

HP Database and Middleware Automation

For Red Hat Enterprise Linux

Software Version: 10.01

Administrator Guide

Document Release Date: April 2013

Software Release Date: April 2013



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2010 - 2013 Hewlett-Packard Development Company, L.P.

Trademark Notices

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

Oracle® is a registered trademark of Oracle and/or its affiliates..

UNIX® is a registered trademark of The Open Group.

Support

Visit the HP Software Support Online web site at:

<http://www.hp.com/go/hpssoftwaresupport>

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

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

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

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

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

To find more information about access levels, go to:

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

Documentation Updates

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

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

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

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

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

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

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

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

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

Document Changes

Chapter	Version	Changes
Special Configurations	10.01	Added the following new topics: <ul style="list-style-type: none"> • Use a Proxy Server with HP DMA • Specify a Renamed Windows Administrator User • Run as a Windows Domain User • Change the Number of Active Connections
Targets	10.01	Added information about administering Custom Fields and Smart Groups.

Contents

Contents	5
Audience	7
Document Map	8
Important Terms	9
Additional Resources	10
Connector	11
Roles, Permissions, and Capabilities	13
Roles	14
Capabilities	16
Permissions	17
Types of Users	19
Targets	22
Organizations	22
Servers	23
Custom Fields	24
Smart Groups	25
Policies	26
Discovery	28
Solution Packs	29
Install a Solution Pack	29
Versioning and Importing Solution Packs	32
Modify a Solution Item	32
Roll Back a Solution Pack	33
Delete a Solution Pack	34
Mail Settings	35
Special Configurations	36
Change the Default Port	37

Use a Proxy Server with HP DMA	38
Default HP DMA Communications	38
Using an SA Satellite as a Proxy Server	39
How HP DMA Manages Proxy Communication	40
How to Set Up a Proxy Server	41
Add a New Egress Rule	41
Add and Configure the HP DMA Custom Fields	42
Run as a Windows Domain User	44
Specify a Renamed Windows Administrator User	46
Update the HP DMA APX	47
Create and Configure the HP DMA Custom Field	48
Change the Number of Active Connections	49
Glossary	50

Audience

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

Document Map

The following table shows you how to navigate this guide:

Topic	Description
Connector	How to configure the Connector between HP DMA and your server management tool.
Roles, Permissions, and Capabilities	How these mechanisms are used to achieve fine-grained role-based access control to HP DMA features, target servers, and automation content.
Targets	How to manage the HP DMA target environment.
Solution Packs	How to import a solution pack.
Mail Settings	How to specify the email settings.
Special Configurations	How to configure HP DMA for certain non-default scenarios.

Important Terms

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

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

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

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

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

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

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

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

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

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

Additional terms are defined in the [Glossary](#) on page 50.

Additional Resources

For information about installing HP DMA, see the *Database and Middleware Automation Installation Guide*.

For information about using the HP DMA web interface, see the *Database and Middleware Automation User Guide*.

For information about using the HP DMA application programming interfaces (APIs), see the *Database and Middleware Automation API Reference Guide*.

For information about specific solution packs and workflows, see the HP DMA solution pack user guides.

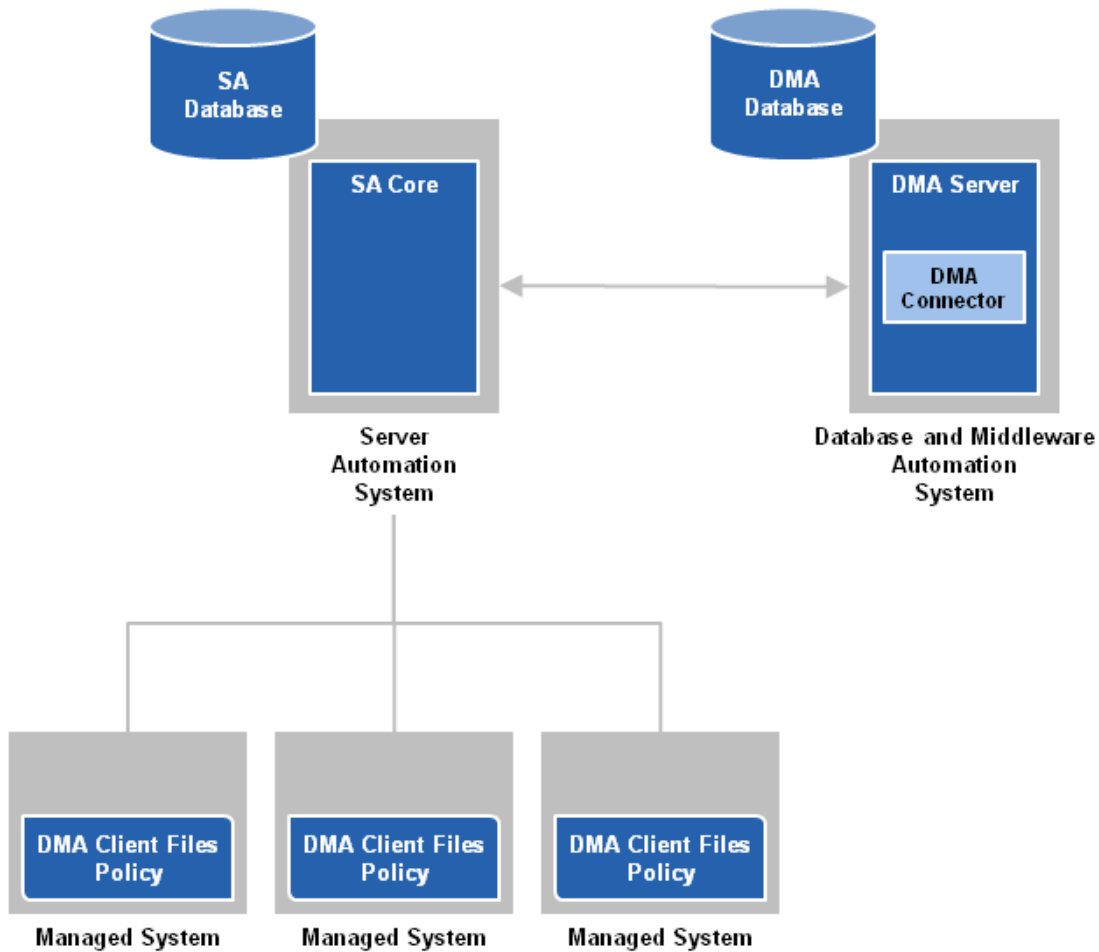
These documents are part of the HP DMA documentation library, which is available on the HP Software Product Manuals web site:

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

Connector

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

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



The Connector is added and initially configured when you install HP DMA. If you change the location or configuration of your server management tool, you may need to reconfigure the Connector.

To configure the Connector:

1. Go to Setup > Connectors.
2. Click the tab that corresponds to the Connector for your server management tool.
3. Specify the information required.

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

hp Database & Middleware Automation

Home Automation Reports Environment Solutions **Setup**

Configuration Permissions Capabilities Roles Connector

Connector

SAsrvr001.mycompany.com

Server Automation Host: SAsrvr001.mycompany.com

Server Automation Username: dma_integration_user

Server Automation Password: ●●●●●●●●

Save

The user specified here must be a valid SA user and have Read and List permissions on the SA Folder containing the DMA Client Files software policy.

4. Click the **Save** button.

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

5. Stop and restart your HP DMA server:

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

Roles, Permissions, and Capabilities

HP DMA provides very finely grained role-based access control over the following things:

- Who can log in to HP DMA
- Who can view, modify, or deploy to a specific organization
- Who can view or modify a specific workflow
- Who can create workflows
- Who can modify a specific step
- Who can view, modify, or execute a specific deployment
- Who can view or modify a specific policy
- Who can administer HP DMA, including setting permissions for all these items

Roles, capabilities, and permissions are the mechanisms HP DMA uses to establish this control. These mechanisms can help you precisely manage the privileges of individual users and groups.

The following topics show you how to use these mechanisms to implement a secure HP DMA environment:

Topic	Description
Roles	Roles represent groups of users with similar privileges. Roles are defined in your server management tool and are subsequently registered in HP DMA.
Capabilities	Capabilities are groups of HP DMA privileges. The HP DMA administrator assigns capabilities to one or more roles.
Permissions	Permissions determine who can view, modify, deploy to, or execute a particular automation item. Permissions can be assigned by the user who creates the item or anyone who has previously been granted Write permission for that item. They can also be assigned by the HP DMA administrator. Note: Organization permissions can only be modified by the HP DMA administrator.
Types of Users	There are five types of HP DMA users, each of whom requires different privileges.

Related Topics:

[Connector](#) on page 11

[Targets](#) on page 22

[Solution Packs](#) on page 29

[Mail Settings](#) on page 35

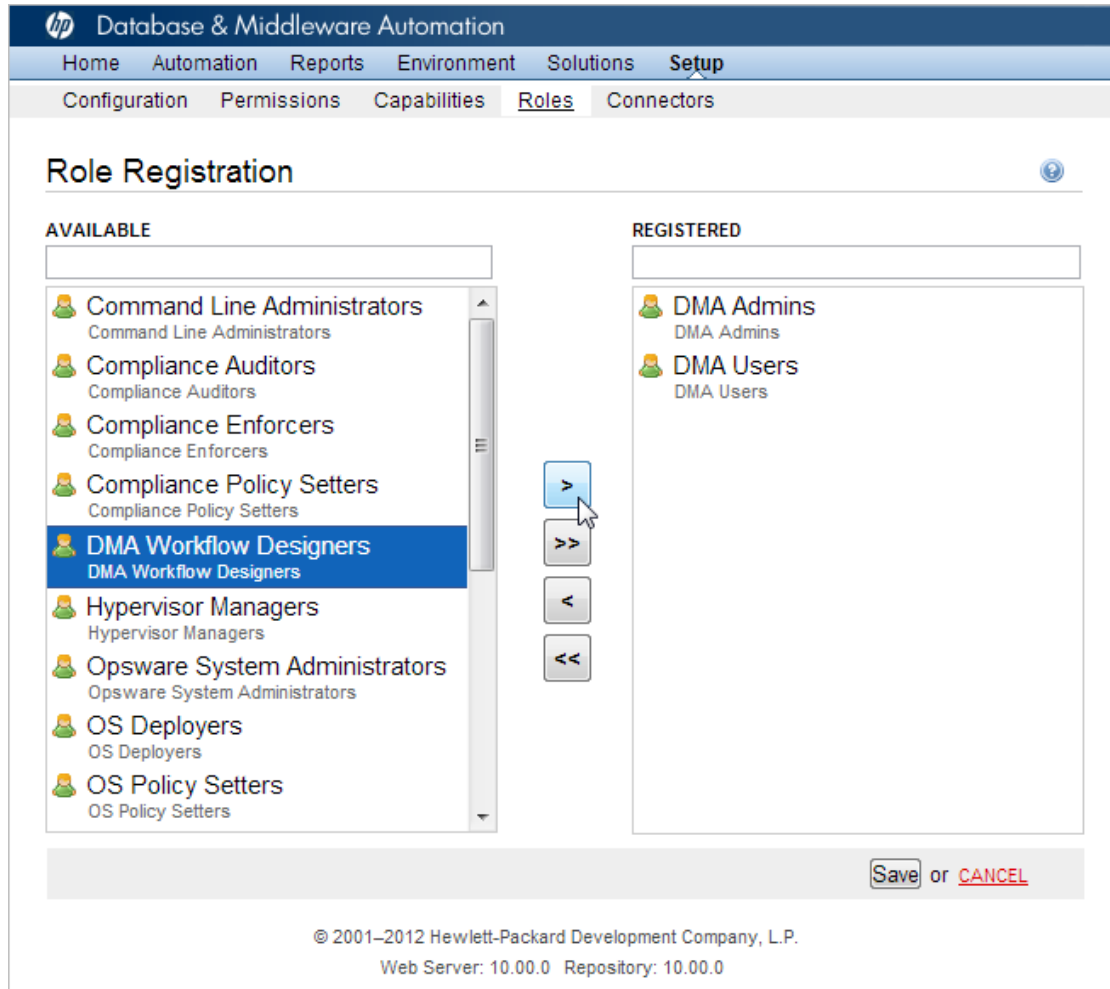
[Special Configurations](#) on page 36

Roles

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

Roles are defined in your server management tool. In HP Server Automation (SA), for example, a role is an SA group to which a user belongs.

Before you can associate a role with an automation item or organization, however, you must register that role. This is done on the Role Registration page:



HP DMA determines your role when you log in. Your access is based on the roles that were registered at the time that you logged in. Whenever the Role Registration page is accessed (or refreshed), HP DMA updates the list of available roles.

Note: If your server management tool administrator removes a role, HP DMA will not become aware of that change until the next time that you log in. HP DMA will continue to use that role for any users that are logged in.

Note: Immediately after HP DMA is installed, there is only one user defined: dma_initial_admin. This user has Administrator capability. To grant access to other users, you must initially log in as dma_initial_admin. See the *HP DMA Installation Guide* for more information.





Note: Administrator capability is required to perform the following tasks.

To register or unregister roles:

1. Go to Setup > Roles.

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

2. Perform one of the following actions:

Goal	Steps Required
Register a single role	In the Available list on the left, select the role that you want to register. Click the  button. The selected role moves to the Registered list on the right.
Register all roles	Click the  button. All the roles move to the Registered list on the right.
Unregister a single role	In the Registered list on the right, select the role that you want to unregister. Click the  button. The selected role moves to the Available list on the left.
Unregister all roles	Click the  button. All the roles move to the Available list on the left. Caution: At least one role with Login Access and Administrator capability must remain registered.

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

Related Topics:

[Types of Users](#) on page 19

[Capabilities](#) on next page

[Permissions](#) on page 17

Capabilities

Capabilities are collections of related privileges. There are three capabilities defined in HP DMA:

- Login Access** Login Access capability enables a user to log in to the HP DMA web interface. This capability does not guarantee that this user can view any organizations or automation items—permissions are required to access those items.
- Workflow Creator** Workflow Creator capability enables a user to create new workflows and make copies of other workflows.
- Administrator** Administrator capability enables a user to perform any HP DMA action and view all organizations. If you have Administrator capability, you do not need Workflow Creator capability.

The HP DMA administrator can assign any of these capabilities to one or more registered roles.

Note: Administrator capability is required to perform the following task.

To assign a capability to a role:

1. Go to the Setup > Capabilities page.
2. In the Capabilities list on the left, select the capability that you would like to grant to one or more registered roles. The Capabilities table opens:

Capabilities

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

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

3. To assign a capability to a role, select the check box for that capability. To assign a capability to all registered roles, click the corresponding ALL link at the bottom of the table.
4. Click **Save**.

Note that HP DMA will refuse to save the changes if no roles have Login Access or Administrator capability.

Related Topics:

[Types of Users](#) on page 19

[Roles](#) on page 14

[Permissions](#) on next page

Permissions

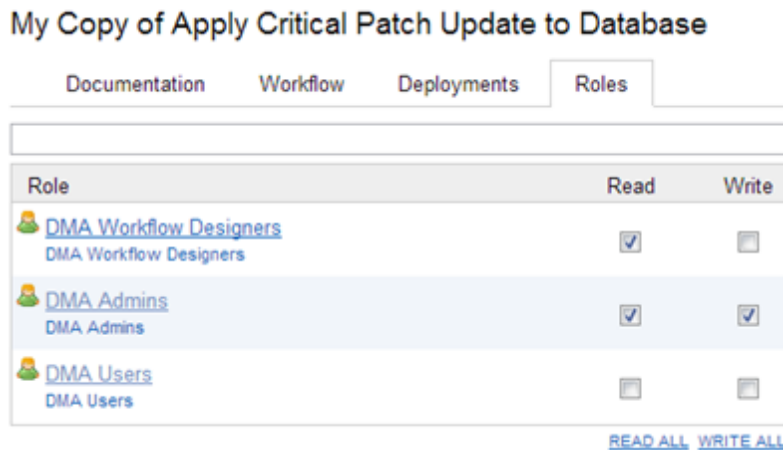
Role-based permissions are assigned to each automation item (workflow, deployment, step, or policy) and to each organization. These permissions determine who is allowed to view, modify, deploy to, or execute the pertinent item. Different types of items have different types of permissions:

Item	Read	Write	Execute	Deploy
Workflows	yes	yes	n/a	n/a
Deployments	yes	yes	yes	n/a
Steps	n/a	yes	n/a	n/a
Policies	yes	yes	n/a	n/a
Organizations	yes	yes	n/a	yes

Permissions can be set by the following users:

- The user who created the automation item or organization
- Any user who has Write permission for that automation item
- Any user who has Administrator capability

If you want other users to be able to access a particular item that you create, you must explicitly grant them permission to do so. You can do this on the Roles tab for that item. For example:



The roles listed on the Roles tab have been registered with HP DMA (see [Roles](#) on page 14). This is typically a subset of the roles defined in your server management tool.

Users with Administrator capability can modify the permissions for any organization or unlocked automation item from the Setup page.

Note: Only users with Administrator capability can create or modify functions.

The following instructions show you how the Administrator can grant permissions for a workflow and an organization. The procedure for the other types of automation items and organizations is similar.

Note: You must have Administrator capability to perform the following procedure.

To grant a role permission to access a specific workflow:

1. Go to Setup > Permissions.
2. Select the role whose permissions you want to modify.
3. Go to the Workflows tab.
4. For each workflow listed:
 - Select Read if you want users with this role to be able to view this workflow.
 - Select Write if you want users with this role to be able to modify this workflow.

Note that you cannot select Write for locked workflows.

5. Click the **Save** button.

HP DMA will not save the workflow unless at least one role has Read permission.

Tip: You can use the ALL links at the bottom of each Permissions tab to quickly assign roles to all the automation items or organizations listed.

If you do not have Administrator capability, but you have Write permission for the workflow, you can grant others permission to access that workflow.

Note: You must have Write permission on the workflow to perform the following procedure.

To grant a role permission to access a workflow that you can Write:

1. Go to Automation > Workflows.
2. Select the workflow to which you want to grant access.
3. Go to the Roles tab.
 - Select Read if you want users with this role to be able to view this workflow.
 - Select Write if you want users with this role to be able to modify this workflow.

4. Click the **Save** button.

HP DMA will not save the workflow unless at least one role has Read permission.

Related Topics:

[Types of Users](#) on next page

[Roles](#) on page 14

[Capabilities](#) on page 16

Types of Users

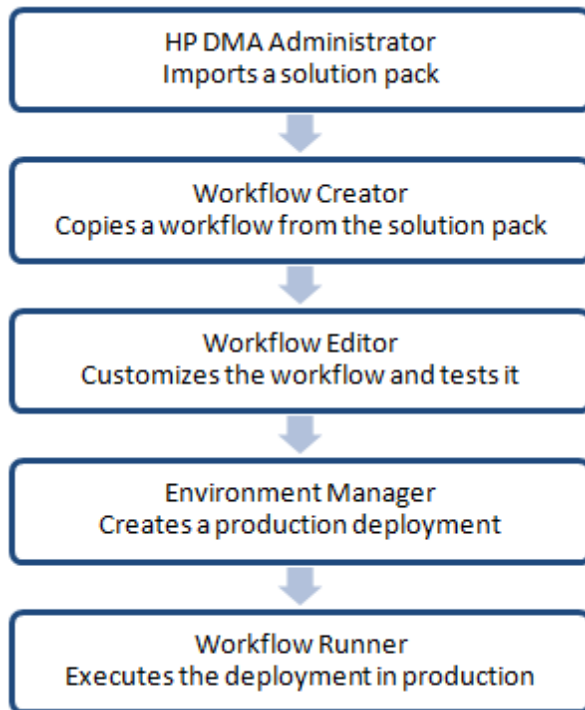
When you think about roles, capabilities, and permissions, it is useful to consider the types of users who interact with HP DMA. What a specific user can do is determined by the capabilities associated with that user's role and the specific permissions assigned to the pertinent automation items and organizations.

In a typical HP DMA managed environment, there are five types of users:

Type of User	Number	Responsibilities	Capabilities and Permissions Required
HP DMA administrator	1 or 2 plus backup	<ul style="list-style-type: none"> Manages roles Manages other users' capabilities Manages access to organizations Imports solution packs 	<ul style="list-style-type: none"> Login Access Administrator
Workflow Creator	1 or 2 plus backup	<ul style="list-style-type: none"> Creates new workflows Sets initial workflow permissions 	<ul style="list-style-type: none"> Login Access Workflow Creator
Workflow Editor	few	<ul style="list-style-type: none"> Modifies or copies existing workflows Creates deployments and executes them in a test or development environment Manages workflow permissions 	<ul style="list-style-type: none"> Login Access PLUS <ul style="list-style-type: none"> • Write permission for any workflows to be edited • Read permission for any workflows to be copied • Deploy permission for the organization where the workflows will be tested
Environment Manager	1 per environment plus backup	<ul style="list-style-type: none"> Adds servers Creates deployments in the production environment Sets deployment permissions Creates policies and sets policy values 	<ul style="list-style-type: none"> Login Access PLUS <ul style="list-style-type: none"> • Read, Write, and Deploy permission for the specific organizations to be managed • Read permission for the workflows that will be used to create the production deployments

Type of User	Number	Responsibilities	Capabilities and Permissions Required
Workflow Runner	many	Executes existing deployments	Login Access PLUS <ul style="list-style-type: none"> • Read and Execute permission for the specific deployments to be executed • Read permission for the organization where the deployments will be executed

Here is an example of how these five users would collaborate to deploy HP DMA automation content in a production environment:



Although it is possible for one person to perform multiple tasks—any user who has Administrator capability, for example, can perform all these tasks—HP strongly recommends that you create separate users and assign specific capabilities and permissions to each user. This enables you to both create a more robust audit trail and reduce the risk of human error by preventing less privileged users from making costly mistakes.

Caution: For security reasons, the Workflow Runner should never have Write permission for any environment or automation item.¹

¹Certain workflows update custom fields or metadata associated with the organization. To run those workflows, a user must have Write permission for the organization.

Related Topics:

[Roles](#) on page 14

[Capabilities](#) on page 16

[Permissions](#) on page 17

Targets

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

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

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

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

Organizations

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

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

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

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

To create an organization:

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

To grant users permission to access a specific organization:

1. Go to Setup > Permissions.
2. Select the role whose permissions you want to modify.
3. Go to the Organizations tab.
4. For each organization listed:

- Select Read if you want users with this role to be able to view information about this organization, including the servers it contains.
- Select Write if you want users with this role to be able to modify this organization.
- Select Deploy if you want users with this role to be able to deploy workflows to the servers in this organization.

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

5. Click the **Save** button.

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

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

To delete an organization:

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

Servers

Servers that will act as HP DMA targets must have the ability to communicate with HP DMA. The mechanism that facilitates this communication depends on the server management tool that you are using.

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

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

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

To add servers to an organization:

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

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

The servers that you can see in the list depend on your permissions in your server management tool.

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

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

To delete a server from an organization:

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

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

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

Custom Fields

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

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

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

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

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


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

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

To create a new Custom Field:

1. Go to Environment > Custom Fields.
2. Click the **New field** button.
3. Specify the following information for your new Custom Field:

- Name – a unique name for the Custom Field
- Object – organization, server, instance, or database
- Type – text, multi-line (contains one or more lines of text), or list
- Options – items that will be available in the list (for list type fields only)

To add a list item, type its name in the box, and click the  (add) button. For example:

To delete a list item, click the  (delete) button.

4. Click **Save**.

To modify an existing Custom Field:

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

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

4. Click **Save**.

To delete a Custom Field:

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

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

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

Smart Groups

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

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

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

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

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

To create a new Smart Group:

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

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

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

4. Click **Save**.

To modify an existing Smart Group:

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

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

4. Click **Save**.

To delete a Smart Group:

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

Policies

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

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

Policies can have three different types of attributes:

- Text – a simple text value that users can view while deploying and running automation.
- Password – also a simple text value, but the value is masked (obfuscated) when displayed so that users cannot see the value.

Note that any parameter whose name contains the string “password” is automatically masked throughout the HP DMA user interface.

- List – a free-form text field that can contain comma-delimited lists of values or other large text data not suitable for a Text type attribute.

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

To create a new policy:

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

To modify an existing policy:

1. Go to Automation > Policies.
2. Select the policy that you want to modify.
3. Make the modifications that you want to make to the policy.

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

Policies that are included in HP DMA solution packs are locked. You cannot modify a locked policy, but you can make a modifiable copy of that policy.

4. Click **Save**.

To delete a policy:

1. Go to Automation > Policies.
2. Select the policy that you want to delete.

You cannot delete a policy that is referenced by a deployment.

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

Discovery

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

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

Related Topics:

[Connector](#) on page 11

[Roles, Permissions, and Capabilities](#) on page 13

[Solution Packs](#) on next page

[Mail Settings](#) on page 35

[Special Configurations](#) on page 36

Solution Packs

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

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

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

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

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

Install a Solution Pack

The HP DMA solution packs are available on your HP DMA installation DVD. You can download the most recent updates to those solution packs from HP Software Support Online (see [Support](#) on page 3).

To install a solution pack:

1. Go to [HP Live Network](#) to view a list of the latest available DMA solution packs.
2. Download the pertinent solution pack file from [HP Software Support Online](#).
3. Extract the ZIP file that contains your solution pack (for example: DBCompliance.zip).
4. On the system where you downloaded the solution pack, open a web browser, and go to the following URL:

```
https://<HP_DMAserver>:8443/dma/login
```

Port 8443 is the default port. You can change this if you prefer to use a different port (for more information, see [Change the Default Port](#) on page 37).

5. Log in to the DMA server as a user with Administrator capability.
6. On the Solutions > Installed tab, click the **Browse** button in the lower right corner. The Choose File dialog opens.

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

7. Locate and select the ZIP file that you extracted in step 3, and click **Open**.

8. Click **Import solution pack**.

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

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

The screenshot shows the HP Database & Middleware Automation web interface. The top navigation bar includes 'Home', 'Automation', 'Reports', 'Environment', 'Solutions', and 'Setup'. Below this, there are tabs for 'Installed' and 'History'. The main content area is titled 'Installed Solutions' and is divided into two panes: 'SOLUTION PACKS' and 'DETAILS'. The 'SOLUTION PACKS' pane lists several solution packs, with 'HP DMA Database Compliance Solution Pack' (Version 10.0) highlighted in blue. The 'DETAILS' pane shows information for the selected pack: Name: HP DMA Database Compliance Solution Pack, Version: 10.0, Targets: 0, Installed: 12 Nov, 2012, and Description: Provides CIS Level I and II, PCI, and SOX auditing for Oracle Database, Microsoft SQL Server, and Sybase ASE. PCI and SOX compliance checks are currently mappings to the existing CSI audits. Build 31753. At the bottom of the interface, there are buttons for 'Choose File', 'No file chosen', and 'Import solution pack'.

© 2001–2012 Hewlett-Packard Development Company, L.P.
Web Server: 10.00.0 Repository: 10.00.0

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

hp Database & Middleware Automation
Home Automation Reports Environment Solutions Setup
Installed History

HP DMA Database Compliance Solution Pack

Version 10.0

General Policies Workflows Steps Reports

Run MS SQL Compliance Audit	
Run Oracle Compliance Audit	
Run Sybase Compliance Audit	

• Gather Parameters for Oracle Compliance	1
• Gather Advanced Parameters for Oracle Compliance	2
• Failure	3
• Prepare Server	4
• Validate Compliance Parameters	5
• Get Oracle Home	6
• Prepare Oracle Instance	7
• Get Listener Names	8
• Audit Unix or Linux OS Specific Settings	9
• Audit Installation and Patch	10
• Audit Directory and File Permissions	11
• Failure	12

 [DELETE](#)

© 2001–2012 Hewlett-Packard Development Company, L.P.
Web Server: 10.00.0 Repository: 10.00.0

Versioning and Importing Solution Packs

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

If you import two solution packs with shared components, the shared component is only imported once, and the higher-versioned component takes precedence over the lower-versioned component. For example, if you import solution pack 1 with step version 1 and solution pack 2 with step version 2, and they share the step, the shared step is only imported once and the higher-versioned step takes precedence and is shared between the two solution packs.

Steps are the only components that can be shared across solution packs. This fact is particularly important when you are removing solution packs. See [Delete a Solution Pack](#) on page 34.

Modify a Solution Item

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

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

To make a copy of a Solution Pack item:

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

Roll Back a Solution Pack

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

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

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

Note the following:

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

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

To roll back a solution pack:


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

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



DOWNGRADE HP SERVER AUTOMATION DISCOVERY SOLUTION PACK TO V9.12?

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



UNINSTALL HP SERVER AUTOMATION DISCOVERY SOLUTION PACK V9.14?

3. Click the **Rollback** button 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.

Remember that steps are the only components that can be shared across solution packs. If a step is shared with another solution pack that you are removing, once you remove the solution pack, that shared step remains in the system.

To delete a specific solution pack:

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



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

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

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

Related Topics:

[Connector](#) on page 11

[Roles, Permissions, and Capabilities](#) on page 13

[Targets](#) on page 22

[Mail Settings](#) on next page

[Special Configurations](#) on page 36

Mail Settings

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

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

To configure the mail settings:

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

Related Topics:

[Connector](#) on page 11

[Roles, Permissions, and Capabilities](#) on page 13

[Solution Packs](#) on page 29

[Targets](#) on page 22

[Special Configurations](#) on page 36

Chapter 5

Special Configurations

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

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

[Use a Proxy Server with HP DMA](#) on page 38

[Run as a Windows Domain User](#) on page 44

[Specify a Renamed Windows Administrator User](#) on page 46

[Change the Number of Active Connections](#) on page 49

Change the Default Port

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

To change the HP DMA port:

1. Stop HP DMA:

```
# service dma stop
```

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

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

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

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

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

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

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

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

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

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

8. Start HP DMA:

```
# service dma start
```

Use a Proxy Server with HP DMA

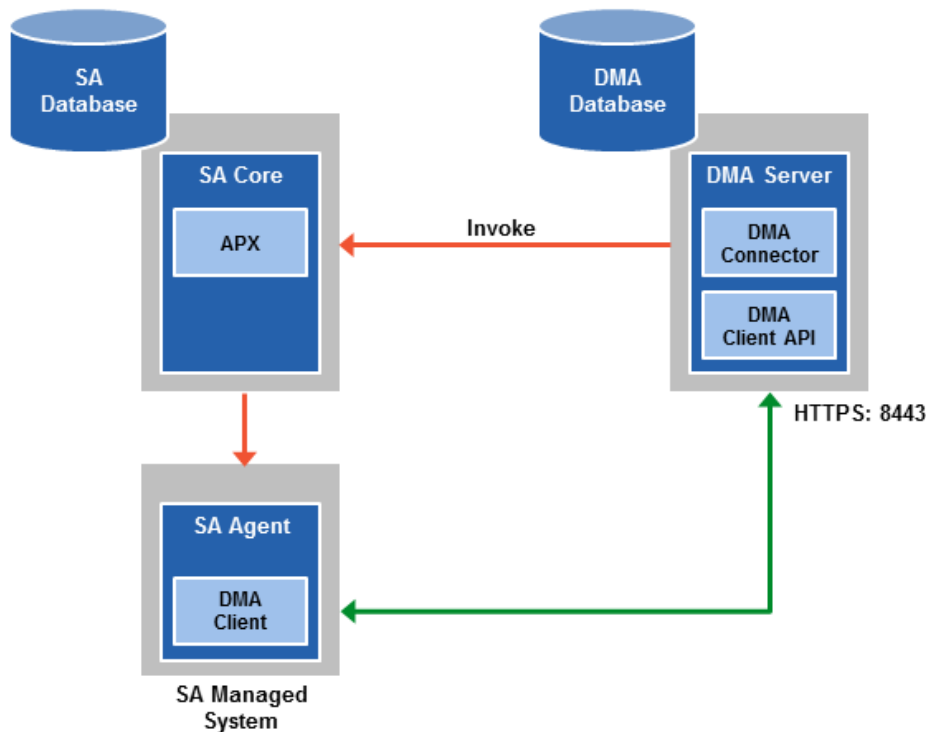
A proxy server can be used to provide additional security for HP DMA communications. This topic shows you how to use an HP Server Automation (SA) Satellite as a proxy server.

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.

Default HP DMA Communications

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

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

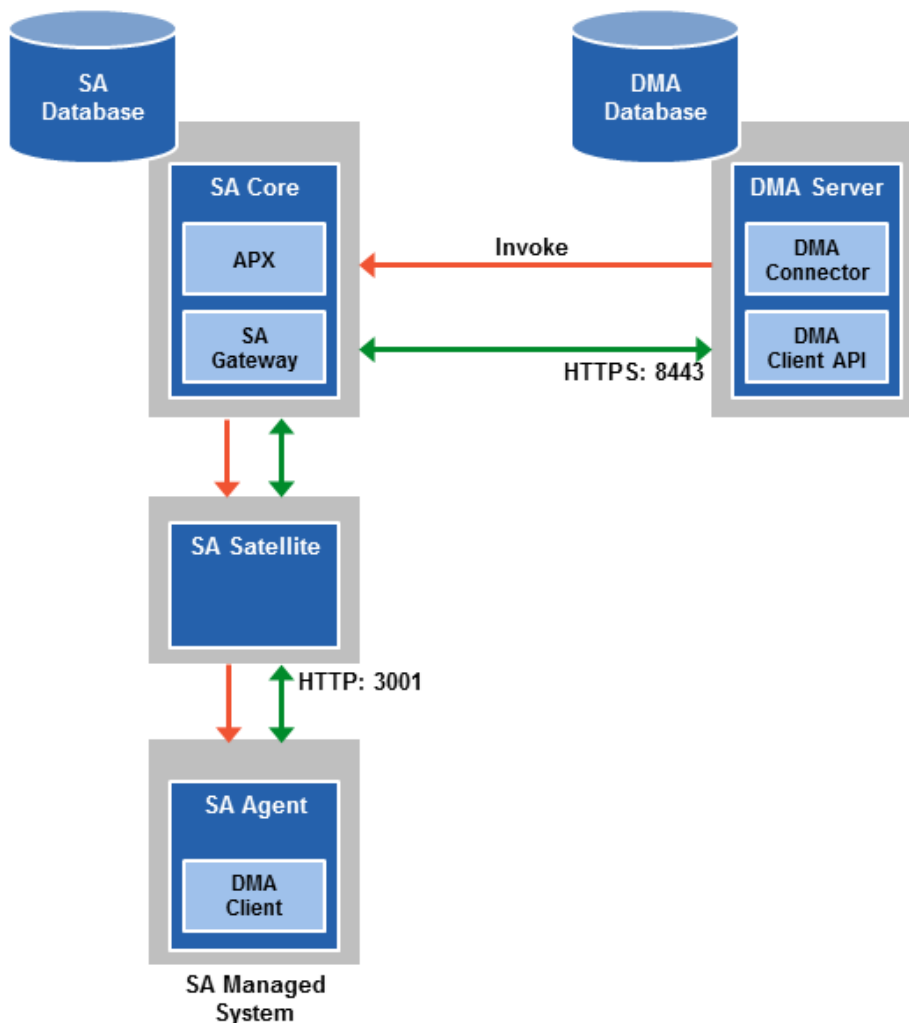


Using an SA Satellite as a Proxy Server

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

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

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



How HP DMA Manages Proxy Communication

HP DMA uses two Custom Fields to control proxy communication:

- `west_proxy_address` contains the full URL of the proxy including the proxy port.
- `west_proxy_in_use` tells HP DMA whether a proxy server will be used. Valid values are:

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

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

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

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

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

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

How to Set Up a Proxy Server

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

1. Add a new Egress 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. Create and configure the two Custom Fields that instruct HP DMA to route traffic through the proxy server. This procedure is performed in the HP DMA UI.

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

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

Add a New Egress Rule

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

To add the new Egress 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-<facilityName>/opswgw.custom
```

Here `<facilityName>` is the name given to the facility when it was created. For example: `DATACENTER1`

- b. Add the following line:

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

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

- c. Save the file.

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

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

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

Add and Configure the HP DMA Custom Fields

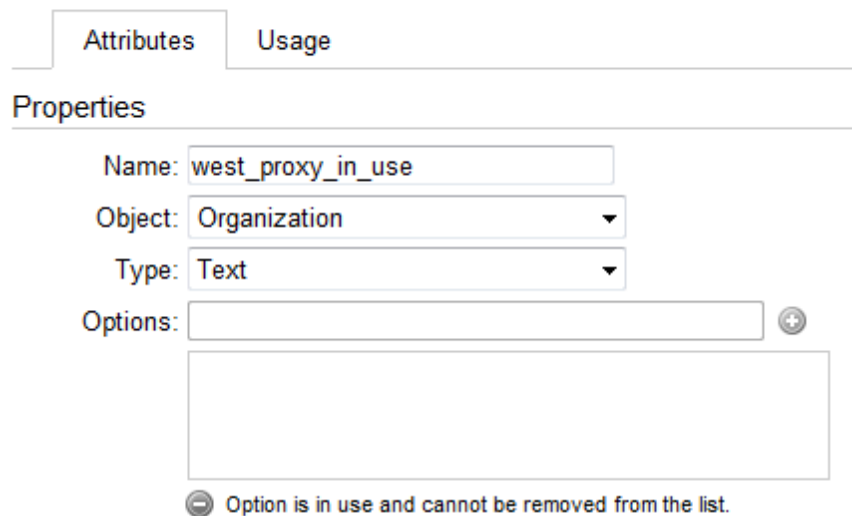
In the HP DMA web UI, create (if necessary) and configure the proxy communication Custom Fields.

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

To create the Custom Fields for proxy communication:

1. Decide whether your proxy is at the organization level or the server level.
2. Perform the following steps to add the `west_proxy_in_use` and `west_proxy_address` Custom Fields to each pertinent organization or server:
 - a. Go to Environment > Dashboard > `<organization_name>`.
 - b. *Optional:* Go to `<server_name>`.
 - c. Go to the Custom Fields tab.
 - d. Click **NEW CUSTOM FIELD**.
 - e. Specify the Custom Field name (`west_proxy_in_use` or `west_proxy_address`).
 - f. Set the Object to Organization or Server, as appropriate.
 - g. Set the Type to Text. For example:

New custom field



Attributes Usage

Properties

Name:

Object:

Type:

Options:

Option is in use and cannot be removed from the list.

- h. Click **Save**.

To specify the Custom Field values:

You can specify the Custom Field values at the organization level, the server level, or both (see [Proxy Precedence](#)).

1. Go to Environment > Dashboard > *<organization_name>*.
2. *Optional:* Go to *<server_name>*.
3. Go to the Custom Fields tab.
4. Set `west_proxy_address` to the full URL of the proxy, including the port, in this format:
`http://<proxy_hostname>:<proxy_port>`
5. Set `west_proxy_in_use` to TRUE, FALSE, or blank.
6. Click **Save**.

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

My Organization

Properties Custom Fields Roles

Custom fields [NEW CUSTOM FIELD](#)

west_proxy_address:

west_proxy_in_use:

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

Run as a Windows Domain User

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

To do this, you must create and configure the following Custom Fields:

`domain_username_win`

`domain_password_win`

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

The value of `domain_password_win` is encrypted before it is stored .

Note: The specified domain user must:

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

To create the Custom Fields:

1. Go to Environment > Custom Fields.
2. Click the **New Field** button.
3. Specify the Custom Field name: `domain_username_win`.
4. From the Object drop-down list, select either Server or Organization.

If each Windows server requires a different Windows domain user, you will need to specify this user name for each server. In this case, select Server here.

If many Windows servers in the same organization will use the same Windows domain user, it will be more convenient to specify the user name at the organization level. In this case, select Organization here.

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

5. From the Type drop-down list, select Text.
6. Click **Save**.
7. Repeat steps 2–6 to create the `domain_password_win` Custom Field.

To configure the Custom Fields:

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

For each organization or server where you want to run workflows on Windows targets as a specific Windows domain user, follow these steps:

1. For an organization, go to Environment > Dashboard > *organization_name*
For a server, go to Environment > Dashboard > *organization_name* > *server_name*
2. Go to the Custom Fields tab.
3. Specify the Windows domain user name in the `domain_username_win` Custom Field.

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

4. Specify the Windows domain user password in the `domain_password_win` Custom Field.
5. Click **Save**.

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

Specify a Renamed Windows Administrator User

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

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

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

Instructions for making each of these changes are provided here.

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

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

Update the HP DMA APX

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

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

- SA Global Shell (OGSH) permission to Launch Global Shell.
- Manage Extensions (Read & Write) permission under Automation Platform Extension.
- List, Read, and Write permission on the /DMA_APX folder.

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

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

To update the HP DMA APX:

1. Log in to Global Shell:

```
ssh -p 2222 <SA_APX_User>@<SA_Slice>
```

2. Enter the password for the <SA_APX_User> when prompted.

3. Export the APX:

```
apxtool export -u com.hp.dma.conn.sa.westapx tmp
```

4. Update the APX permission file:

- a. Open the APX permission file in a text editor. For example:

```
vi tmp/APX-INF/apx.perm
```

- b. Add the Windows Administrator account names to the escalation section. To allow Windows Administrator account names Administrator and HPAdmin, for example, the escalation section would look like this:

```
@use_feature(name="runCommandOnServer",  
             login_names="root,Administrator,HPAdmin",  
             resource(resource_type="device",  
                     expression=ALL))
```

5. Import the updated APX:

```
apxtool import -c tmp
```

Type Y (or y) in response to the two prompts.

6. Exit the Global Shell:

```
rm -rf tmp  
exit
```

Create and Configure the HP DMA Custom Field

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

To create the Custom Field:

1. Go to Environment > Custom Fields.
2. Click the **New Field** button.
3. Specify the Custom Field name `agent_username_win`.
4. From the Object drop-down list, select either Server or Organization.

If each Windows server has a different Windows Administrator user name, you will need to specify this user name for each server. In this case, select Server here.

If many Windows servers in the same organization have the same Windows Administrator user name, it will be more convenient to specify the user name at the organization level. In this case, select Organization here.

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

5. From the Type drop-down list, select Text.
6. Click **Save**.

To configure the Custom Field:

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

For each organization or server where you want to specify the Windows Administrator user name, follow these steps:

1. For an organization, go to Environment > Dashboard > *organization_name*
For a server, go to Environment > Dashboard > *organization_name* > *server_name*
2. Go to the Custom Fields tab.
3. Specify the Windows Administrator user name in the `agent_username_win` Custom Field.
If you do not see this Custom Field, be sure that **Show empty values** is selected.
4. Click **Save**.

Note: If you want HP DMA to run workflows on Windows targets as a specific Windows domain user, also see [Run as a Windows Domain User](#) on page 44.

Change the Number of Active Connections

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

To change the number of active connections:

1. As root, stop the HP DMA server:

```
$ service dma stop
```

2. Open the following file in a text editor:

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

3. Modify the following parameters:

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

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

4. Start the HP DMA server again:

```
$ service dma start
```

Glossary

A

automation items

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

B

bridged execution

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

C

capability

Capabilities are collections of related privileges. There are three capabilities defined in HP DMA. Login Access capability enables a user to log in to the web interface. This capability does not guarantee that this user can view any

organizations or automation items—permissions are required to access those items. Workflow Creator capability enables a user to create new workflows and make copies of other workflows. Administrator capability enables a user to perform any action and view all organizations. If you have Administrator capability, you do not need Workflow Creator capability. The Administrator can assign any of these capabilities to one or more roles registered roles.

connector

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

cross-platform

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

custom field

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

D

deployment

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

F

function

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

I

input parameters

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

M

mapping

An input parameter is said to be "mapped" when its value is linked to an

output parameter from a previous step in the workflow or to a metadata field.

Mapped parameters are not visible on the Deployment page. You can "unmap" a parameter by specifying - User Selected - in the workflow editor. This parameter will then become visible on the Deployment page.

O

organization

An organization is a logical grouping of servers. You can use organizations to separate development, staging, and production resources - or to separate logical business units.

P

parameters

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

policy

Policies are reusable sets of attributes that can be used as parameter values in deployments. Deployments can reference policy attributes to change the automation behavior. Policies provide values for input parameters. They can contain fixed values or reference Custom Fields. Policies enable HP DMA to manage groups of hundreds or thousands of servers at a time without the need to configure each individual server.

R

raw devices

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

role

Each HP DMA user has one or more roles. Roles are used to grant users permission to log in to and to access specific automation items and organizations. Roles are defined in your server management tool. Before you can associate a role with an automation item or organization, however, you must register that role in HP DMA.

S

smart group

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

software repository

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

solution pack

A solution pack contains one or more related workflow templates. These templates are read-only and cannot be

deployed. To run one of the workflows included in a solution pack, you must first create a deployable copy of that template and then customize that copy for your environment. Solution packs are organized by function - for example: database patching or application server provisioning.

steps

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

T

target instance

In the context of MS SQL database refresh, the term "target instance" refers to the SQL Server instance where the database that will be restored resides.

W

workflow

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

workflow editor

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

workflow templates

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