# Database and Middleware Automation

Software Version: 10.50.001.000

Linux, Solaris, AIX, and HP-UX

# Integration 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

# Integrate

This section provides you the information about integrating with Server Automation (SA).

"Integrate with SA" on the next page

# Integrate with SA

You must integrate DMAwith SA before you can use DMA.

> **Caution:** An SA administrator—someone with SA administrator privileges and access must integrate DMA with HP SA.

DMA uses Server Automation (SA) as an agent infrastructure. It integrates with SA to authenticate users, associate users with groups, and determine user privileges. DMA uses SA to acquire knowledge of servers and to send requests to execute workflows on servers.

> **Note:** Any server that will be used as an DMA target needs to be managed by SA. It must also have the DMA Client Files software policy.

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


- "SA integration requirements"
- "SA integration overview"
- "Import DMA APX"
- "Install DMA Client Files policy"
- "Set up SA groups and users"
- "Use SA Gateway Network as a proxy network" on page 15


# SA integration overview

The SA administrator needs to perform the following general steps:

1. Install the DMA Automation Platform Extension (APX) on the SA server.
2. Install the DMA Client Files policy on the SA server.
3. Attach and remediate the DMA Client Files policy on all SA managed servers that will be used as DMA targets.
4. Set up the SA groups that will have DMA access privileges.
5. Set up the SA user that DMA will use to connect to SA. This user must be permitted to access SA APIs.

In the commands that follow, replace the variables (found within <>'s) with values appropriate for your environment:

| Variable | Example | Description |
|---|---|---|
| <*SA_Server*> | saserver.mycompany.com | Fully qualified host name of the Server Automation server |
| <*DMA_server*> | dma.mycompany.com | Fully qualified host name of the DMA server |

# SA integration requirements

You must meet the following requirements before you can integrate DMA with Server Automation (SA):

- Make sure that you have met all the general DMA installation requirements in Pre-Installation Requirements.
- You have already installed and configured the DMA server software. If you have not done so, see Install the DMA Server.
- You have already installed and configured the DMA Client for SA. If you have not done so, see Install the DMA Client for SA.
- The DMA server software and the DMA Client for SA software must be installed on the same system. This system will be referred to as the DMA server in the following instructions.
- Ensure that you have provided appropriate SA permissions to DMA users. The following table lists the SA related permission and policy that needs to be enabled for users or user groups:

| SA permissions and policy | | SA User for APX (DMA WF Runner) | Connector User for DMA | DMA Admin |
|---|---|---|---|---|
| Action Permission | Manage Software Policy | NA | Read, Write | Read, Write |
| | Manage Extension | Read, Write | NA | Read, Write |
| | Managed Servers and Group | NA | YES | YES |
| OGFS Permission | Feature -Launch Global Shell to be selected | YES | NA | YES |
| | Groups - add all relevant groups | YES | NA | YES |
| Folder Permission | DMA_Client | Read, Write, Execute | Read, Write, Execute | Read, Write, Execute |
| | DMA_APX | Read, Write, Execute | NA | Read, Write, Execute |
| Resource Permission | All relevant Customer, facility and Device Group | NA | Read | Read |

# Support for SA 10.60

Database and Middleware Automation (DMA) Ultimate Edition now supports Server Automation (SA) 10.60.

This section provides information on upgrading and integrating DMA 10.50.001.000 with SA 10.60.

1. Stop all DMA and SA services.
2. Install or upgrade SA to 10.60.
3. On the DMA server:
   a. Upgrade JRE to version 1.8.
   b. Delete twistclient.jar and wlclient*.jar files from `/opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/lib/`
   c. Copy the opswclient.jar file from `<SA_install_dir_10.60>/twister/` to `/opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/lib/` directory.
   d. Run the following command to change the ownership of the opswclient.jar file:
   `chown hpdma:hpdma opswclient.jar`
   e. Run the following command to copy binaries to the SA server:sh
   `/opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/copy Jars.sh <FQDN of SA Core>`

4. Start all DMA and SA services.

# Import DMA APX

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

HPE DMA APX can be imported into Server Automation Virtual Appliance 10 (SAVA) or Server Automation Enterprise Edition (Enterprise SA):

- For SAVA: The HP Live Network connector (LNc) must be used.
- For Enterprise SA: LNc can be used or the APX can be imported manually.

## Live Network Connector Overview

Follow the SAVA or Enterprise SA instructions for configuring the HP Live Network connector. The APX is contained in the `content.sa_dma` LN Stream. SAVA uses the "Command-line Web Utilities Launcher" to configure LNc. Enterprise SA uses an installation of HP Live Network connector (LNc).

After the stream is loaded, the following APXs are visible in the `/DMA_APX` folder:

- Update West Apx user on Windows
- westApx

> **Note:** The user who runs the Update West APX must have read, write, and execute permission on the objects within the `/DMA_APX` folder.

## SAVA Installation of the DMA APX

> **Note:** This method can only be used for SAVA.

From the SA client, as a user with list and execute permission on the objects in the `/Opsware/Tools/Administrative Extensions` folder, do the following:

1. Go to the **Library** > **By Type** tab, and then select **Extensions** > **Web**.
2. From **Web**, select the **Command-line Web Utilities Launcher**.
3. Select **Live Network Connect** (the default).
4. To write the configuration to SAVA, execute the following command:

```
/opt/opsware/hpln/lnc/bin/live-network-connector write-config
--username=<username> --password=<password> --stream=content.sa_dma
```

Here *<username>* and *<password>* are your Passport user name and password.

> **Note:** Additional configuration can be added to the configuration using the `--add` option in the `live-network-connector` command. See *HP Live Network connector User Guide* for more information.

5. To download and import using the saved configuration, execute the following command:

   ```
   /opt/opsware/hpln/lnc/bin/live-network-connector download-import
   ```

   The default is `download-import`, so after the configuration is set up `download-import` is not required for this HP Live Network connector command.

# Enterprise SA Manual Import of the DMA APX

> **Tip:** The following steps must be performed by an SA administrator.
>
> The SA user (<*SA_APX_User*>) who imports the HPE DMA APX must belong to a group with the following privileges:
>
> - SA Global Shell (OGSH) permission to Launch Global Shell.
> - Manage Extensions (Read & Write) permission under Automation Platform Extension.
> - List, Read, and Write permission on the `/DMA_APX` folder.
>
>   If the `/DMA_APX` folder does not exist, this user must have List, Read, and Write permission on the `/` (root) folder, where the `/DMA_APX` folder will be created.

> **Note:** This method can only be used for Enterprise SA.
>
> If HP Live Network connector is configured for `content.sa_dma`, then you do not need to manually import the DMA APX.

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

   On the DMA server, copy the HPE DMA APX to the SA server Global Shell. For example:

   ```
   $ scp -P 2222 /opt/hp/dma/server/client_bits/westapx.zip
   <SA_APX_user>@<SA_Server>:westapx.zip
   ```

```
$ scp -P 2222 /opt/hp/dma/server/client_bits/updateWinAdmin.zip
<SA_APX_user>@<SA_Server>:updateWinAdmin.zip
```

2. Log in to the SA server Global Shell, and install the HPE DMA APX using the defaults, for example:

   ```
   $ ssh -p 2222 <SA_APX_user>@<SA_Server>

   $ apxtool import westapx.zip

   $ apxtool import updateWinAdmin.zip
   ```

   By default this places the APX in `/DMA_APX`. If you want to place it somewhere else use the `-f <folder>` option.

   To skip the prompts, add `-F` to the end of the command or else respond Y to all Y/N prompts.

   > **Note:** This creates the `/DMA_APX` (or <*folder*>) folder.

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

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

If you get this error message, verify the location of the APX tool and rerun the `apxtool` command. See the Importing the DMA APX topic in the *DMA Installation Guide*.

# Install DMA Client Files policy

This topic shows you how to install the DMA Client Files policy on the SA server and then to attach and remediate the DMA Client Files policy on all SA managed servers that will be used as DMA targets.

> **Tip:** The following steps must be performed by an SA administrator.
>
> The SA user (<*SA_Policy_User*>) who installs the policy must belong to a group with the following privileges:
>
> - Manage Software Policy—Read & Write under Policy Management.
> - Manage Package—Read & Write under Package Management.
> - List, Read, Write, and Execute permissions on the folder (`/DMA_Client`) that will contain the DMA packages and policy.

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

Perform the following steps to install the DMA Client Files policy on your SA server, <*SA_Server*>:

1. In the SA Client, create a `/DMA_Client` folder.
2. As root on the DMA server, go to the `client_bits` folder and then run the `dma_upload` script using your <*SA_Policy_User*> account. For example:

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

   ```
   $ sh ./dma_upload.sh -host <SA_Server> -user <SA_Policy_User>
    -password <SA_Policy_Password>
    -keyFile /opt/hp/dma/server/tomcat/webapps/dma/WEB-INF/publicKey
    -folderName /DMA_Client
   ```

   > **Note:** If you omit the password option (-password), you will be prompted for the password.

3. *Optional:* To verify if the policy has been uploaded, perform the following steps in the SA Client:

   Go to **Library** > **By Folder** > `DMA_Client`

   The `DMA_Client` folder should be populated. Verify that the DMA Client Files policy is included.

4. For each server that is used as an DMA target, attach and remediate the DMA Client Files policy.

# Set up SA groups and users

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

> **Tip:** An SA administrator must perform the following steps.
>
> Your SA administrator may have a security model that is more finely grained. Follow your SA policies for naming and granting permissions to groups.

## DMA User Groups

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

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

To set up your DMA user groups, perform the following steps:

1. On the SA server that connects to DMA, create each of the groups listed in the table and any additional groups that you need.
2. Grant the following permissions to each group:
   - List, Read, and Execute permission for the `/DMA_APX` folder
   - Managed Servers and Groups
   - READ access to all managed servers that are added to DMA

To add servers to DMA organizations, a user must also have permission to see those servers in SA. This requires either Read permission on the pertinent customer or facility, or Read permission on the device group (or groups) where the servers reside.

> **Note:** Use the SA Client to grant these permissions.

3. Add at least one user to each group.

The next step is to register these groups as DMA roles and assign each role the appropriate DMA capability. These tasks are performed while you are logged in as dma_initial_admin. For instructions, see the Registering DMA roles and the Assigning DMA Capabilities sections in the Administration GuideAssign DMA capabilities.

# DMA Connector User

An additional SA user, *<dma_connector_user>*, is required to configure the DMA connector to SA. You must be logged in as dma_initial_admin. For instructions, see the Configuring the connector section in the Administration Guide.

> **Note:** This user does not need to be a member of any of the SA groups that you just created.
>
> This user will be used by DMA to connect to SA whenever a specific, personalized SA account cannot be used—for example, to verify whether a login is allowed.

**To create the DMA connector user:**

1. On the SA server that connects to DMA, create a new SA user (for example: dma_connector_user).
2. Grant this new user the following permissions:
   - List, Read, and Execute permission for the `/DMA_Client` folder
   - List permission for all parent folders of the `/DMA_Client` folder
   - Managed Servers and Groups
   - Manage Software Policy (READ)
   - READ access to all managed servers that are added to DMA

     This requires either Read permission on the pertinent customer or facility or Read permission on the device group (or groups) where the servers reside.

This completes the SA installation and integration steps that must be done by the SA administrator.

Next, start DMA.

# Use SA Gateway Network as a proxy network

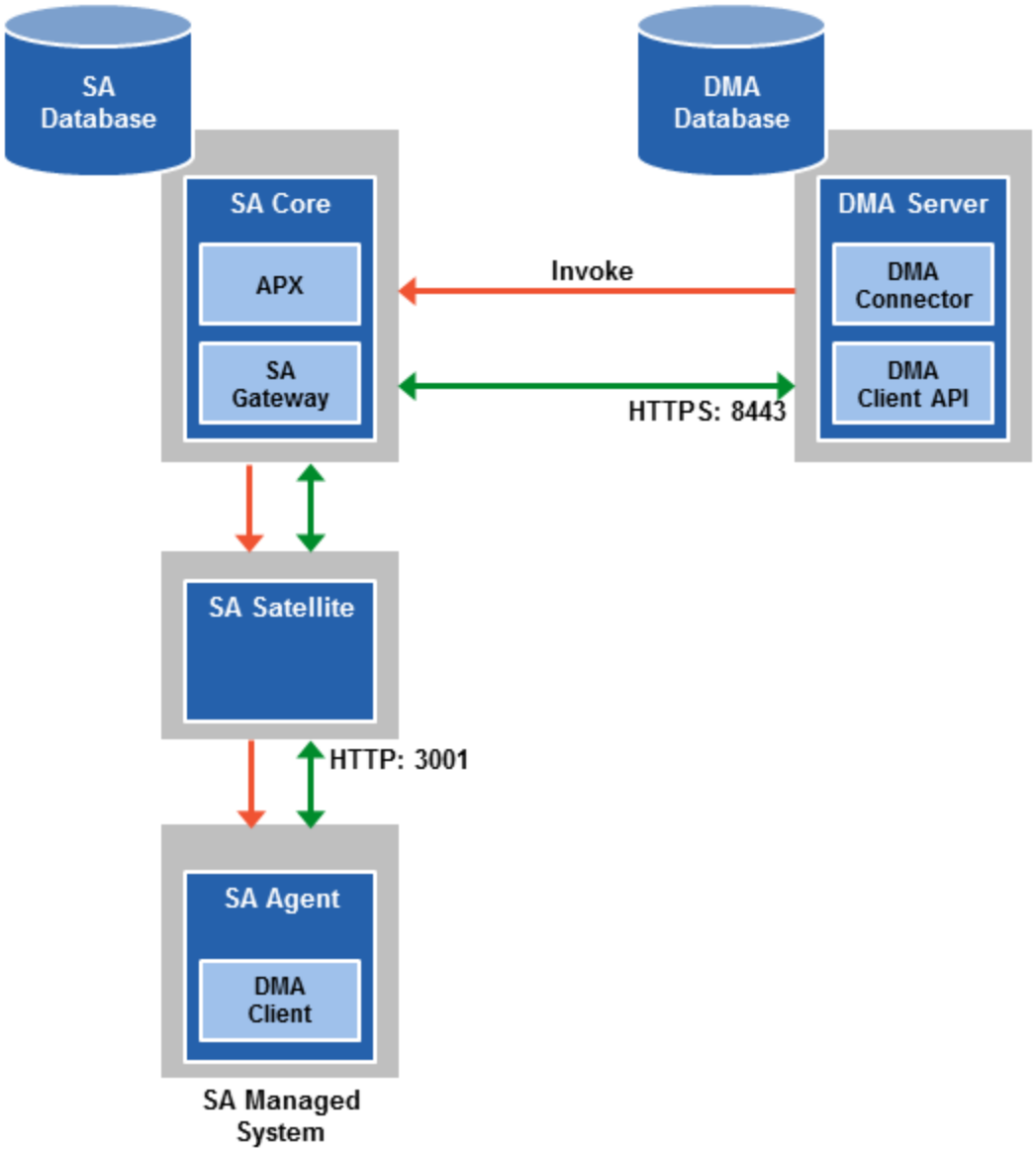
This section describes how to configure Database and Middleware Automation (DMA) and Server Automation (SA) to use the SA Gateway Network as a Proxy Network for DMA communication traffic.

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 routes the information to the DMA Server.

> Note: You can configure DMA with a port other than 8443 (8443 is the default).




# Prerequisites

Before you perform the steps in this section, ensure your environment meets the following requirements:

- An SA mesh environment (SA 10.x) with one or more SA Cores must exist, with optional Satellites (connect Satellite to SA Core over a Gateway).
- You must have administrative access to all SA Core servers within the mesh and the DMA Server.
- DMA 10.10 (or later) is required.

> Note: An existing DMA Server installation is not required. The steps to using SA Gateway Network as a Proxy Network can be completed during the installation process. For more information, see the Install DMA Client for SA in the *DMA Install Guide*.

# Process Overview

Perform the following process to complete the configuration:

1. Add the egress filter to the SA Core Gateway configuration. This is required for the DMA Server to be allowed as a traffic target. (See "Step 1: How to Configure the SA Core Gateway Properties" below.)
2. Add the SA Realm of the SA Core (that the DMA Server is connected to) into the DMA Server context file. (See "Step 2: How to Configure the SA Realm Parameter in the DMA Server" on the next page.)
3. Add and configure the Custom Fields within the DMA Server Environment page. (See "Step 3: How to Add and Configure Custom Fields on the DMA Server" on page 19.)

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

# Step 1: How to Configure the SA Core Gateway Properties

You must add an egressfilter rule to the gateway properties of each slice within the SA Core that the DMA Server is connected to:

1. If it does not exist, create the 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>`).

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

   ```
   opswgw.EgressFilter=tcp:<DMA Server IP Address>:8443:*:*
   ```

3. Restart the gateway by executing the following command:

   ```
   se4. Repeat steps 1-3 for each slice with the same realm within the SA Core to which the DMA Server is connected.rvice opsware-sas restart opswgw-cgws
   ```

4. Repeat steps 1-3 for each slice with the same realm within the SA Core to which the HPEDMA Server is connected.
5. 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
   ```

   You must restart the load balancer gateway after all other gateways.

> **Note:** An egress filter rule is only required on each slice within the same realm within the SA Core that the DMA Server is connected to.

# Step 2: How to Configure the SA Realm Parameter in the DMA Server

If you have already installed the DMAServer, perform the following:

1. Open the following file for editing:

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

2. Ensure that the webServiceUrl parameter is specified with an IP Address.
3. Add the following parameter line beneath the other parameters already specified:

   ```
   <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. Restart the DMA Server by running the following command:

```
service dma restart
```

If you are installing DMA Server, perform the above steps after baselining is completed and before starting the DMA Server.

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

```
<?xml version="1.0" encoding="UTF-8"?>
<Context allowLinking="true" disableURLRewriting="true" path="/dma"
privileged="true" swallowOutput="true" workDir="/var/opt/hp/dma/work/dma">
<Valve className="org.apache.catalina.valves.AccessLogValve"
directory="/var/log/hp/dma/" pattern="%h %l %u %t '%r' %s %b %S"
prefix="localhost_access." suffix=".log"/> <Parameter
name="com.hp.dma.core.webServiceUrl" value="https://192.0.2.0:8443/dma"/>
<Parameter name="com.hp.dma.conn.trustAllCertificates" value="false" />
<Parameter name="com.hp.dma.conn.sa.SAConnector.saRealm" value="REALMNAME" />
```

**Note:** Setting the Realm in the dma.xml file specifies the Realm of the SA Core to which DMA is connected. The client on the target server receives this information when a workflow starts. The DMA client tells the SA agent that the traffic in SA needs to be routed to this Realm so that DMA will receive the communication. The egress filter in the Realm where DMA exists allows the communications in the Realm to leave the SA network and arrive at the DMA server. Because there is no guarantee which slice within the Realm will receive the communication, all slices in the Realm need the egress filter.

**Note:** For more information about specifying the Server Automation Realm, see the Set up a proxy server topic in the *DMA Administration Guide*Set up a proxy server.

# Step 3: How to Add and Configure Custom Fields on the DMA Server

Create and configure the two Custom Fields that instruct DMA to route traffic through the proxy server. you can add and configure the custom fields by using the DMAUI or DMA REST API commands. See the *Developing Guide*.

**Configuring DMA Custom Fields for Proxy Communication**

DMA uses two Custom Fields to control proxy communication:

- west_proxy_in_use tells DMA if a proxy server is used. Valid values are TRUE and FALSE: Or SA_auto_select versus an actual URL.
- 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.

> **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 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 the proxy specified for this server | Use the proxy specified for the organization |
| **Organization value is FALSE** | Use the proxy specified for the server | Do not use the proxy specified 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 the proxy specified for this server | Do not use a proxy for this server |

# 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 Integration 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!