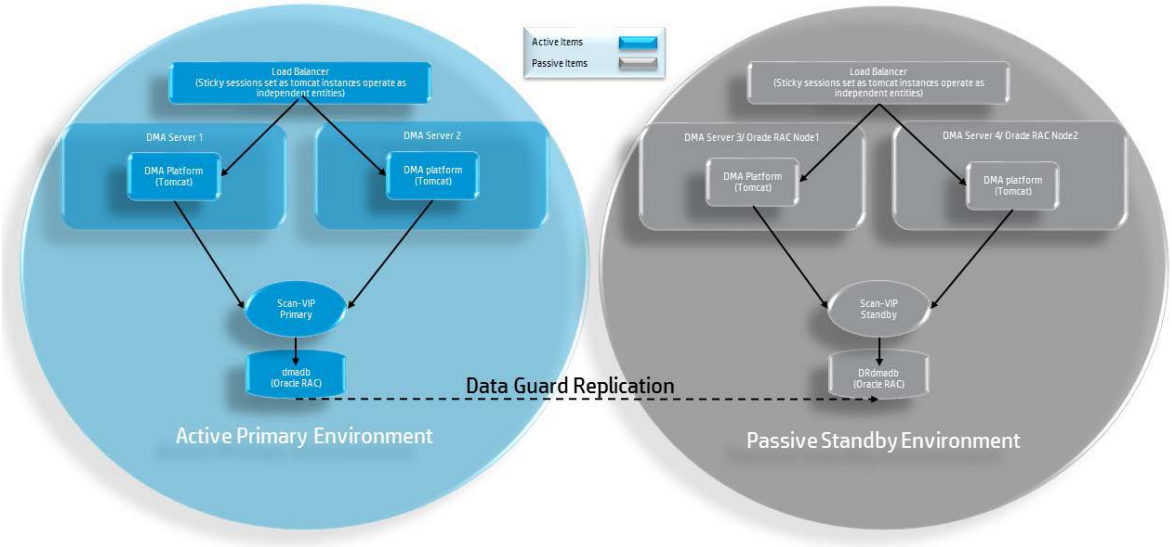
```
sh dmaBaselineData.sh -cc -dbu dma -dbpw dma -dbp 1521 -dbs dmadb
-dbh dma-rac(2/3/4…).company.com -dmah dma-rac(2/3/4…).company.com
-jdbccs jdbc:oracle:thin:@scan-vip.company.com:1522/dmadb.servicename
```

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

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

DMA HA and DR architecture solution (active-passive)

The following is an example of HA architecture with DR (active-passive).



Set up the DMA Server on the standby environment

After you have set up your primary active environment (see DMA HA Standard Architecture Solution), perform the following steps in the passive standby environment (right side of the diagram) to set up the active-passive architecture:

> Note: Perform the steps after you run Baseline commands to set up your Primary active environment. You only need to modify the server.xml files for the standby environment. For more information about Baseline commands, see the DMA baseline options topic in the *Installation Guide*.

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

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

2. On each node, edit the webServiceUrl parameter and the jdbc/dma resource in the server.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/DRdmadb.servicename"
   factory="com.hp.dma.util.DmaTomcatContextHandler" />
   ```

Handle a failover for an active standby environment

In the event of a failover, do the following:

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

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

   > Note: The cancelWorkflow script identifies the workflows that need to be canceled.

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

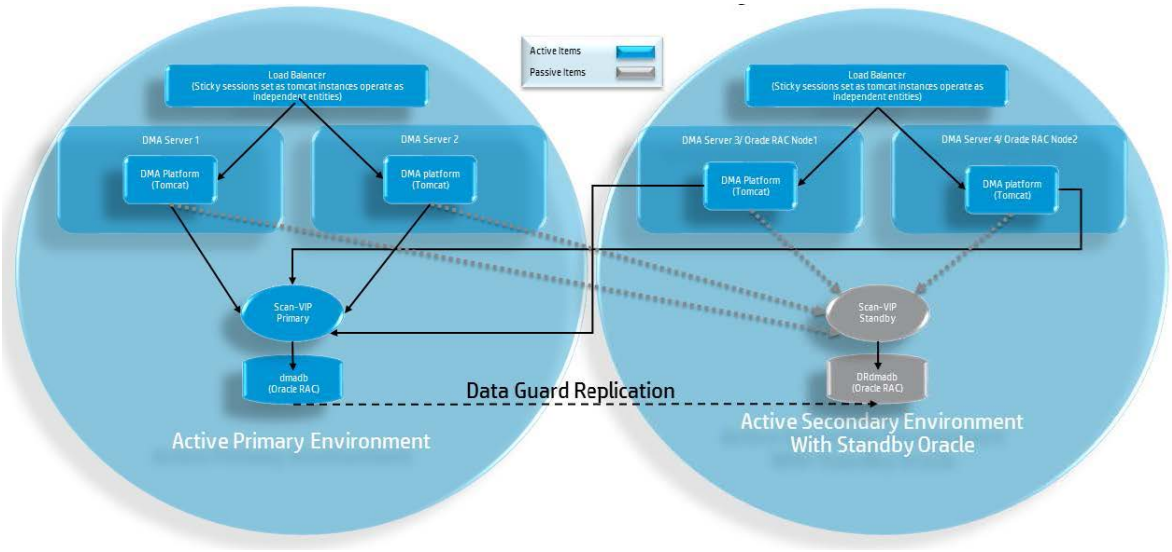
3. Restart the DMA Service by running the following command on all standby DMA Servers:

   ```
   service dma restart
   ```

4. Change the SA slice or gateway of the standby environment:
   a. Log in to the DMA user interface
   b. Navigate to **Setup** > **Connector**
   c. Specify the required connector information

DMA HA and DR architecture solution (active-active Tomcat and active-passive database)

The following is an example o HA architecture with DR (active-active Tomcat and active-passive database).



Set up the DMA Server on the standby environment

After you have set up your primary active environment (see DMA HA Standard Architecture Solution), perform the following 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: Perform the following steps after you run Baseline commands to set up your pPrimary active environment. You only need to modify the server.xml files. For more information about Baseline commands, see the DMA baseline options topic in the *Installation Guide*.

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

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

2. On each node, edit the webServiceUrl parameter in the server.xml file to match the standby environment, for example:

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

Handle a failover when the primary database is lost

If the primary database is lost, perform a failover operations active-active:

1. Execute the Oracle failover operation to change the database from 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 DMA servers:

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

   > Note: The cancelWorkflow script identifies the workflows that need to be canceled.

3. Clean up any targets that had workflows running against them.
4. On all DMA Servers, edit the jdbc/dma resource in the server.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/DRdmadb.servicename"
   factory="com.hp.dma.util.DmaTomcatContextHandler" />
   ```

5. Restart the DMA Service by running the following command on all DMA Servers:

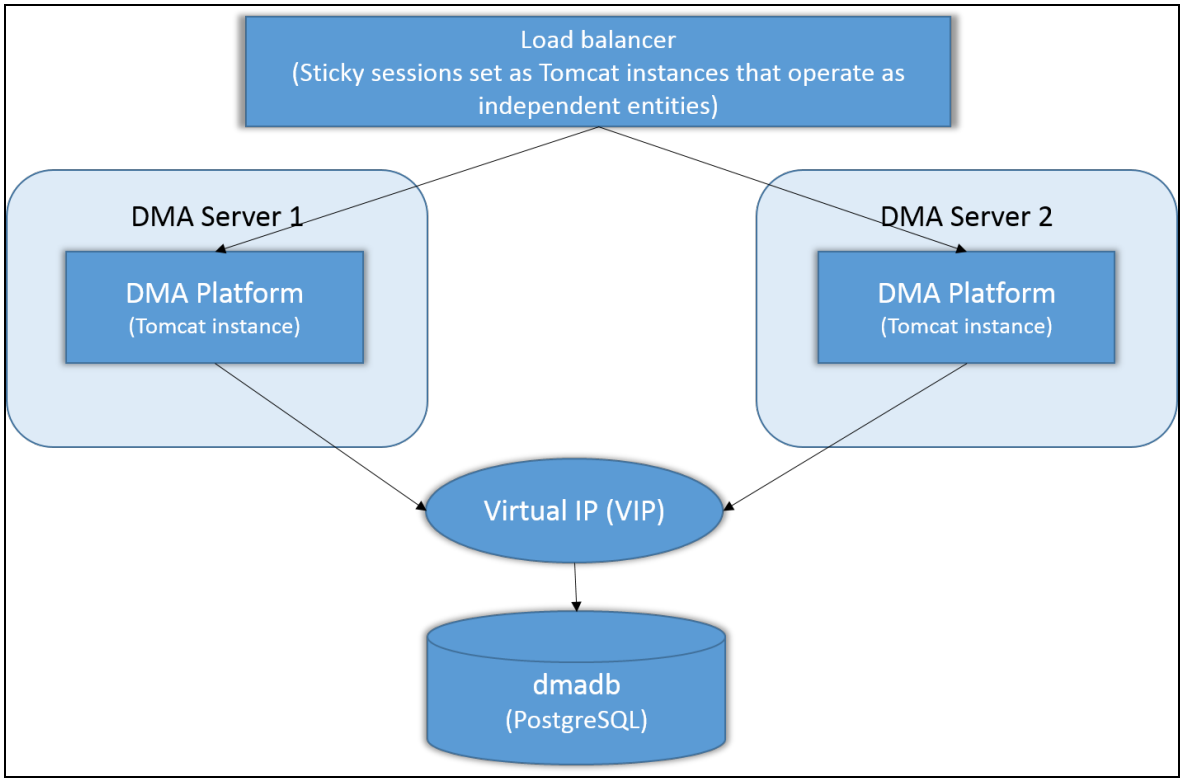
   ```
   service dma restart
   ```

Configuring HADR using PostgreSQL database

This section includes the following topics:

DMA HA standard architecture solution

The following is an example of the HA architecture without DR:



Run the baseline command on PostgreSQL

To set up the primary active environment, use these examples to modify the DMA installation baseline command. For instructions about using the baseline command is described in the Installing the DMA Server section in the *Installation Guide*. To see the full list of baseline options, see "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.

Baseline options

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

Baseline Option	Example Value	Description
-?,--help		Print this usage message.
-c,--create-tables		Create tables for database.
-cc,--create-context		Create a context file with the specified settings.
-context,--deployed-context-file <server.xml>	server.xml	Fully qualified path to the deployed context file to get database connection settings.
-dbh,--database-hostname <arg>	postgres.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.

Baseline Option	Example Value	Description
-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/postgres/dma	The base directory for the database tablespace creation.
-dbtype,--database-type <arg>	postgres	(optional) The underlying database type. The default is postgres.
-dbu,--database-username <dbusernameValue>		The username used to connect to the database.
-dmah,--dma-hostname <dmahostnameValue>	dma.mycompany.com	Set the fully qualified host name of the DMA server. 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. Do not do this unless instructed to by Software Support.

How to run the Baseline Command on PostgreSQL

To set up the primary active environment, use these examples to modify the DMA installation baseline command. How to use the baseline command is described in “Install the DMA Server” section in the DMA Installation Guide available at https://softwaresupport.softwaregrp.com/. To see the full list of baseline options, see the DMA baseline options topic in the *Installation Guide*.

1. Change your directory:

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

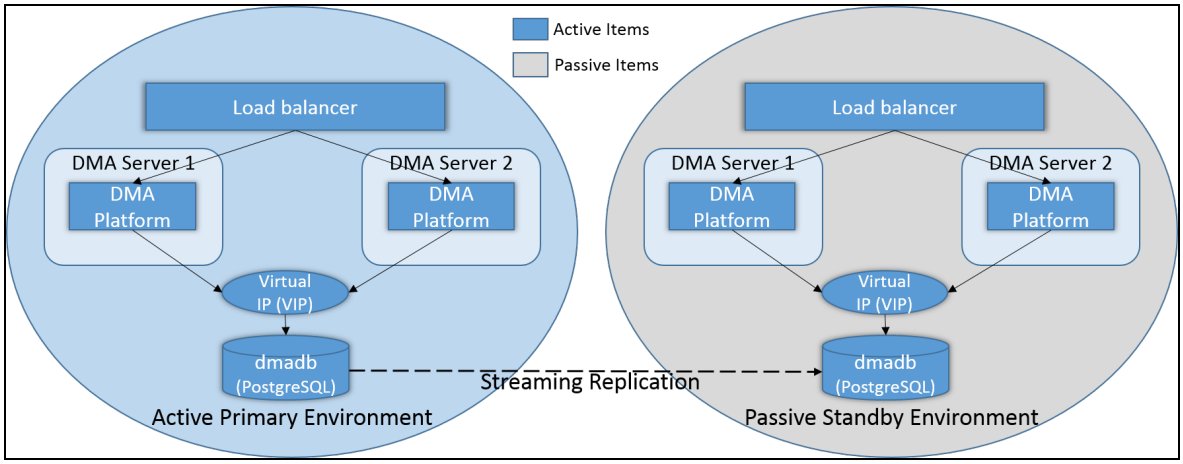
2. Run the baseline command on the primary node of PostGRESQL:

   ```
   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.

DMA HA and DR architecture solution (active-passive)

The following is an example of the HA architecture with DR (active-passive).



Set up the DMA Server on the passive standby environment

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

> **Note:** Perform the steps after you run the baseline commands to set up your primary active environment. You only need to modify the **server.xml** files for the standby environment.

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

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

2. On each node, edit the webServiceUrl parameter and the JDBC/DMA resource in the **server.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"/>
```

Handle failover for an active standby environment

In the event of a failover, perform the following:

1. Run the following script to cancel the workflows that were running when the failure occurred, on any of the Standby 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 **server.xml** file:
   - testOnBorrow="true"
   - removeAbandoned="true"
   - timeBetweenEvictionRunsMillis="5000"
   - minEvictableIdleTimeMillis="5000"
   - minIdle="0"

   The application attempts to reconnect to the datasource after restarting the database.

How to set up 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 `server.xml` files for the standby environment. For more information on the server.xml file, see HPE DMA Installation Guide available at http://h20230.www2.hp.com/selfsolve/manuals.

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

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

2. On each node, edit the webServiceUrl parameter and the JDBC/DMA resource in the server.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
   ```

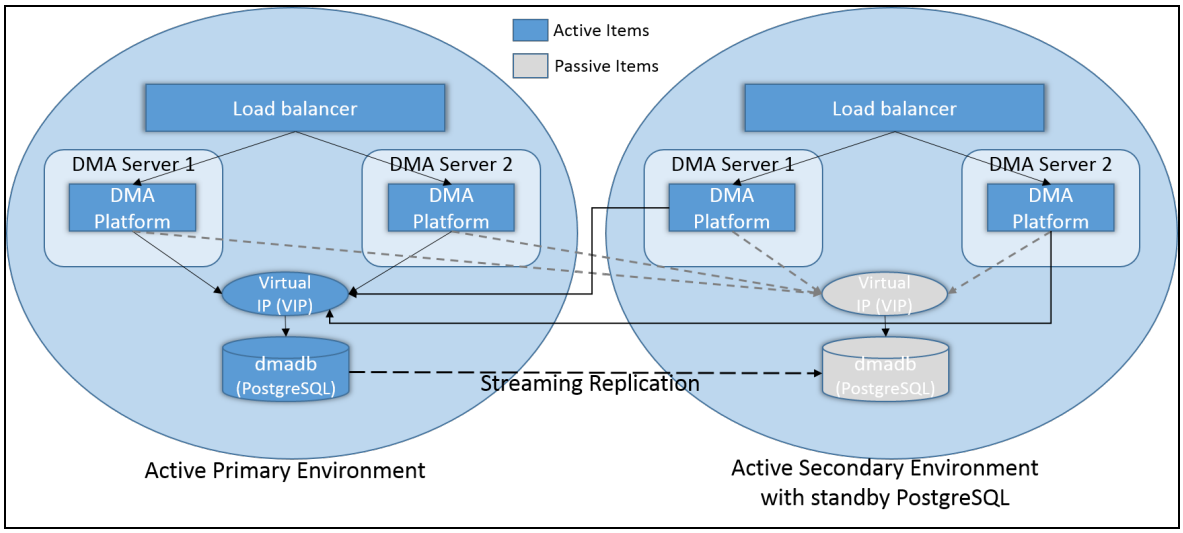
2. Clean up any targets that may have had workflows running against them.

3. Change the values for the following parameters in the server.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.

DMA HA and DR architecture solution (active-active Tomcat and active-passive database)

The following is an example of the HA architecture with DR (active-active Tomcat and active-passive database).



Set up the DMA Server on the active standby environment

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

> **Note:** Perform the steps after you run the baseline commands to set up your primary active environment. You only need to modify the `server.xml` files for the standby environment.

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

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

2. On each node, edit the webServiceUrl parameter in the server.xml file to match the standby environment:

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

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. Run the following script to cancel the workflows that were running when the failure occurred, on any of the Standby DMA servers:

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

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

   The application attempts to reconnect to the datasource after restarting the database.

How to set up 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 `server.xml` files for the standby environment. For more information on the server.xml file, see HPE DMA Installation Guide available at http://h20230.www2.hp.com/selfsolve/manuals.

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

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

2. On each node, edit the webServiceUrl parameter in the server.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 server.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.

Replicate data

To help Database and Middleware Automation (DMA) extend across broader geographical regions, you can build multiple DMA servers and use Oracle Streams replication between those servers. This ensures that your DMA solution packs, policies, and deployments, all 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 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 following:
  - 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 set up and is running as the DMA server.
- The schema for the 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 thefollowing 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 takes some time to complete, and the time varies 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 DMA user that you have configured and run the following script to initialize the quartz tables that handle scheduling for DMA.

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

Example 2 – Second database is used only for read operations

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 set up and is running as the DMA server.
- The schema for the 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 thefollowing 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 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.

Run 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. Perform the following steps to run a bridged 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 **Automatio**n > **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 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

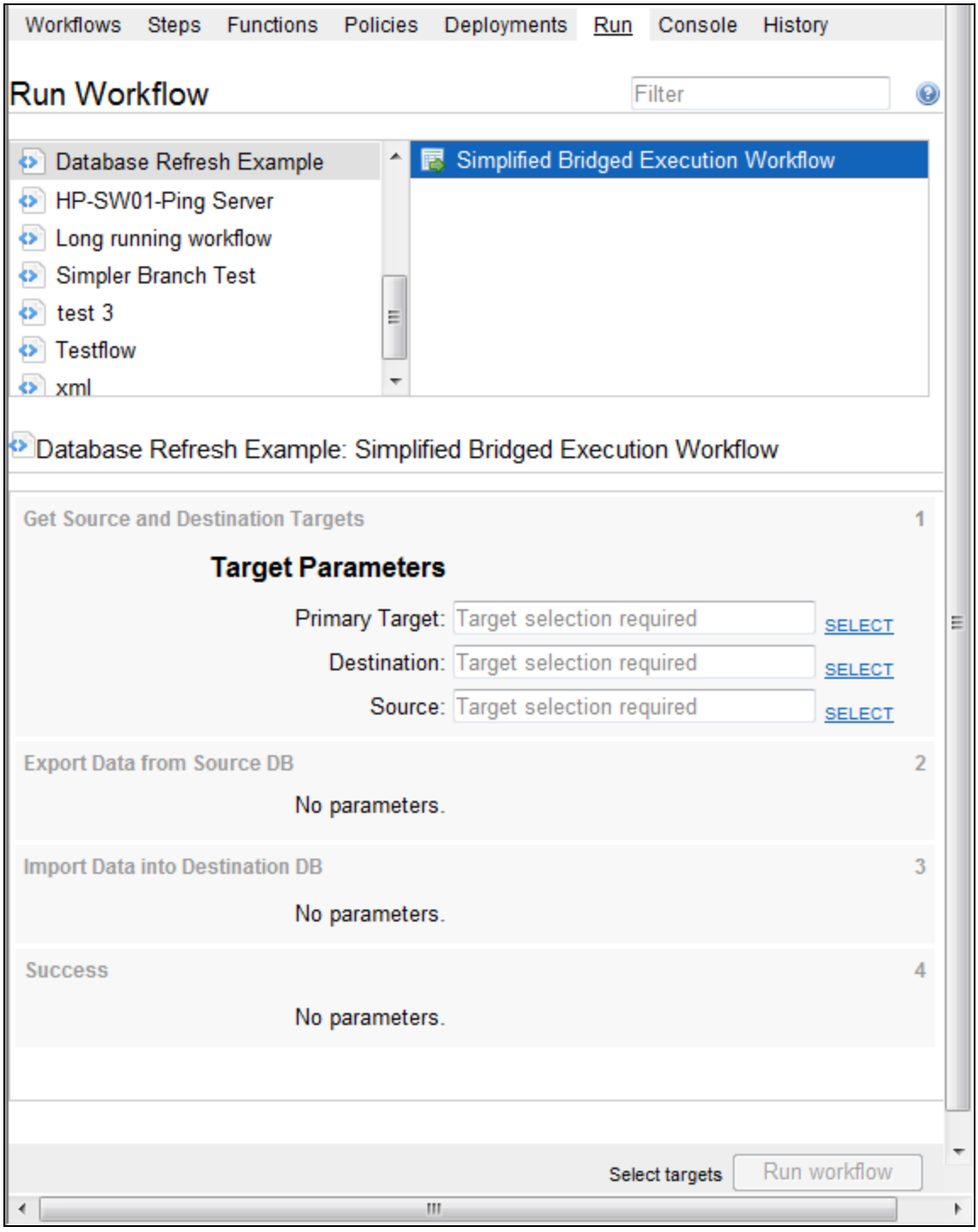
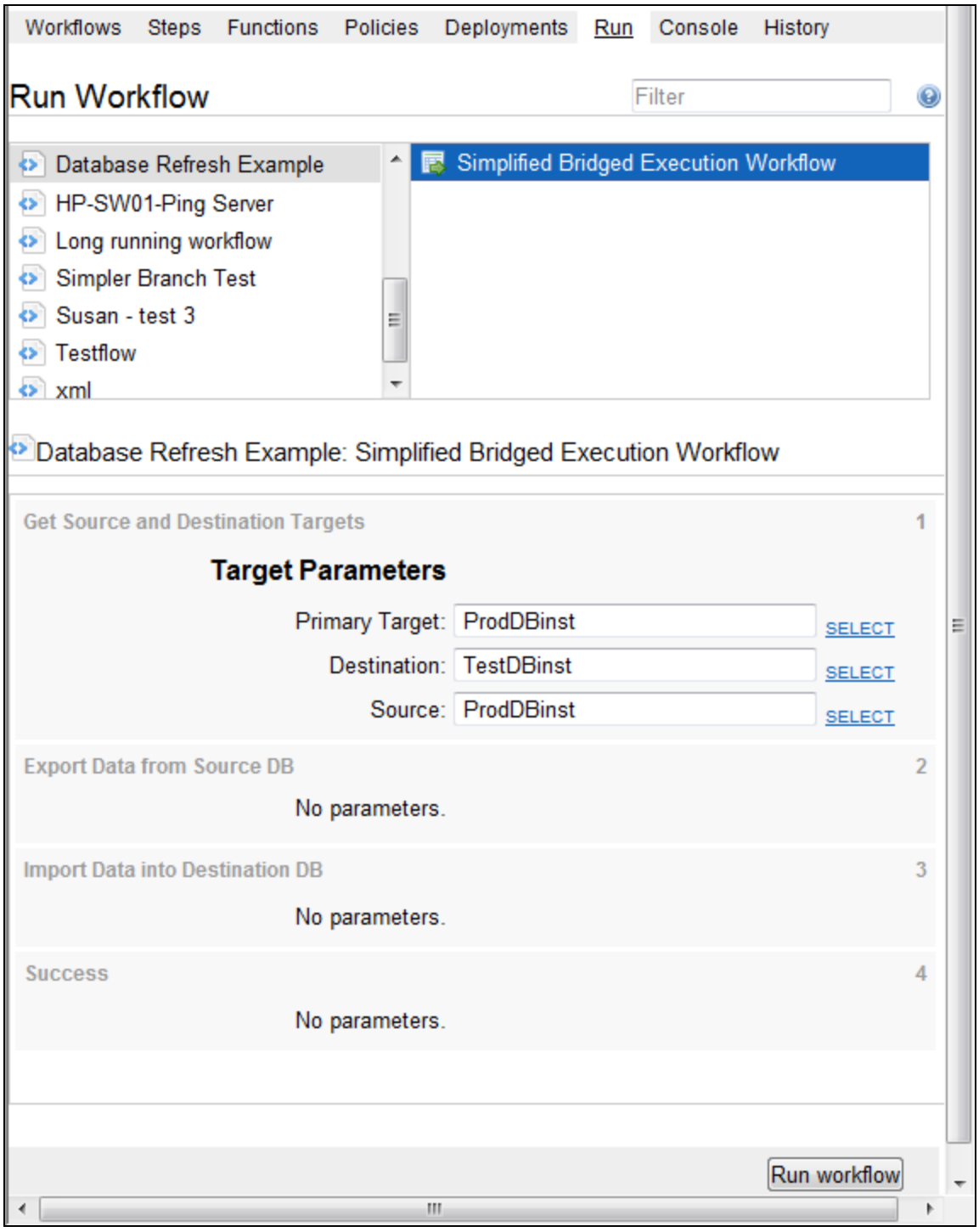


Figure: Run Page AfterTarget Selection


Workflows
Steps
Functions
Policies
Deployments
Run
Console
History
Run Workflow
Filter
Database Refresh Example
HP-SW01-Ping Server
Long running workflow
Simpler Branch Test
Susan - test 3
Testflow
xml
Simplified Bridged Execution Workflow
Database Refresh Example: Simplified Bridged Execution Workflow
Get Source and Destination Targets
1
Target Parameters
Primary Target:
ProdDBinst
SELECT
Destination:
TestDBinst
SELECT
Source:
ProdDBinst
SELECT
Export Data from Source DB
2
No parameters.
Import Data into Destination DB
3
No parameters.
Success
4
No parameters.
Run workflow

Additional considerations

An 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

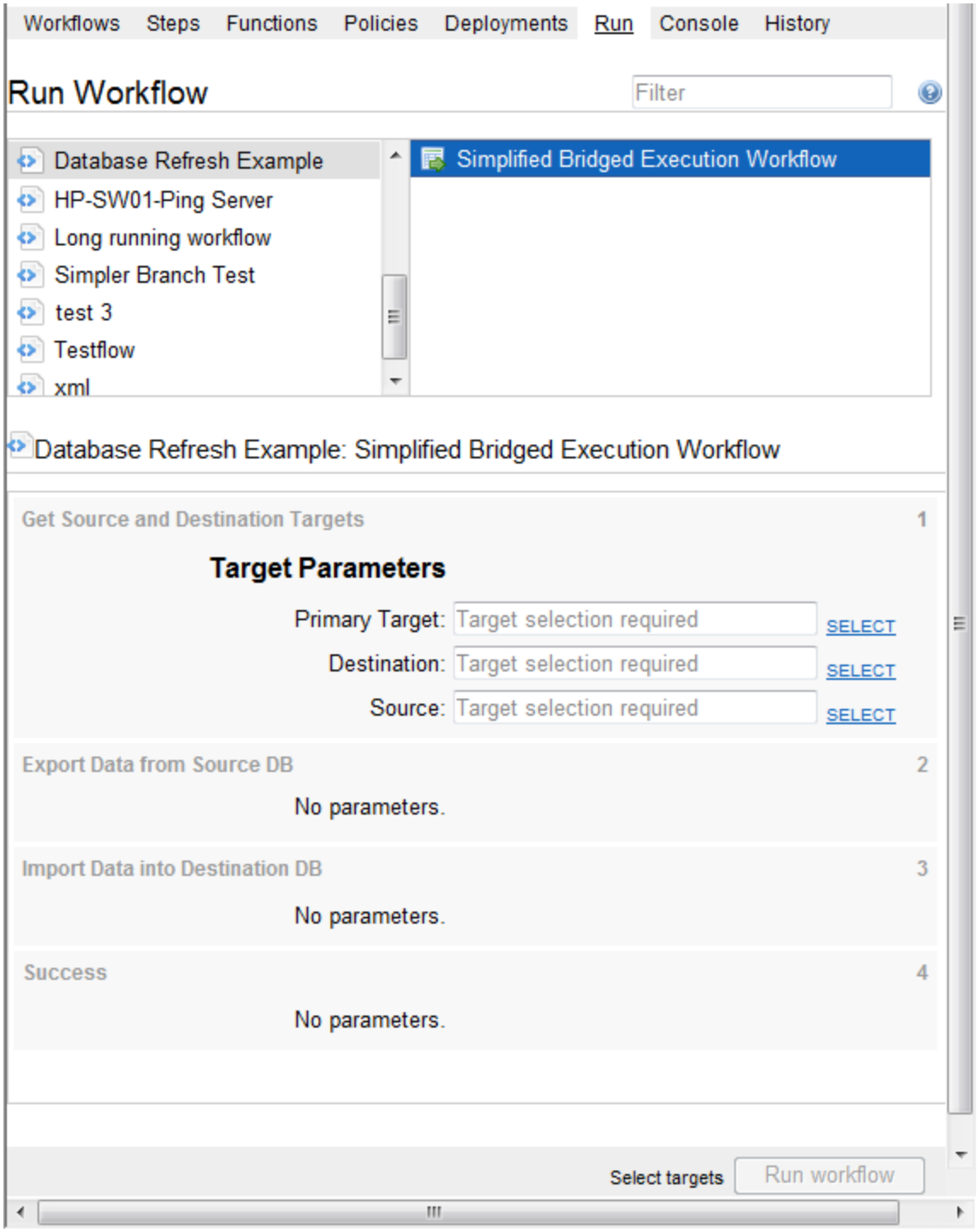
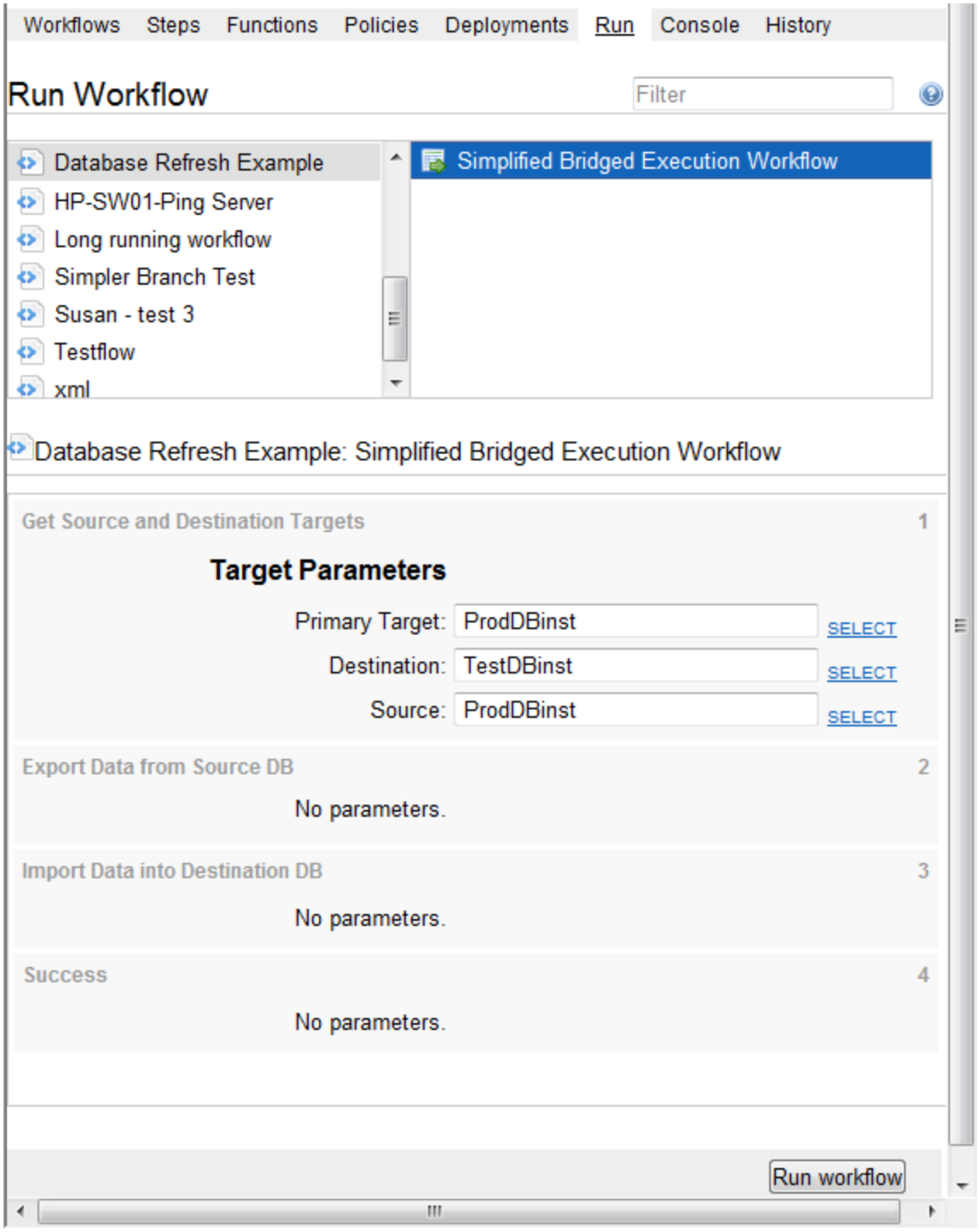


Figure: Run Page AfterTarget Selection



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.

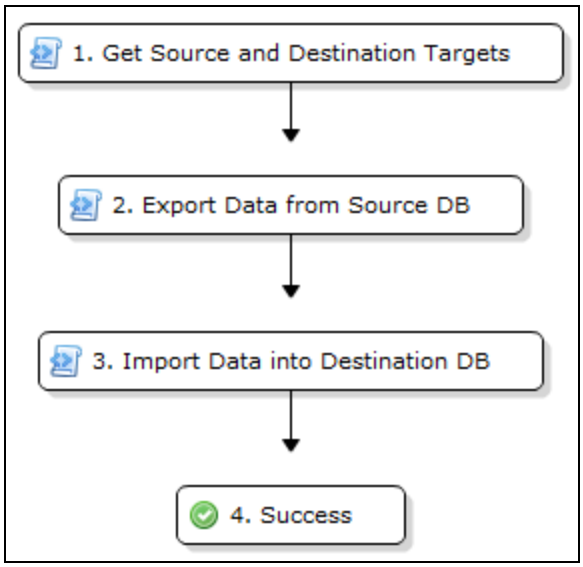
Workflow

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 are exported.
- The Destination target is the database instance where those contents are imported.

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

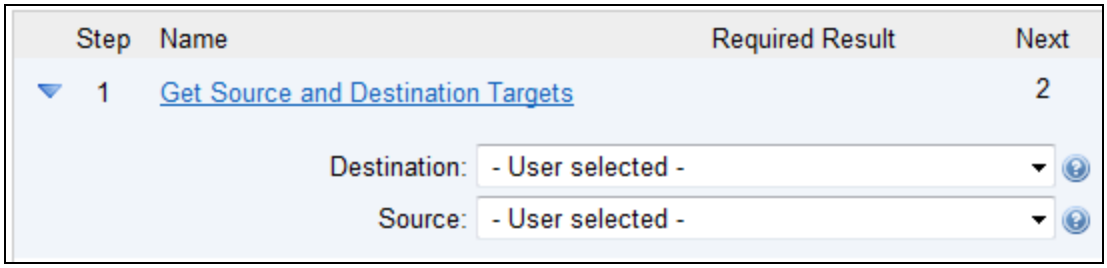
All targets for a bridged execution workflow must have the same target level (Server, Instance, or Database) as the workflow itself. In this example, the target level is Instance.



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.



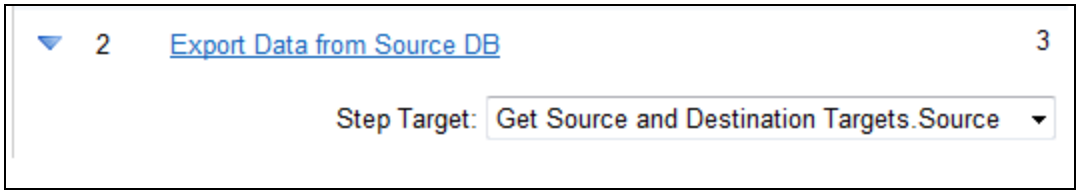
Both input parameters must be set to **- User selected -** in the workflow.

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.

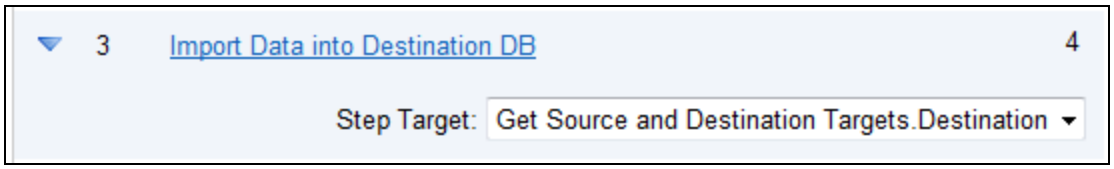
Export Data from Source DB

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.



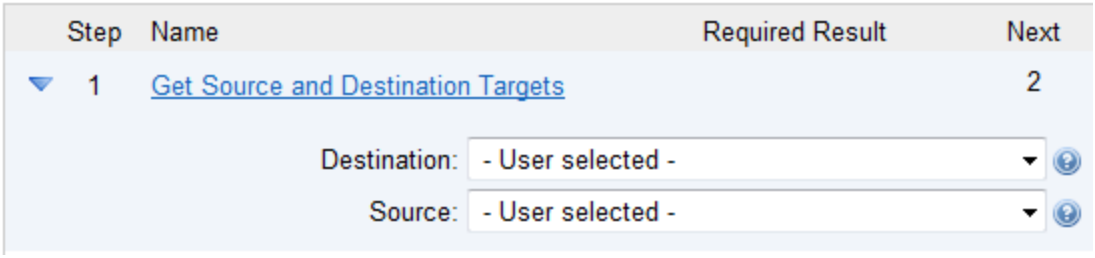
Importing Data into Destination DB

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.



Obtain 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.



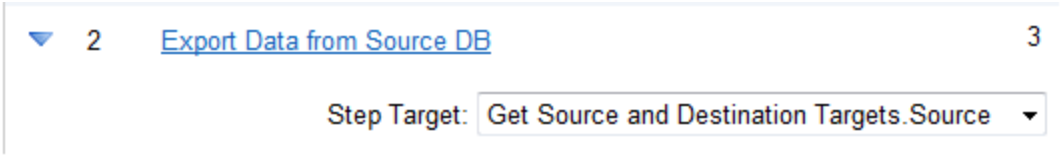
Both input parameters must be set to - User selected - in the workflow.

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.

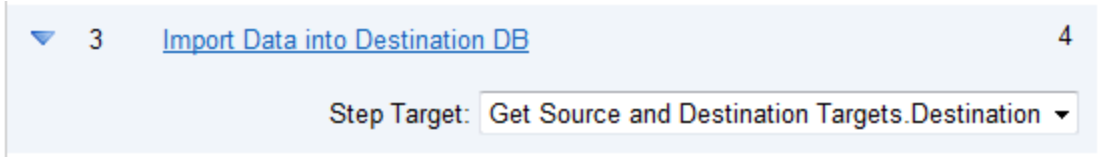
Export Data from Source DB

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.



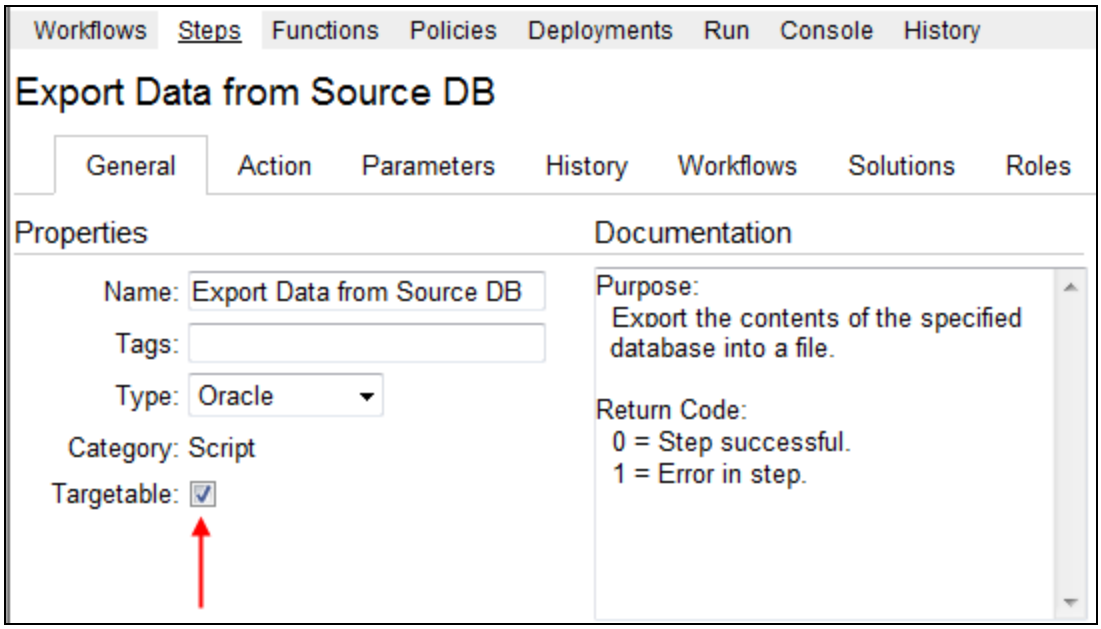
Import Data into Destination DB

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.

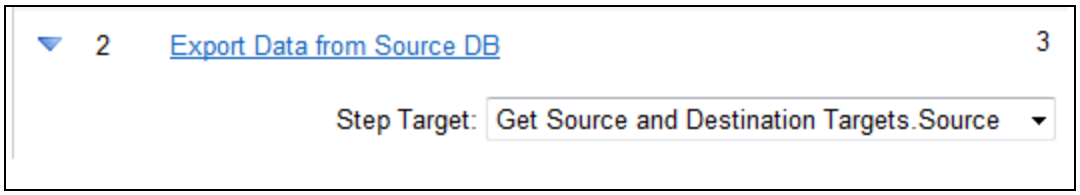


Targetable Steps

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.



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 box 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.

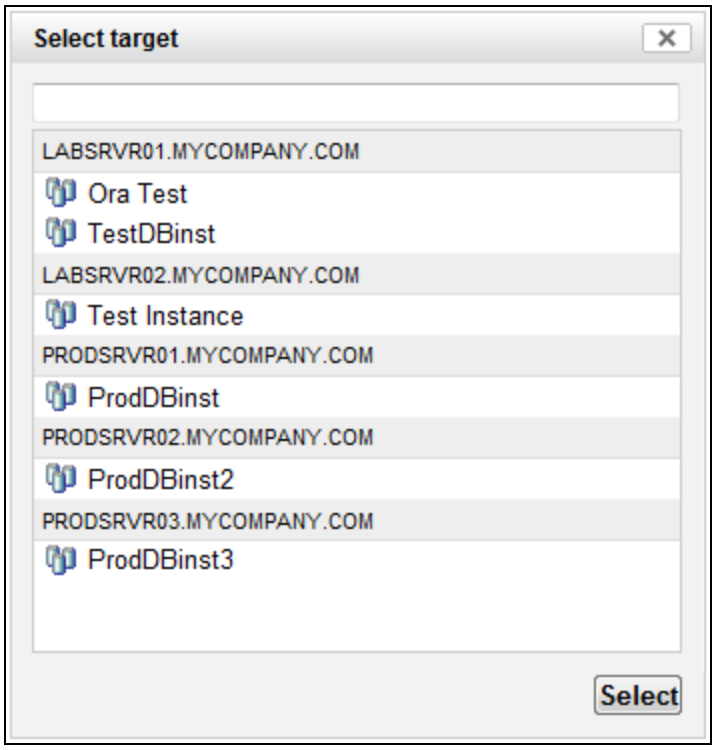
Run

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 **Run workflow** is disabled.

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

Import a file into the software repository

Many workflows are capable of downloading files from the software repository on the 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.

DMA uses the 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** > **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 *Server Automation Single-Host Installation Guide*.
2. In the navigation pane in the SA Client, select **Library** > **By Folde**r.
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 box, click **Browse** to the right of the **File(s)** box.
6. In the **Open** dialog box:
   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 box 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, do the following:
   a. Click **Browse** 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 box 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.

DMA version history

The DMA version history is a command line utility that displays the history of DMA Server RPMs, Client RPMs, and Solution Packs that you installed or upgraded. The file `dmaVersionHistory.sh` is located at **/opt/hp/dma/server/tomcat/webapps/dma/WEB-INF**.

The following table provides the list of the dmaVersionHistory.sh options:

Option	Description
-?,--help	Print this usage message.
-all	Print version history for Server, Client RPM & Solution Packs
-c,--client	Print version history for client RPM only
-context,--deployed-context-file <*context*>	Path to context file
-e,--erase	Erase Version history for the presently logged in server
-eh,--eraseforhost	Erase Version history for the hostname passed in as value for "-h" parameter
-eraseall	Erase complete Version history
-h,--hostname <*h*>	Erase Version history for particular hostname
-s,--server	Print version history for server RPM only
-sp,--solutionpack	Show Solution Pack History

The following are a few examples of the DMA Version History command line utility:

- To view history for both RPM and Solution Pack:

  ```
  sh dmaVersionHistory.sh –context <path_to_context_file> -all
  ```

- To view RPM history(client and server):

  ```
  sh dmaVersionHistory.sh –context <path_to_context_file>
  ```

- To view only client history:

  ```
  sh dmaVersionHistory.sh –context <path_to_context_file> --client
  ```

- To view only server:

  ```
  sh dmaVersionHistory.sh –context <path_to_context_file> --server
  ```

- To view Solution pack history:

```
sh dmaVersionHistory.sh –context <path_to_context_file> --solutionpack
```

You can delete the history of RPMs based on the hostname. For example:

- To delete the RPM history of the currently logged in server:

```
sh dmaVersionHistory.sh –context <path_to_context_file> --erase
```

- To delete the history of a particular hostname:

```
sh dmaVersionHistory.sh –context <path_to_context_file> --eraseforhost –h
<hostname>
```

- To delete complete history:

```
sh dmaVersionHistory.sh –context <path_to_context_file> -eraseall
```

> **Note:** You cannot delete Solution Pack history.

Maintenance

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

- "Reset the DMA Initial Admin password" below

  Reset the password for the DMA Initial Admin (dma_initial_admin) account.

- "Update the self-signed SSL certificate" on page 89

  Generate a new self-signed SSL certificate and distribute your certificate to your managed servers.

Reset the DMA Initial Admin password

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

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

If you want to obtain the online help, run the following command on the 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 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 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, the following message is displayed:

```
Successfully updated the dma_intial_admin password.
```

If the password is not reset successfully, the following message is displayed:

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

Update 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 helpful when you have to update your certificate when it expires. This section includes:

- "Update self-signed SSL certificate on the DMA Server"
- "Update self-signed SSL certificate on the DMA Client" on page 93

Update self-signed SSL certificate on the DMA Server

Perform the following steps to update the self-signed SSL certificate on the DMA Server :

1. Stop DMA:

   ```
   # service dma stop
   ```

2. To list the certificates, execute the following command (all in one line):

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

   For example (with the default 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 are similar to the following:

   ```
   [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 in one line):

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

   For example (with the default 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 are similar to the following:

   ```
   [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 in one line):

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

   For example (with the default 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 are similar to the following:

   ```
   [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 in 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 "Use a proxy server" on page 28.

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 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.
<keyalias>	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`.
<password>	The password for both the keystore and this private key.
<storefile>	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.

6. 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 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:#
```

7. Start DMA:

   ```
   # service dma start
   ```

8. Using the browser, log in to DMA.

Update self-signed SSL certificate on the DMA Client

Before you update the self-signed SSL certificate, you must verify if your DMA Server trusts all certificates. To verify, do the following:

1. Open the `server.xml` file located on the DMA server at:

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

   > **Note:** You do not need to stop and restart the DMA Server unless you change the value of `trustAllCertificates` in the file.

2. Search for `trustAllCertificates`:

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

   If the <*value*> is true, the DMA Server trusts all certificates. If the <*value*> is false the Server, does not trust all certificates.

Perform either of the following steps based on the <*value*> you got in the verification step:

Value of trustAllCertificates	Instructions
true	"When trusting all certificates"
false	"When not trusting all certificates"

When trusting all certificates

The DMA Clients can be set to trust any certificate coming from the DMA Server. This is the default setting.

> **Note:** When trusting all SSL Certificates, there is no need to import the certificates to the DMA Client. Updating the SSL Certificate on the DMA Server is enough for the Clients to work. No changes are required on the DMA Clients.

When not trusting all certificates

You can set the DMA CLients to not trust all certificates from the DMA Server. When this is the case, the certificate sent from the DMA Server to the DMA Client needs to be validated against the certificates that are trusted.

To enable DMA to use a self-signed SSL Certificate for WEST to communicate with the DMA Server, you must add the certificate to the client as a trusted certificate. To do this for all clients, create an SA policy following the instructions in "Add the certificate to UNIX targets" and "Add the certificate to Windows targets".

To enable DMA to use a self-signed SSL certificate for WEST to communicate with the DMA Server, the certificate needs to be added to the client as a trusted certificate. To do this for all clients, create an SA policy following the instructions in "Add the certificate to UNIX targets" and "Add the certificate to Windows targets".

Add the certificate to UNIX targets

Add the certificate to the UNIX targets after the new certificate is applied to the DMA Server (see "Update self-signed SSL certificate on the DMA Server").

1. Open a browser and export this certificate to <*download location*>. The steps required depends on your browser.

   Example for the Firefox browser:

   - Go to **Open menu** () > **Options** > **Certificates** > **View Certificates**> **Servers**
   - Scroll down to <*company_name*> and <*dma_server_name*>
   - Click **Export**
   - Save the certificate to <*download location*> with file extension CRT.

2. Zip the certificate file into a file named `cert_file_unix.zip`.
3. Launch the SA Client from the **Windows Start Menu**.

   By default, the HP SA Client is located in **Start** > **All Programs** > **HP Business Service Automation** > **Server Automation Client**

4. Upload the ZIP file as a package to SA:
   a. In the navigation pane in the SA Client, select **Library** > **By Folder**.
   b. Select or create the folder where you want to store the file.
   c. From the Actions menu, select **Import Software** and then browse to the certificate ZIP file.
   d. Click **Import**.
   e. Click **Close** after the import is completed.
5. Create a new software policy that is applicable to UNIX:

a. Right-click the certificate that you just uploaded, and then select **New** > **Software Policy**.

b. Add `cert_file_unix.zip` as the package.

c. Select UNIX as the applicable OS for the ZIP file.

d. Specify `/opt/hp/dma/client/java_certs` as the default install path.

e. Under Install Scripts for the package, add the following lines as Post-Install Scripts (all in single lines):

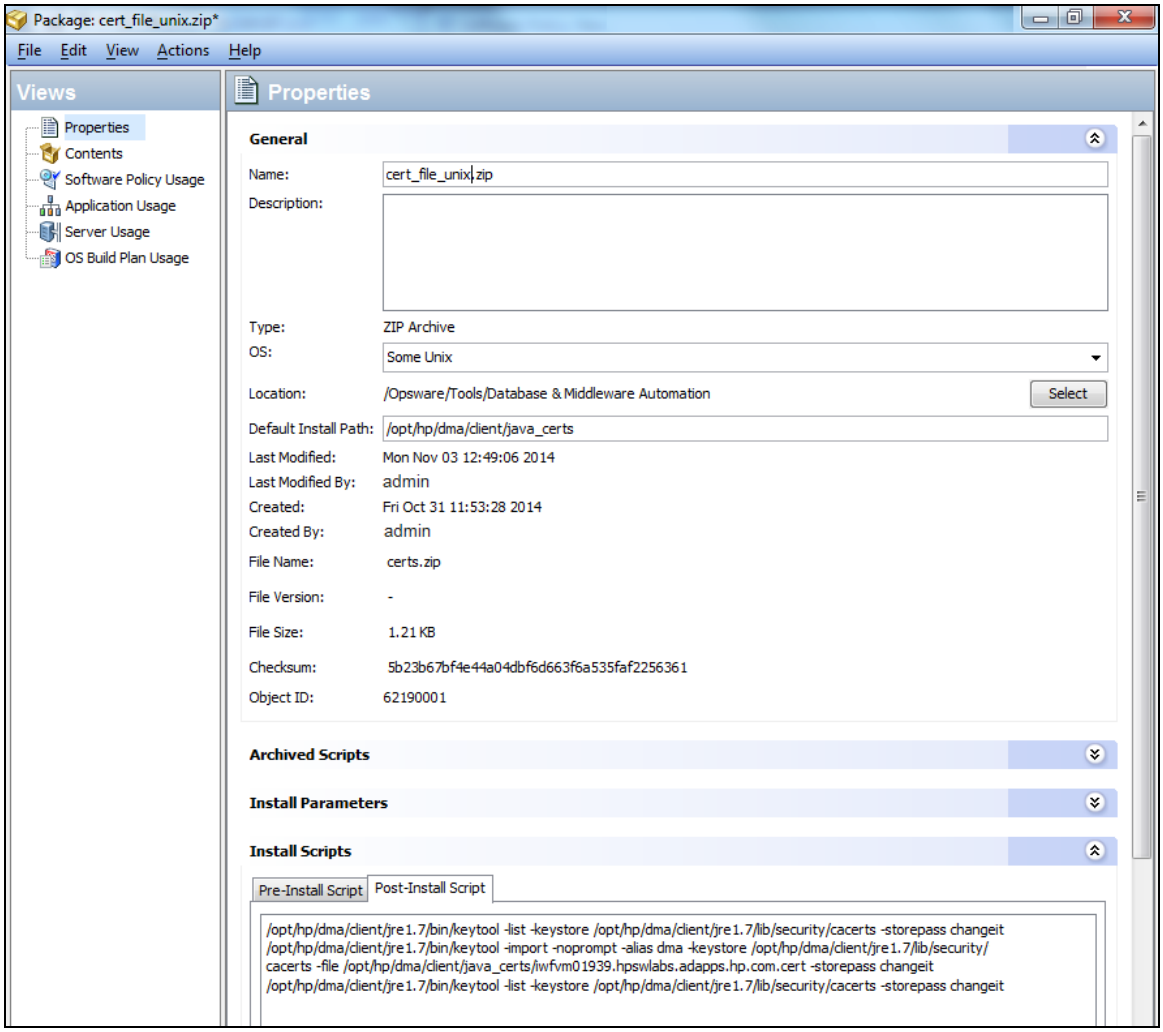
```
/opt/hp/dma/client/jre1.7/bin/keytool -list -keystore /opt/hp/dma/client/
jre1.7/lib/security/cacerts -storepass <password>
```

```
/opt/hp/dma/client/jre1.7/bin/keytool -import -noprompt -alias dma
-keystore /opt/hp/dma/client/jre1.7/lib/security/cacerts -file /opt/hp/
dma/client/java_certs/<certificate file name> -storepass <password>
```

```
/opt/hp/dma/client/jre1.7/bin/keytool -list -keystore /opt/hp/dma/client/
jre1.7/lib/security/cacerts -storepass <password>
```

> **Note:** Here, <*certificate file name*> is the name of the certificate file inside the ZIP file and not the ZIP file itself and <*password*> is the appropriate password (the default is `changeit`).

For example:



6. Apply this software policy on the UNIX devices.
7. Verify that this job has no failures. The post install message should say: Certificate was added to keystore.
8. Run the DMA workflows.

Add the certificate to Windows targets

Add the certificate to the Windows targets after the new certificate is applied to the DMA Server (see "Update self-signed SSL certificate on the DMA Server").

1. Open a browser and export this certificate to <*download location*>. The steps required depends on your browser.

Example for the Firefox browser:

- Go to **Open menu** () > **Options** > **Certificates** > **View Certificates**> **Servers**
- Scroll down to <*company_name*> and <*dma_server_name*>
- Click **Export**
- Save the certificate to <*download location*> with file extension CRT.

2. Zip up the certificate file into a file named `cert_file_win.zip`.
3. Launch the SA Client from the **Windows Start Menu**.

   By default, the SA Client is located in **Start** > **All Programs** > **HP Business Service Automation** > **Server Automation Client**

   > **Note:** If theSA Client is not installed locally, follow the instructions under "Installing the SA Client Launcher" in the Server Automation User Guide.

4. Upload the ZIP file as a package to SA:
   a. In the navigation pane in the SA Client, select **Library** > **By Folder**.
   b. Select (or create) the folder where you want to store the file.
   c. From the Actions menu, select **Import Software** and then browse to the certificate ZIP file.
   d. Click **Import**.
   e. Click **Close** after the import is completed.
5. Create a new software policy that is applicable to Windows:
   a. Right-click the certificate that you just uploaded, and then select **New** > **Software Policy**.
   b. Add `cert_file_win.zip` as the package.
   c. Select **Windows** as the applicable OS for the ZIP file.
   d. Specify `%SystemDrive%\Program Files\HP\DMA\Client\java_certs` as the default install path.
   e. Under Install Scripts for the package, add the following lines as Post-Install Scripts (all on single lines):

   ```
   cd "%SystemDrive%\Program Files\HP\DMA\Client\jre1_7\bin"
   ```

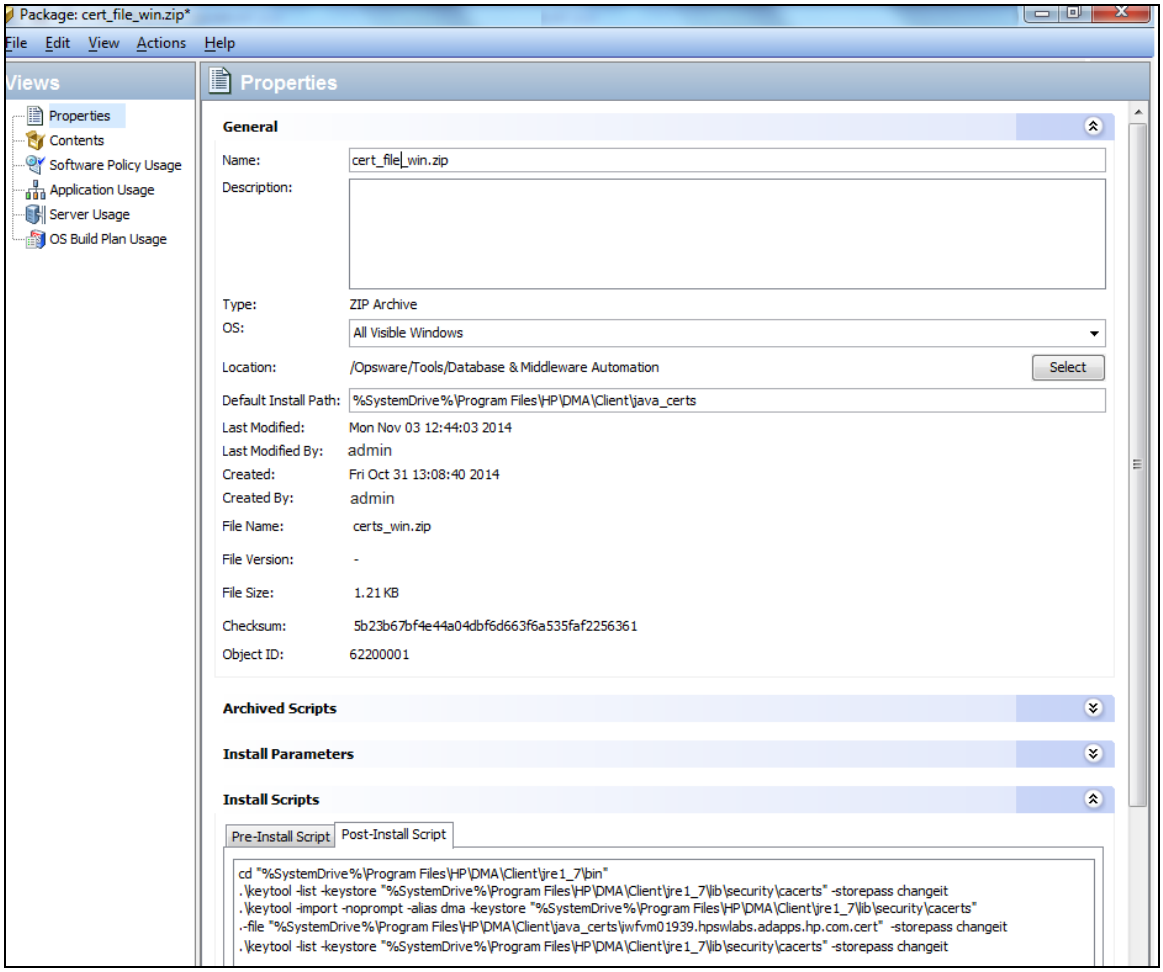
   ```
   .\keytool -list -keystore "%SystemDrive%\Program Files\HP\DMA\Client\jre1_
   7\lib\security\cacerts" -storepass <password>
   ```

```
.\keytool -import -noprompt -alias tomcat -keystore "%SystemDrive%\Program
Files\HP\DMA\Client\jre1_7\lib\security\cacerts" -file
"%SystemDrive%\Program Files\HP\DMA\Client\java_certs\<certificate file
name>"  -storepass <password>

.\keytool -list -keystore "%SystemDrive%\Program Files\HP\DMA\Client\jre1_
7\lib\security\cacerts" -storepass <password>
```

> **Note:** Here, *<certificate file name>* is the name of the certificate file inside the ZIP file and not the ZIP file itself and *<password>* is the appropriate password (the default is `changeit`).

For example:



6. Apply this software policy on the Windows devices.
7. Verify that this job has no failures. The post install message should say: Certificate was added to keystore.

8. Run the DMA workflows.

Delete an SSL Server Certificate

You may find it necessary at some point to delete a certificate from the keystore–for example, if the certificate expires or is revoked by the Certificate Authority (CA).

A certificate should be revoked under any of the following circumstances:

- The private key is lost.
- The private key is compromised.
- The certificate contains incorrect or outdated information.

A revoked certificate immediately becomes invalid. It cannot be renewed, re-keyed, or re-issued.

If your DMA server certificate expires, is revoked, or otherwise becomes invalid, you must remove it from the keystore and replace it with a valid certificate.

You can delete a certificate from the DMA server keystore by using the `keytool` utility.

To delete the server certificate from the DMA server keystore:

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

   ```
   keytool -delete -alias <keyalias> -keystore <storeFile> -keypass <password>
   ```

   Here, *<keyalias>* is the alias associated with the DMA server's private key (`tomcat`), *<storeFile>* is the file that contains the keystore, and *<password>* is the keystore password.

   For example:

   ```
   keytool -delete -alias tomcat -keystore /opt/hp/dma/server/.keystore
   -storepass mypassword
   ```

3. Repeat step 2 for each client server where this certificate was installed (see the Configure SSL on the DMA Server topic in the *Installation Guide*). In this case, specify the client server keystore file and password. For example:

   ```
   keytool -delete -alias tomcat -keystore
   /opt/hp/dma/server/java/lib/security/cacerts -storepass changeit
   ```

4. Install a valid server certificate on the DMA server and all client servers.

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 10.50.001.000)

Just add your feedback to the email and click send.

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

We appreciate your feedback!