

HP Database and Middleware Automation Solution Packs

For Linux, Solaris, AIX, HP-UX, and Windows

Software Version: 10.00

WebSphere 8 Provisioning User Guide

Document Release Date: February 2013

Software Release Date: December 2012



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 2013 Hewlett-Packard Development Company, L.P.

Trademark Notices

Oracle® and Java® are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Windows® is a U.S. registered trademark of Microsoft Corporation.

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.

Document Changes

Chapter	Version	Changes
Workflow Details	10.00	Synchronized parameter information to the DMA user interface. Made cosmetic and consistency changes.

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

Contents

Contents	5
Audience	8
Document Map	9
Important Terms	10
The WebSphere 8 Provisioning Solution	11
What this Solution Includes	12
Supported Products and Platforms	13
Prerequisites	14
WebSphere 8 Provisioning Quick Start	15
Import the Solution Pack	16
Create a Deployable Workflow	17
Create a Deployment	18
Run Your Workflow	19
View the Results	20
Workflow Details	21
Provision WebSphere 8 and StandAlone	23
Prerequisites for this Workflow	24
How this Workflow Works	26
How to Run this Workflow	30
Sample Scenario	34
Parameters for Provision WebSphere 8 and StandAlone	36
Provision WebSphere 8 and Deployment Manager	40
Prerequisites for this Workflow	41
How this Workflow Works	43
How to Run this Workflow	47
Sample Scenario	51
Parameters for Provision WebSphere 8 and Deployment Manager	53

Provision WebSphere 8 and Custom Node	57
Prerequisites for this Workflow	58
How this Workflow Works	60
How to Run this Workflow	64
Sample Scenario	69
Parameters for Provision WebSphere 8 and Custom Node	72
Provision Websphere 8 Standalone Profile From Existing Install	76
Prerequisites for this Workflow	77
How this Workflow Works	79
How to Run this Workflow	81
Sample Scenario	85
Parameters for Provision WebSphere 8 Standalone Profile from Existing Install	87
Provision Websphere 8 Custom Node Profile From Existing Install	91
Prerequisites for this Workflow	92
How this Workflow Works	94
How to Run this Workflow	96
Sample Scenario	100
Parameters for Provision Websphere 8 Custom Node Profile From Existing Install ...	102
Reference Information	106
WebSphere 8 Product Documentation	106
HP DMA Documentation	106
Tips and Best Practices	107
How this Solution is Organized	108
How to Expose Additional Workflow Parameters	112
How to Use a Policy to Specify Parameter Values	113
Create a Policy	113
Extract a Policy	114
Reference the Policy in the Deployment	114
How to Import a File into the Software Repository	116
Troubleshooting	117
Target Type	117
User Permissions and Related Requirements	117

Discovery in HP DMA	118
Glossary	119

Audience

This solution is designed for IT architects and engineers who are responsible for planning, implementing, and maintaining application-serving environments using IBM WebSphere Application Server Network Deployment version 8 (WebSphere 8).

To use this solution, you should be familiar with WebSphere 8 and its requirements (see links to the [WebSphere 8 Product Documentation](#) on page 106).

Document Map

The following table shows you how to navigate this guide:

Topic	Description
The WebSphere 8 Provisioning Solution	General information about this solution, including what it contains and what it does.
WebSphere 8 Provisioning Quick Start	A step-by-step tutorial that shows you how to run the workflows to provision WebSphere 8.
Workflow Details	Information about the WebSphere 8 workflows included in this solution, including: prerequisites, how it works, how to run it, sample scenarios, and a list of input parameters.
Reference Information	Links to current WebSphere 8 product documentation and additional HP DMA documentation.
Tips and Best Practices	Simple procedures that you can use to accomplish a variety of common HP DMA tasks.
Troubleshooting	Tips for solving common problems.

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 119.

The WebSphere 8 Provisioning Solution

The WebSphere 8 provisioning solution provides tools that you can use to provision many features of a WebSphere 8 environment.

You can use these workflows to automate and simplify the following processes:

- Installing IBM Installation Manager
- Installing IBM WebSphere Application Server Network Deployment version 8 (WebSphere 8)
- Creating stand-alone or custom node profiles for new or existing WebSphere 8 installations

By consistently using the tools provided in this solution, you can quickly, efficiently, and accurately set up your WebSphere 8 environment. You maintain immense flexibility over the architecture by configuring environment-specific information through the input parameters.

What this Solution Includes

The Application Server Provisioning solution pack contains the following WebSphere 8 provisioning composite workflows:

Workflow Name	Purpose
Provision WebSphere 8 and StandAlone	<p>Use this workflow to install the WebSphere 8 Base core binaries and, optionally, create a stand-alone profile.</p> <p>A stand-alone application server works independently—it is not part of a cell and does not interact with a deployment manager. The stand-alone profile is not suitable for distributed application server environments.</p>
Provision WebSphere 8 and Deployment Manager	<p>Use this workflow to install the WebSphere 8 Base core binaries and, optionally, create a deployment manager profile.</p> <p>A deployment manager is the administration point for a cell that contains multiple application servers. This type of profile is appropriate for distributed application server environments.</p>
Provision WebSphere 8 and Custom Node	<p>Use this workflow to install the WebSphere 8 Base core binaries and, optionally, create a custom profile.</p> <p>A custom profile initially contains an empty node with no servers. The workflow can add (federate) the server to the pertinent cell when the profile is created, or you can add it later yourself.</p>
Provision Websphere 8 Standalone Profile From Existing Install	<p>Use this workflow to create a stand-alone profile on an existing WebSphere 8 installation.</p> <p>A stand-alone application server works independently—it is not part of a cell and does not interact with a deployment manager. The stand-alone profile is not suitable for distributed application server environments.</p>
Provision Websphere 8 Custom Node Profile From Existing Install	<p>Use this workflow to create a custom profile on an existing WebSphere 8 installation.</p> <p>A custom profile initially contains an empty node with no servers. The workflow can add (federate) the server to the pertinent cell when the profile is created, or you can add it later yourself.</p>

Supported Products and Platforms

The WebSphere 8 provisioning workflows are supported on Linux and Solaris platforms:

Operating Systems

For specific target operating system versions supported by each workflow, see the *HP Database and Middleware Automation Support Matrix* available on the HP Software Product Manuals web site:

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

Hardware Requirements

For HP DMA server hardware requirements, see the *HP DMA Installation Guide* and the *HP DMA Release Notes* (version 10.00 or later).

HP Software Requirements

This solution requires HP DMA version 10.00 (or later).

Prerequisites

The following prerequisites must be satisfied before you can run the WebSphere 8 provisioning workflows in this solution pack:

Per the IBM WebSphere 7 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server version 7 on 64-bit Red Hat Linux targets:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 ksh-20080202-14 gtk2-2.10.4-20 gtk2-engines-2.8.0-3 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 rpm-build-4.4.2-37.architecture.el5 (or later) elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48
64-bit Red Hat Enterprise Linux version 6	compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 ksh-20100621-2 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 rpm-build-4.8.0-12 elfutils-0.148-1 elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13

Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.

Note: Be sure to review the additional prerequisites for each workflow.

Chapter 1

WebSphere 8 Provisioning Quick Start

This tutorial shows you how to install a solution pack and run a simple workflow. There are five basic steps:

1. [Import the Solution Pack](#) on next page
2. [Create a Deployable Workflow](#) on page 17
3. [Create a Deployment](#) on page 18
4. [Run Your Workflow](#) on page 19
5. [View the Results](#) on page 20

In this tutorial, default values will be used for most input parameters. Before executing these steps, make sure that these default values are suitable for your environment.

Note: See the "Parameter" topic associated with each workflow for descriptions of all available input parameters for your workflow, including default values.

The information presented in this tutorial assumes the following:

- HP DMA is installed and operational.
- At least one valid target is available.

Note: This tutorial is included in every HP DMA solution pack user guide. To skip directly to information about the Application Server Provisioning workflows, see the [Workflow Details](#).

Import the Solution Pack

The following instructions assume that you have purchased a license for the HP DMA solution pack that you want to import.

The HP DMA 10.00 solution packs are included on the HP DMA 10.00 installation media. They are located in the following folders:

- The `DMA_10.0_Server_and_Client` folder contains the Discovery solution pack.
- The `DMA_10.0_Database_Solution_Packs` folder contains all of the database solution packs (provisioning, advanced provisioning, patching, advanced patching, compliance, refresh, and release management).
- The `DMA_10.0_Middleware_Solution_Packs` folder contains all of the application server solution packs (provisioning, patching, and release management).

Note: The Discovery solution pack is not automatically installed in HP HP DMA version 10.00 (and later). You must import it if you want to use the discovery workflows.

Always check to see if there are more recent versions of the HP DMA solution packs available online. Due to frequent releases, it is likely that the solution packs provided on the installation media have since been updated.

To install the solution pack:

1. Go to [HP Live Network](#) to view a list of the latest available HP 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: `ASProvisioning.zip`).

Note: This ZIP file may be included in a larger ZIP file that contains multiple solution packs.

4. On the system where you downloaded the solution pack, open a web browser, and go to the following address:

`https://<HP_DMAserver>:8443/dma/login`
5. Log in to the HP DMA server using an account 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**.

Create a Deployable Workflow

The workflow templates provided by HP in your solution pack are read-only and cannot be deployed. When you are viewing a read-only item in the HP DMA web UI, you will see the lock icon in the lower right corner:

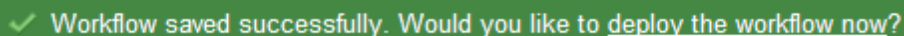


Read-only workflows are not deployable. You can create a deployable workflow by making a copy of a workflow template.¹

To create a deployable copy of the workflow template:

1. In the HP DMA web interface, go to Automation > Workflows.
2. From the list of workflows, select the workflow template that you want to use (for example, Provision WebSphere 8 and StandAlone).
3. Click the **Copy** button in the lower left corner.
4. On the Documentation tab, specify the following:
 - Name – Name that will appear in the list of available workflows
 - Tags – Keywords that you can use later to search for this workflow (optional)
 - Type – Either OS or the specific type of database (the correct type will be selected as a result of the copy)
 - Target level – Server, Instance, or Database (the correct target level will be selected as a result of the copy)
5. On the Roles tab, grant Read access to at least one user or group and Write access to at least one user or group.
6. Click **Save**.

Your new workflow now appears in the list of available workflows, and the following message is displayed:



Workflow saved successfully. Would you like to [deploy the workflow now?](#)

7. Click the **deploy the workflow now** link in the green message bar.

¹For more information about creating and working with workflows, see “Workflows” in the *HP DMA User Guide*. This document is available on the HP Software Product Manuals web site: <http://h20230.www2.hp.com/selfsolve/manuals>

Create a Deployment

Before you can run your new workflow, you must create a deployment. A deployment associates a workflow with one or more specific targets (servers, instances, or databases).

To create a deployment:

1. If you do not see the green message bar—for example, if you navigated to another page after you created your copy of the workflow template—follow these steps:
 - a. Go to the Automation > Deployments page.
 - b. In the lower right corner, click **New deployment**.
2. Specify the following:
 - Name – Name that will appear in the list of available deployments.
 - Workflow – From the drop-down list, select the deployable workflow that you just created.
 - Schedule – Frequency or date when the workflow will run. If you select None, the workflow will run only once when you explicitly tell it to run.
3. From the list of AVAILABLE servers on the left side of the Targets area, click the **ADD** link for the target (or targets) where the workflow will run.

Note: If you are running a bridged execution workflow, the targets that you select on the Deployment page will be included in the lists of available targets that you can choose from on the Run page.

For more information about bridged execution workflows, see the *HP DMA User Guide*. This document is available on the HP Software Product Manuals web site:
<http://h20230.www2.hp.com/selfsolve/manuals>

4. On the Parameters tab, specify values for the input parameters listed there.

These are a subset of the required parameters for this workflow. Parameters that are not visible in the deployment will have default values.

Note: See the [Workflow Details](#) included in this guide for descriptions of all available input parameters for your workflow, including default values.

5. If you do not want to explicitly enter the values here, you can create a policy that stores the values and then reference that policy in your deployment (see [How to Use a Policy to Specify Parameter Values](#) on page 113).
6. Click **Save**.

Your new deployment now appears in the list of available workflows, and the following message is displayed:

✓ Deployment saved successfully. Would you like to [run the workflow now?](#)

7. Click the **run the workflow now** link in the green message bar.

Run Your Workflow

Now you are ready to run your workflow against the server that you selected.

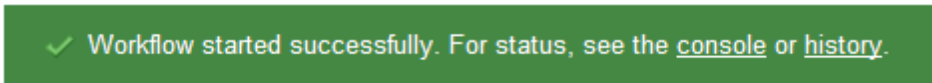
To run the workflow:

1. If you do not see the green message bar—for example, if you navigated to another page after you created your deployment—follow these steps:
 - a. Go to the Automation > Run page.
 - b. In the list of WORKFLOWS on the left side, select the workflow that you created.
 - c. In the list of DEPLOYMENTS on the right side, select the deployment that you just created.

2. If you are running a single-target workflow, select the check box for each target where you want to run the workflow.

If you are running a bridged execution workflow, click the **SELECT** link to specify each target. The targets that are available to choose from here are the targets that you selected on the Deployment page.

3. Click the **Run workflow** button.
4. The following message is displayed:



✓ Workflow started successfully. For status, see the [console](#) or [history](#).

5. To view the progress of your deployment, click the **console** link in the green message bar.

View the Results

While your workflow is running, you can watch its progress on the Automation > Console page.

- To view the progress of the workflow as the deployment proceeds, click the workflow name in the upper box on the Console page.
- To view the outcome of a specific step, select that step in the left box in the Output area. Informational messages are displayed in the right box, and the values of any output parameters are listed.

While the workflow is running, its status indicator on the Console says **RUNNING**. After the workflow finishes, its status indicator changes to **SUCCESS**, **FAILURE**, or **FINISHED**.

After the workflow has finished running, you can view a summary of your deployment on the History page. This page lists all the workflows that have run on this HP DMA server during the time period specified in the Filter box.

To view step-by-step results, select the row in the table that corresponds to your deployment. The tabs below the table show you information about each step in the workflow. This includes the start and end time for each step, the exit code, and the following information:

- Output tab – any informational messages that were produced
- Errors tab – any errors that were reported
- Header tab – values assigned to any output parameters

Chapter 2

Workflow Details

The Application Server Provisioning solution pack contains the following WebSphere 8 provisioning workflows. You can run these workflows ad-hoc for custom WebSphere 8 installations or create reusable deployments to standardize WebSphere 8 installations in your environment.

Workflow Name	Purpose
Provision WebSphere 8 and StandAlone	<p>Use this workflow to install the WebSphere 8 Base core binaries and, optionally, create a stand-alone profile.</p> <p>A stand-alone application server works independently—it is not part of a cell and does not interact with a deployment manager. The stand-alone profile is not suitable for distributed application server environments.</p>
Provision WebSphere 8 and Deployment Manager	<p>Use this workflow to install the WebSphere 8 Base core binaries and, optionally, create a deployment manager profile.</p> <p>A deployment manager is the administration point for a cell that contains multiple application servers. This type of profile is appropriate for distributed application server environments.</p>
Provision WebSphere 8 and Custom Node	<p>Use this workflow to install the WebSphere 8 Base core binaries and, optionally, create a custom profile.</p> <p>A custom profile initially contains an empty node with no servers. The workflow can add (federate) the server to the pertinent cell when the profile is created, or you can add it later yourself.</p>
Provision Websphere 8 Standalone Profile From Existing Install	<p>Use this workflow to create a stand-alone profile on an existing WebSphere 8 installation.</p> <p>A stand-alone application server works independently—it is not part of a cell and does not interact with a deployment manager. The stand-alone profile is not suitable for distributed application server environments.</p>
Provision Websphere 8 Custom Node Profile From Existing Install	<p>Use this workflow to create a custom profile on an existing WebSphere 8 installation.</p> <p>A custom profile initially contains an empty node with no servers. The workflow can add (federate) the server to the pertinent cell when the profile is created, or you can add it later yourself.</p>

Each workflow included in this solution pack has a set of input parameters whose values will be unique to your environment. If you provide correct values for the parameters that each scenario requires, the workflow will be able to accomplish its objective.

There are two steps required to customize this solution:

1. Ensure that all required parameters are visible. You do this by using the workflow editor.

For simple provisioning scenarios, you can use the default values for most parameters. To use this solution's more advanced features, you will need to expose additional parameters.

2. Specify the values for those parameters. You do this when you create a deployment.

Tip: Detailed instructions are provided in the "How to Use this Workflow" topic associated with each workflow.

The information presented here assumes the following:

- HP DMA is installed and operational.
- At least one suitable target server is available (see [Supported Products and Platforms](#) on page 13).
- You are logged in to the HP DMA web interface.
- You have permission to create, edit, and deploy copies of the workflows included in this solution pack.

Tip: All parameters used by the workflows in this solution are described in the "Parameters" topic associated with each workflow.

Provision WebSphere 8 and StandAlone

Use this workflow to install the WebSphere 8 Base core binaries and, optionally, create a stand-alone profile.

A stand-alone application server works independently—it is not part of a cell and does not interact with a deployment manager. The stand-alone profile is not suitable for distributed application server environments.

To use this workflow in your environment, see the following information:

Topic	Information Included
Prerequisites for this Workflow	List of prerequisites that must be satisfied before you can run this workflow
How this Workflow Works	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
How to Run this Workflow	Instructions for running this workflow in your environment
Sample Scenario	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere 8 and StandAlone workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically root) who can access all required files and directories.
2. Per the IBM WebSphere 7 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server version 7 on 64-bit Red Hat Linux targets:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 ksh-20080202-14 gtk2-2.10.4-20 gtk2-engines-2.8.0-3 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 rpm-build-4.4.2-37.architecture.el5 (or later) elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48
64-bit Red Hat Enterprise Linux version 6	compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 ksh-20100621-2 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 rpm-build-4.8.0-12 elfutils-0.148-1 elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13

Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.

3. This workflow will install WebSphere Application Server as root because of the following IBM documented limitations:
 - Creation of a Linux service for WebSphere Application Server
 - Native registration with the operating system

- Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 8, refer to the [WebSphere 8 Product Documentation](#) on page 106.

How this Workflow Works

This topic contains the following information about the [Provision WebSphere 8 and StandAlone](#) workflow:

Overview

This workflow does the following three things in the order shown:

1. Installs the IBM Install Manager
2. Installs IBM WebSphere Application Server Network Deployment version 8
3. Creates a stand-alone profile

The workflow checks to see if the WebSphere 8 binary archive files exist on the target machine. If they do not, the files are downloaded from the software repository (for more information, see [How to Import a File into the Software Repository](#) on page 116).

See the following topics for detailed information:

[Validation Checks Performed](#)

[Steps in this Workflow](#)

[Process Flow](#)

Note: This workflow has been updated to account for the significant changes in the way that WebSphere 8 is installed.

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks for Red Hat Linux.

The workflow first performs the following parameter checks:

1. None of the following characters are used in the Admin User, Cell Name, Node Name, or Profile Name parameters: / \ * , : ; = + ? | < > & % ' " [] # \$ ^ { }
2. If Enable Security is true, Admin Password and Admin User are specified.
3. Admin Password (if specified) does not begin with a dash or contain a space.
4. Admin User (if specified) does not begin with a dash, a period, or a space.
5. Profile Name does not begin with a period.
6. Personal CertDN and Signing CertDN do not contain spaces.
7. If Ports File is specified, Validate Ports is true.
8. All specified file names are legal file names.

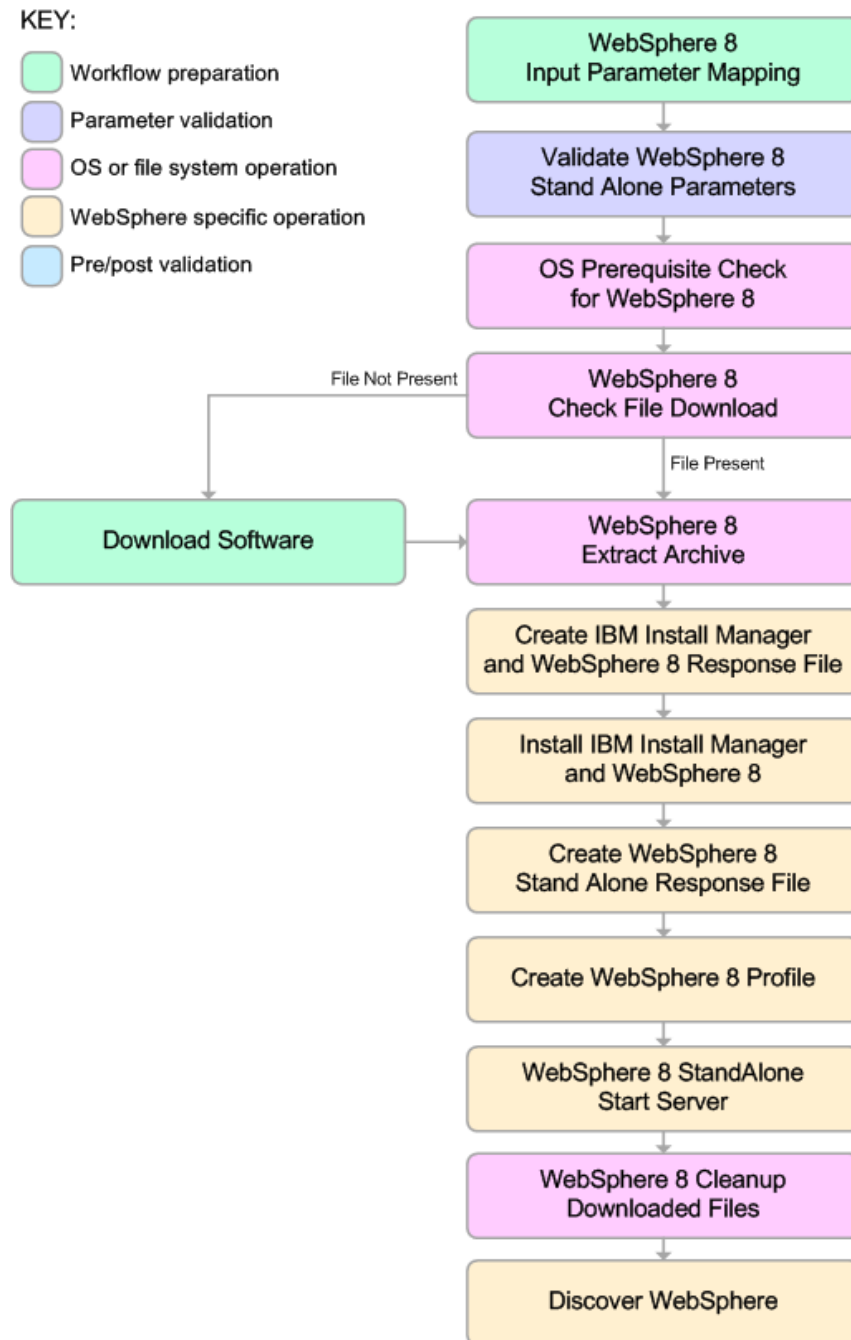
The workflow then performs the following operating system checks on the target machine:

1. All required libraries are present (see [Prerequisites for this Workflow](#) on page 24).
2. Sufficient disk space is available to install WebSphere 8.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

The Provision WebSphere 8 and StandAlone workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.

Click each box in the diagram to view additional information about that step.



Process Flow

This workflow performs the following tasks:

1. Creates the call wrapper and determines the target server platform type.
2. Validates the parameters needed to install WebSphere 8 and create a stand-alone profile (see [Validation Checks Performed](#) on page 27).
3. Checks the following:
 - a. Documented library requirements for WebSphere 8(see the [Prerequisites for this Workflow](#) on page 24).
 - b. File system space requirements where WebSphere 8 will be installed.
 - c. Temporary space requirements where the compressed software will be extracted before it is installed.
4. Determines whether the WebSphere 8 binary archive is present on the target machine. If the archive is not present, the workflow downloads it from the software repository (see [How to Import a File into the Software Repository](#) on page 116).
5. Extracts the WebSphere 8 binary archive to the specified directory.
6. Creates a response file for the purpose of installing a new instance of WebSphere 8.
7. Installs the IBM Installation Manager and a new WebSphere 8 instance on the target server.
8. Creates a new response file for the purpose of creating a stand-alone profile on top of the WebSphere 8 installation.
9. Creates a stand-alone profile on top of the WebSphere 8 installation.
10. Starts the new stand-alone WebSphere 8 application server.
11. Cleans up any files that were downloaded.
12. *Optional:* Discovers any WebSphere 8 cells, clusters, and managed servers associated with the Profile Root that you specify. If these items are found, they are added to the HP DMA environment.

How to Run this Workflow

The following instructions show you how to customize and run the [Provision WebSphere 8 and StandAlone](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in [Parameters for Provision WebSphere 8 and StandAlone](#) on page 36.

Note: Before following this procedure, review the [Prerequisites for this Workflow](#), and ensure that all requirements are satisfied.

To customize and run the Provision WebSphere 8 and StandAlone workflow:

1. Create a deployable copy of the workflow (see [Create a Deployable Workflow](#) on page 17).
2. Determine the values that you will specify for the following parameters:

Parameters Defined in this Step: Validate WebSphere 8 Stand Alone Parameters

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash (-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }.
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Install Manager Binary Location	no default	required	Fully qualified path to the compressed Install Manager software package on the target machine.

Parameters Defined in this Step: Validate WebSphere 8 Stand Alone Parameters (continued)

Parameter Name	Default Value	Required	Description
Install Manager Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Install Manager Install Location	no default	required	Fully qualified path where Install Manager will be installed.
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Server Name	no default	required	Name of the application server that will be created under the profile.
WebSphere Binary Location	no default	required	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Parameters Defined in this Step: Discover WebSphere

Parameter Name	Default Value	Required	Description
Known Profile Roots	no default	optional	Comma delimited list of any known (or suspected) PROFILE_ROOTs. Use this to discover WebSphere cells which aren't currently running.
Trust SSL Certificates	False	optional	If "True", this step will trust any SSL used to connect to the DMA Web Service.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service URL	see description	required	URL for the discovery web service API. The default is: <code>https://host:8443/dma</code>
Web Service User	administrator	required	User capable of modifying the managed environment through the discovery web service API.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your provisioning objectives.

See [Parameters for Provision WebSphere 8 and StandAlone](#) on page 36 for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see [How to Use a Policy to Specify Parameter Values](#) on page 113).

3. In the workflow editor, expose any additional parameters that you need (see [How to Expose Additional Workflow Parameters](#) on page 112). You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment (see [Create a Deployment](#) on page 18 for instructions).
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment (see [Run Your Workflow](#) on page 19 for instructions).

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Be sure to also perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

```
WAS_ROOT/bin/versionInfo.sh
```

Here, *WAS_ROOT* is the directory where WebSphere 8 is installed. This is the path that you specified in the WebSphere Install Location parameter.

2. Validate that the profile has been created and is running by doing the following:

- a. View the *WAS_ROOT/profiles/PROFILE_NAME/logs/AboutThisProfile.txt* file. This file is created after the creation of the profile and contains specific information about the profile.

Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.

- b. Change to the *WAS_ROOT/profiles/PROFILE_NAME/logs/CELL_NAME* directory, and tail the *SystemOut.log* file. Look for the following line:

```
Server CELL_NAME open for e-business
```

Here, *CELL_NAME* is the name of the WebSphere 8 cell to which this profile pertains. This is the name that you specified in the Cell Name parameter.

Sample Scenario

This topic shows you typical parameter values used for the [Provision WebSphere 8 and StandAlone](#) workflow.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see [How to Use a Policy to Specify Parameter Values](#) on page 113).

New Install with Standalone Profile – Parameter Value Examples

Parameter Name	Example Value	Description
Admin Password	wasPassWord	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Admin User	wasadmin	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }.
Cell Name	DevCell	Unique cell name that does not contain any of the following special characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	true	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Install Manager Binary Location	/opt/IBM/iim/IBM_Install_Manager_Linux.zip	Fully qualified path to the compressed Install Manager software package on the target machine.
Install Manager Extract Location	/opt/IBM/iim	Fully qualified path where the compressed software will be extracted on the target machine.
Install Manager Install Location	/opt/IBM/installManager	Fully qualified path where Install Manager will be installed.

New Install with Standalone Profile – Parameter Value Examples (continued)

Parameter Name	Example Value	Description
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	DevNode	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	standAlone	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Server Name	Server1	Name of the application server that will be created under the profile.
WebSphere Binary Location	/opt/IBM/wasv8/WAS_V8.0_disk1.zip, /opt/IBM/wasv8/WAS_V8.0_disk2.zip,	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Extract Location	/opt/IBM/wasv8	Fully qualified path where the compressed software will be extracted on the target machine.
WebSphere Install Location	/opt/IBM/WebSphere8/AppServer	Fully qualified path where WebSphere will be installed.

Parameters for Provision WebSphere 8 and StandAlone

The following tables describe the required and optional input parameters for this workflow. Most of these parameters are not initially visible in a deployment (see [How to Expose Additional Workflow Parameters](#) on page 112). For most parameters, if you do not specify a value for a parameter, a default value is assigned

Parameters Defined in this Step: Validate WebSphere 8 Stand Alone Parameters

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash (-) or contain a space().
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash (-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. Defaults are: UNIX targets: <code>/opt/hp/dma/client/jython.sh</code> running as root Windows targets: <code>jython</code> running as Administrator
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Default Ports	false	optional	Provides the option to assign default ports to a profile. Valid values are true or false. If true, the WebSphere Application Server default ports will be used, and the Ports File and Starting Port parameters should not have values. If false, the workflow will increment the default port until it finds a free port. The default value is false.
Developer Server	no default	optional	Use this parameter for development environments only to help with start up time. Valid value is true. Do not use in production environments.
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.

Parameters Defined in this Step: Validate WebSphere 8 Stand Alone Parameters (continued)

Parameter Name	Default Value	Required	Description
Host Name	Server.name	required	Hostname or IP address of the target machine.
Install Manager Binary Location	no default	required	Fully qualified path to the compressed Install Manager software package on the target machine.
Install Manager Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Install Manager Install Location	no default	required	Fully qualified path where Install Manager will be installed.
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Omit Action	no default	optional	Enables you to prevent certain optional features from being installed. Valid values are deployAdminConsole or defaultAppDeployAndConfig. You may only specify one of these options.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmlab-example.com,OU=WAS7LabCell,OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.

Parameters Defined in this Step: Validate WebSphere 8 Stand Alone Parameters (continued)

Parameter Name	Default Value	Required	Description
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_adminhost=9060). This option should be used with the Validate Ports option.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Profile Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation.
Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Name	no default	required	Name of the application server that will be created under the profile.
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: CN=dmalab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.
Starting Port	no default	optional	Starting port number that the profile will use to generate and assign port values. Port values are assigned sequentially from the Starting Port. Do not specify this parameter if you specify Default Ports or Ports File.

Parameters Defined in this Step: Validate WebSphere 8 Stand Alone Parameters (continued)

Parameter Name	Default Value	Required	Description
Validate Ports	no default	optional	Indicates that the ports should be validated to ensure that they are not already in use. Valid values are true or false. You should use this option if you specify a Ports File.
WebSphere Binary Location	no default	required	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Parameters Defined in this Step: Discover WebSphere

Parameter Name	Default Value	Required	Description
Known Profile Roots	no default	optional	Comma delimited list of any known (or suspected) PROFILE_ROOTs. Use this to discover WebSphere cells which aren't currently running.
Trust SSL Certificates	False	optional	If "True", this step will trust any SSL used to connect to the DMA Web Service.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service URL	see description	required	URL for the discovery web service API. The default is: <code>https://host:8443/dma</code>
Web Service User	administrator	required	User capable of modifying the managed environment through the discovery web service API.

Provision WebSphere 8 and Deployment Manager

Use this workflow to install the WebSphere 8 Base core binaries and, optionally, create a deployment manager profile.

A deployment manager is the administration point for a cell that contains multiple application servers. This type of profile is appropriate for distributed application server environments.

To use this workflow in your environment, see the following information:

Topic	Information Included
Prerequisites for this Workflow	List of prerequisites that must be satisfied before you can run this workflow
How this Workflow Works	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
How to Run this Workflow	Instructions for running this workflow in your environment
Sample Scenario	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere 8 and Deployment Manager workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically root) who can access all required files and directories.
2. Per the IBM WebSphere 7 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server version 7 on 64-bit Red Hat Linux targets:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 ksh-20080202-14 gtk2-2.10.4-20 gtk2-engines-2.8.0-3 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 rpm-build-4.4.2-37.architecture.el5 (or later) elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48
64-bit Red Hat Enterprise Linux version 6	compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 ksh-20100621-2 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 rpm-build-4.8.0-12 elfutils-0.148-1 elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13

Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.

3. This workflow will install WebSphere Application Server as root because of the following IBM documented limitations:
 - Creation of a Linux service for WebSphere Application Server
 - Native registration with the operating system

- Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 8, refer to the [WebSphere 8 Product Documentation](#) on page 106.

How this Workflow Works

This topic contains the following information about the [Provision WebSphere 8 and Deployment Manager](#) workflow:

Overview

This workflow does the following three things in the order shown:

1. Installs the IBM Install Manager
2. Installs IBM WebSphere Application Server Network Deployment version 8
3. Creates a Deployment Manager profile

The workflow checks to see if the WebSphere 8 binary archive files exist on the target machine. If they do not, the files are downloaded from the software repository (for more information, see [How to Import a File into the Software Repository](#) on page 116).

See the following topics for detailed information:

[Validation Checks Performed](#)

[Steps in this Workflow](#)

[Process Flow](#)

Note: This workflow has been updated to account for the significant changes in the way that WebSphere 8 is installed.

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks for Red Hat Linux.

The workflow first performs the following parameter checks:

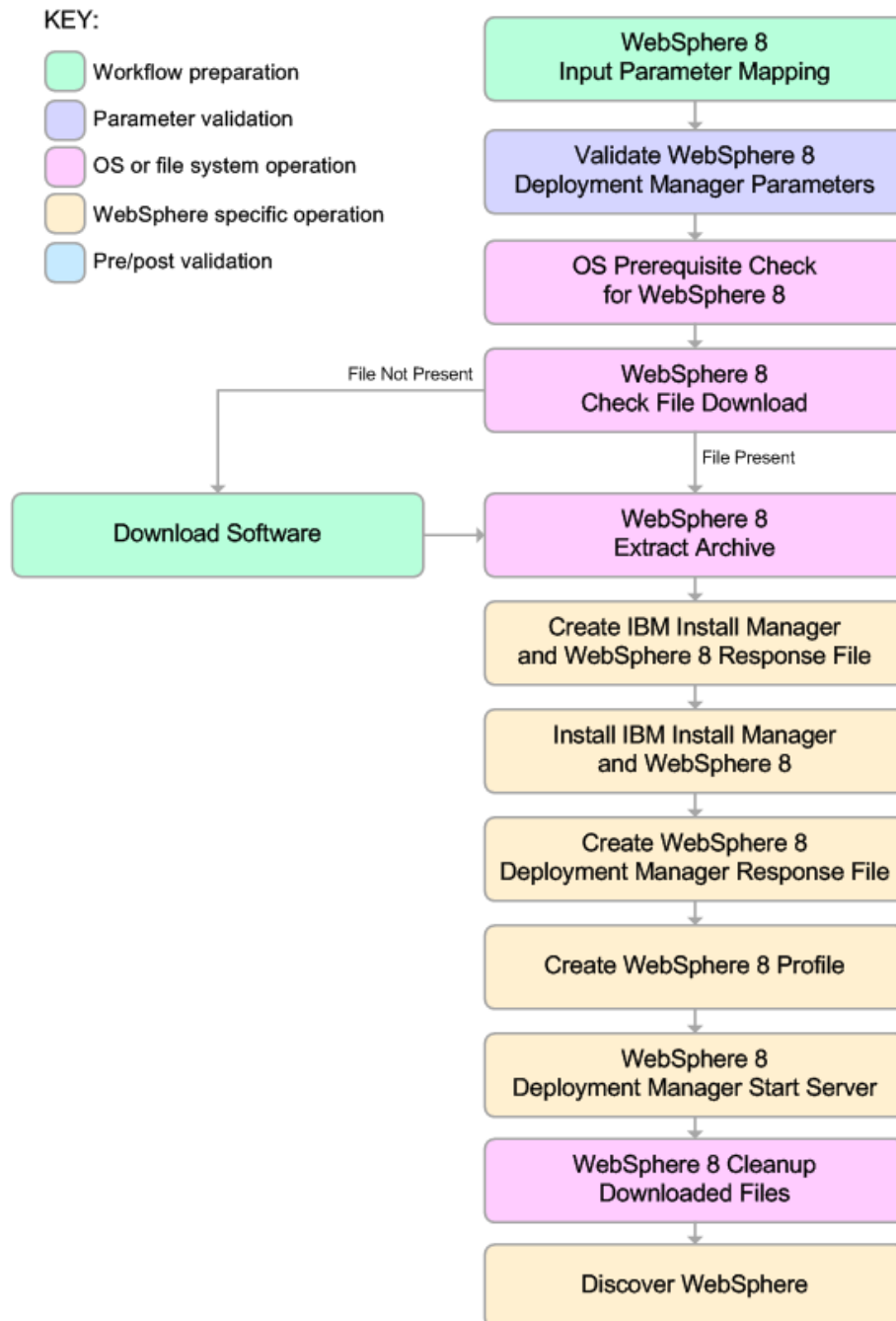
1. None of the following characters are used in the Admin User, Cell Name, Node Name, or Profile Name parameters: / \ * , : ; = + ? | < > & % ' " [] # \$ ^ { }
2. If Enable Security is true, Admin Password and Admin User are specified.
3. Admin Password (if specified) does not begin with a dash or contain a space.
4. Admin User (if specified) does not begin with a dash, a period, or a space.
5. Profile Name does not begin with a period.
6. Personal CertDN and Signing CertDN do not contain spaces.
7. If Ports File is specified, Validate Ports is true.
8. All specified file names are legal file names.

The workflow then performs the following operating system checks on the target machine:

1. All required libraries are present (see [Prerequisites for this Workflow](#) on page 41).
2. Sufficient disk space is available to install WebSphere 8.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

The Provision WebSphere 8 and Deployment Manager workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Process Flow

This workflow performs the following tasks:

1. Creates the call wrapper and determines the target server platform type.
2. Validates the parameters needed to install WebSphere 8 and create a Deployment Manager profile (see [Validation Checks Performed](#) on page 44).
3. Checks the following:
 - a. Documented library requirements for WebSphere 8(see the [Prerequisites for this Workflow](#) on page 41).
 - b. File system space requirements where WebSphere 8 will be installed.
 - c. Temporary space requirements where the compressed software will be extracted before it is installed.
4. Determines whether the WebSphere 8 binary archive is present on the target machine. If the archive is not present, the workflow downloads it from the software repository (see [How to Import a File into the Software Repository](#) on page 116).
5. Extracts the WebSphere 8 binary archive to the specified directory.
6. Creates a response file for the purpose of installing a new instance of WebSphere 8.
7. Installs the IBM Installation Manager and a new WebSphere 8 instance on the target server.
8. Creates a new response file for the purpose of creating a Deployment Manager profile on top of the WebSphere 8 installation.
9. Creates a Deployment Manager profile on top of the WebSphere 8 installation.
10. Starts the new Deployment Manager WebSphere 8 application server.
11. Cleans up any files that were downloaded.
12. *Optional:* Discovers any WebSphere 8 cells, clusters, and managed servers associated with the Profile Root that you specify. If these items are found, they are added to the HP DMA environment.

How to Run this Workflow

The following instructions show you how to customize and run the [Provision WebSphere 8 and Deployment Manager](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in [Parameters for Provision WebSphere 8 and Deployment Manager](#) on page 53.

Note: Before following this procedure, review the [Prerequisites for this Workflow](#) on page 41, and ensure that all requirements are satisfied.

To customize and run the Provision WebSphere 8 and Deployment Manager workflow:

1. Create a deployable copy of the workflow (see [Create a Deployable Workflow](#) on page 17).
2. Determine the values that you will specify for the following parameters:

Parameters Defined in this Step: Validate WebSphere 8 Deployment Manager Parameters

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash (-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }.
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Install Manager Binary Location	no default	required	Fully qualified path to the compressed Install Manager software package on the target machine.

Parameters Defined in this Step: Validate WebSphere 8 Deployment Manager Parameters (continued)

Parameter Name	Default Value	Required	Description
Install Manager Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Install Manager Install Location	no default	required	Fully qualified path where Install Manager will be installed.
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Server Name	no default	required	Name of the application server that will be created under the profile.
WebSphere Binary Location	no default	required	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Parameters Defined in this Step: Discover WebSphere

Parameter Name	Default Value	Required	Description
Known Profile Roots	no default	optional	Comma delimited list of any known (or suspected) PROFILE_ROOTs. Use this to discover WebSphere cells which aren't currently running.
Trust SSL Certificates	False	optional	If "True", this step will trust any SSL used to connect to the DMA Web Service.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service URL	see description	required	URL for the discovery web service API. The default is: <code>https://host:8443/dma</code>
Web Service User	administrator	required	User capable of modifying the managed environment through the discovery web service API.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your provisioning objectives.

See [Parameters for Provision WebSphere 8 and Deployment Manager](#) on page 53 for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see [How to Use a Policy to Specify Parameter Values](#) on page 113).

3. In the workflow editor, expose any additional parameters that you need (see [How to Expose Additional Workflow Parameters](#) on page 112). You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment (see [Create a Deployment](#) on page 18 for instructions).
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment (see [Run Your Workflow](#) on page 19 for instructions).

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Be sure to also perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

```
WAS_ROOT/bin/versionInfo.sh
```

Here, *WAS_ROOT* is the directory where WebSphere 8 is installed. This is the path that you specified in the WebSphere Install Location parameter.

2. Validate that the profile has been created and is running by doing the following:

- a. View the *WAS_ROOT/profiles/PROFILE_NAME/logs/AboutThisProfile.txt* file. This file is created after the creation of the profile and contains specific information about the profile.

Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.

- b. Change to the *WAS_ROOT/profiles/PROFILE_NAME/logs/CELL_NAME* directory, and tail the *SystemOut.log* file. Look for the following line:

```
Server CELL_NAME open for e-business
```

Here, *CELL_NAME* is the name of the WebSphere 8 cell to which this profile pertains. This is the name that you specified in the Cell Name parameter.

Sample Scenario

This topic shows you typical parameter values used for the [Provision WebSphere 8 and Deployment Manager](#) workflow.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see [How to Use a Policy to Specify Parameter Values](#) on page 113).

New Install with Deployment Manager – Parameter Value Examples

Parameter Name	Example Value	Description
Admin Password	wasadmin	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Admin User	wasadmin	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }.
Cell Name	Dev CellManager	Unique cell name that does not contain any of the following special characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	true	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Install Manager Binary Location	/opt/IBM/iim/IBM_Install_Manager_Linux.zip	Fully qualified path to the compressed Install Manager software package on the target machine.
Install Manager Extract Location	/opt/IBM/iim	Fully qualified path where the compressed software will be extracted on the target machine.
Install Manager Install Location	/opt/IBM/installManager	Fully qualified path where Install Manager will be installed.

New Install with Deployment Manager – Parameter Value Examples (continued)

Parameter Name	Example Value	Description
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	DevManager	Unique node name that cannot contain any of the following special characters / \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	DevDmgr	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }.
WebSphere Binary Location	/opt/IBM/wasv8/WAS_V8.0_disk1.zip, /opt/IBM/wasv8/WAS_V8.0_disk2.zip,	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Extract Location	/opt/IBM/wasv8	Fully qualified path where the compressed software will be extracted on the target machine.
WebSphere Install Location	/opt/IBM/WebSphere8/AppServer	Fully qualified path where WebSphere will be installed.

Parameters for Provision WebSphere 8 and Deployment Manager

The following tables describe the required and optional input parameters for this workflow. Most of these parameters are not initially visible in a deployment (see [How to Expose Additional Workflow Parameters](#) on page 112). For most parameters, if you do not specify a value for a parameter, a default value is assigned

Input Parameters Defined in this Step: Validate WebSphere 8 Deployment Manager Parameters

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash (-) or contain a space().
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash (-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. Defaults are: UNIX targets: <code>/opt/hp/dma/client/jython.sh</code> running as root Windows targets: <code>jython</code> running as Administrator
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Default Ports	false	optional	Provides the option to assign default ports to a profile. Valid values are true or false. If true, the WebSphere Application Server default ports will be used, and the Ports File and Starting Port parameters should not have values. If false, the workflow will increment the default port until it finds a free port. The default value is false.
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Host Name	Server.name	required	Hostname or IP address of the target machine.

Input Parameters Defined in this Step: Validate WebSphere 8 Deployment Manager Parameters (continued)

Parameter Name	Default Value	Required	Description
Install Manager Binary Location	no default	required	Fully qualified path to the compressed Install Manager software package on the target machine.
Install Manager Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Install Manager Install Location	no default	required	Fully qualified path where Install Manager will be installed.
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Omit Action	no default	optional	Enables you to prevent certain optional features from being installed. Valid values are deployAdminConsole or defaultAppDeployAndConfig. You may only specify one of these options.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmlab-example.com,OU=WAS7LabCell,OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.

Input Parameters Defined in this Step: Validate WebSphere 8 Deployment Manager Parameters (continued)

Parameter Name	Default Value	Required	Description
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_adminhost=9060). This option should be used with the Validate Ports option.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Profile Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation.
Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Signing CertDN	no default	optional	<p>Distinguished name of the signing certificate. For example:</p> <p>CN=dmalab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US</p> <p>The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.</p>
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.
Starting Port	no default	optional	Starting port number that the profile will use to generate and assign port values. Port values are assigned sequentially from the Starting Port. Do not specify this parameter if you specify Default Ports or Ports File.

Input Parameters Defined in this Step: Validate WebSphere 8 Deployment Manager Parameters (continued)

Parameter Name	Default Value	Required	Description
Validate Ports	no default	optional	Indicates that the ports should be validated to ensure that they are not already in use. Valid values are true or false. You should use this option if you specify a Ports File.
WebSphere Binary Location	no default	required	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Parameters Defined in this Step: Discover WebSphere

Parameter Name	Default Value	Required	Description
Known Profile Roots	no default	optional	Comma delimited list of any known (or suspected) PROFILE_ROOTs. Use this to discover WebSphere cells which aren't currently running.
Trust SSL Certificates	False	optional	If "True", this step will trust any SSL used to connect to the DMA Web Service.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service URL	see description	required	URL for the discovery web service API. The default is: <code>https://host:8443/dma</code>
Web Service User	administrator	required	User capable of modifying the managed environment through the discovery web service API.

Provision WebSphere 8 and Custom Node

Use this workflow to install the WebSphere 8 Base core binaries and, optionally, create a custom profile.

A custom profile initially contains an empty node with no servers. The workflow can add (federate) the server to the pertinent cell when the profile is created, or you can add it later yourself.

To use this workflow in your environment, see the following information:

Topic	Information Included
Prerequisites for this Workflow	List of prerequisites that must be satisfied before you can run this workflow
How this Workflow Works	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
How to Run this Workflow	Instructions for running this workflow in your environment
Sample Scenario	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere 8 and Custom Node workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically root) who can access all required files and directories.
2. Per the IBM WebSphere 7 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server version 7 on 64-bit Red Hat Linux targets:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 ksh-20080202-14 gtk2-2.10.4-20 gtk2-engines-2.8.0-3 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 rpm-build-4.4.2-37.architecture.el5 (or later) elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48
64-bit Red Hat Enterprise Linux version 6	compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 ksh-20100621-2 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 rpm-build-4.8.0-12 elfutils-0.148-1 elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13

Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.

3. This workflow will install WebSphere Application Server as root because of the following IBM documented limitations:
 - Creation of a Linux service for WebSphere Application Server
 - Native registration with the operating system

- Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 8, refer to the [WebSphere 8 Product Documentation](#) on page 106.

How this Workflow Works

This topic contains the following information about the [Provision WebSphere 8 and Custom Node](#) workflow:

Overview

This workflow does the following three things in the order shown:

1. Installs the IBM Install Manager
2. Installs IBM WebSphere Application Server Network Deployment version 8
3. Creates a Custom Node profile

The workflow checks to see if the WebSphere 8 binary archive files exist on the target machine. If they do not, the files are downloaded from the software repository (for more information, see [How to Import a File into the Software Repository](#) on page 116).

See the following topics for detailed information:

[Validation Checks Performed](#)

[Steps in this Workflow](#)

[Process Flow](#)

Note: This workflow has been updated to account for the significant changes in the way that WebSphere 8 is installed.

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks for Red Hat Linux.

The workflow first performs the following parameter checks:

1. None of the following characters are used in the Admin User, Cell Name, Node Name, or Profile Name parameters: / \ * , : ; = + ? | < > & % ' " [] # \$ ^ { }
2. If Enable Security is true, Admin Password and Admin User are specified.
3. Admin Password (if specified) does not begin with a dash or contain a space.
4. Admin User (if specified) does not begin with a dash, a period, or a space.
5. Profile Name does not begin with a period.
6. Personal CertDN and Signing CertDN do not contain spaces.
7. If Ports File is specified, Validate Ports is true.
8. All specified file names are legal file names.

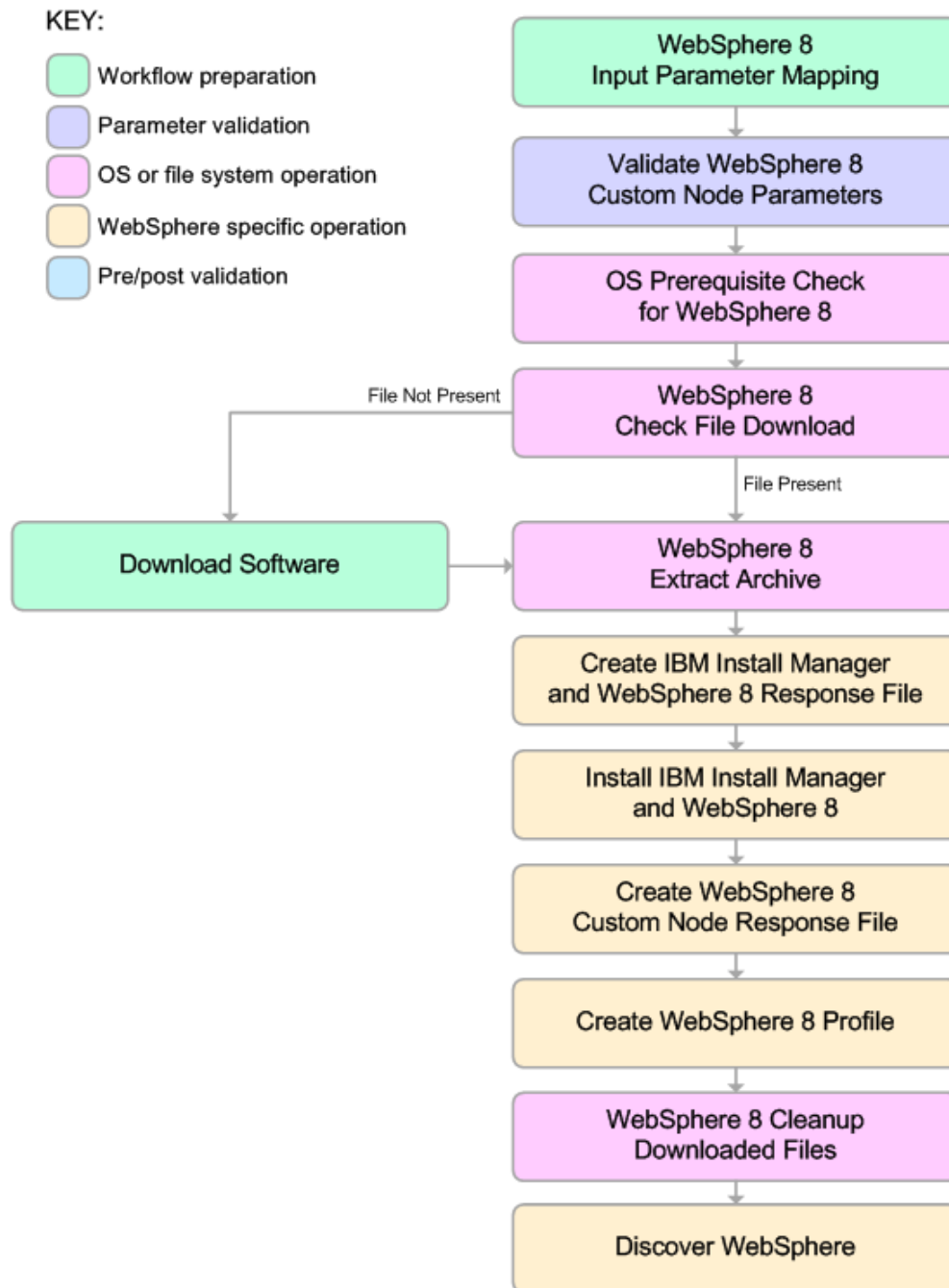
The workflow then performs the following operating system checks on the target machine:

1. All required libraries are present (see [Prerequisites for this Workflow](#) on page 58).
2. Sufficient disk space is available to install WebSphere 8.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

The Provision WebSphere 8 and Custom Node workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.

Click each box in the diagram to view additional information about that step.



Process Flow

This workflow performs the following tasks:

1. Creates the call wrapper and determines the target server platform type.
2. Validates the parameters needed to install WebSphere 8 and create a Custom Node profile (see [Validation Checks Performed](#) on page 61).
3. Checks the following:
 - a. Documented library requirements for WebSphere 8(see the [Prerequisites for this Workflow](#) on page 58).
 - b. File system space requirements where WebSphere 8 will be installed.
 - c. Temporary space requirements where the compressed software will be extracted before it is installed.
4. Determines whether the WebSphere 8 binary archive is present on the target machine. If the archive is not present, the workflow downloads it from the software repository (see [How to Import a File into the Software Repository](#) on page 116).
5. Extracts the WebSphere 8 binary archive to the specified directory.
6. Creates a response file for the purpose of installing a new instance of WebSphere 8.
7. Installs the IBM Installation Manager and a new WebSphere 8 instance on the target server.
8. Creates a new response file for the purpose of creating a Custom Node profile on top of the WebSphere 8 installation.
9. Creates a custom profile on top of the WebSphere 8 installation.
10. Cleans up any files that were downloaded.
11. *Optional:* Discovers any WebSphere 8 cells, clusters, and managed servers associated with the Profile Root that you specify. If these items are found, they are added to the HP DMA environment.

How to Run this Workflow

The following instructions show you how to customize and run the [Provision WebSphere 8 and Custom Node](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in [Parameters for Provision WebSphere 8 and Custom Node](#) on page 72.

Note: Before following this procedure, review the [Prerequisites for this Workflow](#) on page 58, and ensure that all requirements are satisfied.

To use the Provision WebSphere 8 and Custom Node workflow:

1. Create a deployable copy of the workflow (see [Create a Deployable Workflow](#) on page 17).
2. Determine the values that you will specify for the following parameters: show

Parameters Defined in this Step: Validate WebSphere 8 Custom Node Parameters

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash (-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	no default	optional	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().

Parameters Defined in this Step: Validate WebSphere 8 Custom Node Parameters (continued)

Parameter Name	Default Value	Required	Description
Dmgr Admin User	no default	optional	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Dmgr HostName	no default	optional	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later).
Dmgr Port	no default	optional	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later).
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Install Manager Binary Location	no default	required	Fully qualified path to the compressed Install Manager software package on the target machine.
Install Manager Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Install Manager Install Location	no default	required	Fully qualified path where Install Manager will be installed.
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.

Parameters Defined in this Step: Validate WebSphere 8 Custom Node Parameters (continued)

Parameter Name	Default Value	Required	Description
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Server Name	no default	required	Name of the application server that will be created under the profile.
WebSphere Binary Location	no default	required	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Parameters Defined in this Step: Discover WebSphere

Parameter Name	Default Value	Required	Description
Known Profile Roots	no default	optional	Comma delimited list of any known (or suspected) PROFILE_ROOTs. Use this to discover WebSphere cells which aren't currently running.
Trust SSL Certificates	False	optional	If "True", this step will trust any SSL used to connect to the DMA Web Service.

Parameters Defined in this Step: Discover WebSphere (continued)

Parameter Name	Default Value	Required	Description
Web Service Password	no default	required	Password for the discovery web service API.
Web Service URL	see description	required	URL for the discovery web service API. The default is: <code>https://host:8443/dma</code>
Web Service User	administrator	required	User capable of modifying the managed environment through the discovery web service API.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your provisioning objectives.

See [Parameters for Provision WebSphere 8 and Custom Node](#) on page 72 for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see [How to Use a Policy to Specify Parameter Values](#) on page 113).

3. In the workflow editor, expose any additional parameters that you need (see [How to Expose Additional Workflow Parameters](#) on page 112). You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment (see [Create a Deployment](#) on page 18 for instructions).
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment (see [Run Your Workflow](#) on page 19 for instructions).

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Be sure to also perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

```
WAS_ROOT/bin/versionInfo.sh
```

Here, *WAS_ROOT* is the directory where WebSphere 8 is installed. This is the path that you specified in the WebSphere Install Location parameter.

2. Validate that the profile has been created and is running by doing the following:

- a. View the *WAS_ROOT/profiles/PROFILE_NAME/logs/AboutThisProfile.txt* file. This file is created after the creation of the profile and contains specific information about the profile.

Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.

- b. Change to the *WAS_ROOT/profiles/PROFILE_NAME/logs/CELL_NAME* directory, and tail the *SystemOut.log* file. Look for the following line:

```
Server CELL_NAME open for e-business
```

Here, *CELL_NAME* is the name of the WebSphere 8 cell to which this profile pertains. This is the name that you specified in the Cell Name parameter.

Sample Scenario

This topic shows you typical parameter values used for the [Provision WebSphere 8 and Custom Node](#) workflow.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see [How to Use a Policy to Specify Parameter Values](#) on page 113).

New Install with Custom Node Profile – Parameter Value Examples

Parameter Name	Example Value	Description
Cell Name	Dev NodeCell	Unique cell name that does not contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	wasadmin	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Dmgr Admin User	wasadmin	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Dmgr HostName		Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later).
Dmgr Port		The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later).

New Install with Custom Node Profile – Parameter Value Examples (continued)

Parameter Name	Example Value	Description
Enable Security	true	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Federate Later	true	If false, the new custom node will be federated by the workflow during profile creation. If true, you must federate it later manually by using the addNode command.
Install Manager Binary Location	/opt/IBM/iim/IBM_Install_Manager_Linux.zip	Fully qualified path to the compressed Install Manager software package on the target machine.
Install Manager Extract Location	/opt/IBM/iim	Fully qualified path where the compressed software will be extracted on the target machine.
Install Manager Install Location	/opt/IBM/installManager	Fully qualified path where Install Manager will be installed.
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	DevNode	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	DevNode	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
WebSphere Binary Location	/opt/IBM/wasv8/WAS_V8.0_disk1.zip, /opt/IBM/wasv8/WAS_V8.0_disk2.zip,	Fully qualified path to the compressed WebSphere software package on the target machine.

New Install with Custom Node Profile – Parameter Value Examples (continued)

Parameter Name	Example Value	Description
WebSphere Extract Location	/opt/IBM/wasv8	Fully qualified path where the compressed software will be extracted on the target machine.
WebSphere Install Location	/opt/IBM/WebSphere8/AppServer	Fully qualified path where WebSphere will be installed.

Parameters for Provision WebSphere 8 and Custom Node

The following tables describe the required and optional input parameters for this workflow. Most of these parameters are not initially visible in a deployment (see [How to Expose Additional Workflow Parameters](#) on page 112). For most parameters, if you do not specify a value for a parameter, a default value is assigned

Input Parameters Defined in this Step: Validate WebSphere 8 Custom Node Parameters

Parameter Name	Default Value	Required	Description
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. Defaults are: UNIX targets: <code>/opt/hp/dma/client/jython.sh</code> running as root Windows targets: <code>jython</code> running as Administrator
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters <code>/ \ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> . If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	no default	optional	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Dmgr Admin User	no default	optional	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters <code>/ \ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> .
Dmgr HostName	no default	optional	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later).
Dmgr Port	no default	optional	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later).

Input Parameters Defined in this Step: Validate WebSphere 8 Custom Node Parameters (continued)

Parameter Name	Default Value	Required	Description
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Federate Later	no default	optional	If false, the new custom node will be federated by the workflow during profile creation. If true, you must federate it later manually by using the addNode command.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Install Manager Binary Location	no default	required	Fully qualified path to the compressed Install Manager software package on the target machine.
Install Manager Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Install Manager Install Location	no default	required	Fully qualified path where Install Manager will be installed.
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.

Input Parameters Defined in this Step: Validate WebSphere 8 Custom Node Parameters (continued)

Parameter Name	Default Value	Required	Description
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmalab-example.com,OU=WAS7LabCell,OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_adminhost=9060). This option should be used with the Validate Ports option.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters <code>/ \ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> .
Profile Path	no default	required	Fully qualified path to the profile. For example: <code>/opt/IBM/WebSphere/AppServer/profiles/AppServer1</code>
Profile Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation.
Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: CN=dmalab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.

Input Parameters Defined in this Step: Validate WebSphere 8 Custom Node Parameters (continued)

Parameter Name	Default Value	Required	Description
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.
WebSphere Binary Location	no default	required	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Parameters Defined in this Step: Discover WebSphere

Parameter Name	Default Value	Required	Description
Known Profile Roots	no default	optional	Comma delimited list of any known (or suspected) PROFILE_ROOTs. Use this to discover WebSphere cells which aren't currently running.
Trust SSL Certificates	False	optional	If "True", this step will trust any SSL used to connect to the DMA Web Service.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service URL	see description	required	URL for the discovery web service API. The default is: <code>https://host:8443/dma</code>
Web Service User	administrator	required	User capable of modifying the managed environment through the discovery web service API.

Provision Websphere 8 Standalone Profile From Existing Install

Use this workflow to create a stand-alone profile on an existing WebSphere 8 installation.

A stand-alone application server works independently—it is not part of a cell and does not interact with a deployment manager. The stand-alone profile is not suitable for distributed application server environments.

To use this workflow in your environment, see the following information:

Topic	Information Included
Prerequisites for this Workflow	List of prerequisites that must be satisfied before you can run this workflow
How this Workflow Works	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
How to Run this Workflow	Instructions for running this workflow in your environment
Sample Scenario	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the [Provision Websphere 8 Standalone Profile From Existing Install](#) workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically root) who can access all required files and directories.
2. Per the IBM WebSphere 7 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server version 7 on 64-bit Red Hat Linux targets:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 ksh-20080202-14 gtk2-2.10.4-20 gtk2-engines-2.8.0-3 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 rpm-build-4.4.2-37.architecture.el5 (or later) elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48
64-bit Red Hat Enterprise Linux version 6	compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 ksh-20100621-2 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 rpm-build-4.8.0-12 elfutils-0.148-1 elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13

Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.

3. This workflow will install WebSphere Application Server as root because of the following IBM documented limitations:
 - Creation of a Linux service for WebSphere Application Server
 - Native registration with the operating system

- Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 8, refer to the [WebSphere 8 Product Documentation](#) on page 106.

How this Workflow Works

This topic contains the following information about the [Provision Websphere 8 Standalone Profile From Existing Install](#) on page 76 workflow:

Overview

This workflow creates a stand-alone profile on an existing WebSphere 8 installation.

See the following topics for detailed information:

[Validation Checks Performed](#)

[Steps in this Workflow](#)

[Process Flow](#)

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks for Red Hat Linux.

The workflow first performs the following parameter checks:

1. None of the following characters are used in the Admin User, Cell Name, Node Name, or Profile Name parameters: / \ * , : ; = + ? | < > & % ' " [] # \$ ^ { }
2. If Enable Security is true, Admin Password and Admin User are specified.
3. Admin Password (if specified) does not begin with a dash or contain a space.
4. Admin User (if specified) does not begin with a dash, a period, or a space.
5. Profile Name does not begin with a period.
6. Personal CertDN and Signing CertDN do not contain spaces.
7. If Ports File is specified, Validate Ports is true.
8. All specified file names are legal file names.




The workflow then checks to make sure that all required libraries are present on the target machine (see [Prerequisites for this Workflow](#) on page 77).

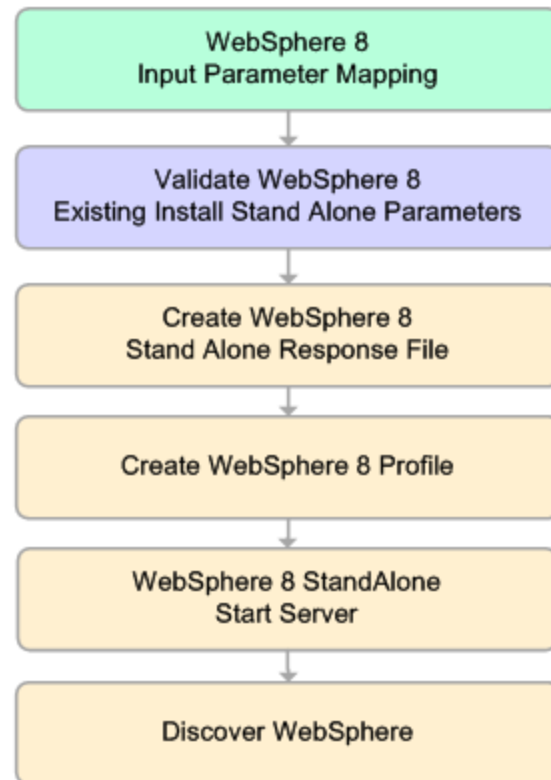
Steps Executed

The Provision WebSphere 8 Standalone Profile From Existing Install workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.

Click each box in the diagram to view additional information about that step.

KEY:

-  Workflow preparation
-  Parameter validation
-  WebSphere specific operation



Process Flow

This workflow performs the following tasks:

1. Creates the call wrapper and determines the target server platform type.
2. Validates the parameters needed to create a stand-alone profile (see [Validation Checks Performed](#) on previous page).
3. Creates a new response file for the purpose of creating a stand-alone profile on top of the existing WebSphere 8 installation.
4. Creates a stand-alone profile on top of the WebSphere 8 installation.
5. Starts the stand-alone application server.
6. *Optional:* Discovers any WebSphere 8 cells, clusters, and managed servers associated with the Profile Root that you specify. If these items are found, they are added to the HP DMA environment.

How to Run this Workflow

The following instructions show you how to customize and run the [Provision Websphere 8 Standalone Profile From Existing Install](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in [Parameters for Provision WebSphere 8 Standalone Profile from Existing Install](#) on page 87.

Note: Before following this procedure, review the [Prerequisites for this Workflow](#), and ensure that all requirements are satisfied.

To customize and run the Provision Websphere 8 Custom Node Profile From Existing Install workflow:

1. Create a deployable copy of the workflow (see [Create a Deployable Workflow](#) on page 17).
2. Determine the values that you will specify for the following parameters:

Parameters Defined in this Step: Validate WebSphere 8 Existing Install Stand Alone Parameters

Parameter Name	Default Value	Required	Description
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	no default	optional	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Dmgr Admin User	no default	optional	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.

Parameters Defined in this Step: Validate WebSphere 8 Existing Install Stand Alone Parameters (continued)

Parameter Name	Default Value	Required	Description
Dmgr HostName	no default	optional	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later).
Dmgr Port	no default	optional	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later).
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Parameters Defined in this Step: Discover WebSphere

Parameter Name	Default Value	Required	Description
Known Profile Roots	no default	optional	Comma delimited list of any known (or suspected) PROFILE_ROOTs. Use this to discover WebSphere cells which aren't currently running.
Trust SSL Certificates	False	optional	If "True", this step will trust any SSL used to connect to the DMA Web Service.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service URL	see description	required	URL for the discovery web service API. The default is: <code>https://host:8443/dma</code>
Web Service User	administrator	required	User capable of modifying the managed environment through the discovery web service API.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your provisioning objectives.

See [Parameters for Provision Websphere 8 Custom Node Profile From Existing Install](#) on page 102 for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see [How to Use a Policy to Specify Parameter Values](#) on page 113).

3. In the workflow editor, expose any additional parameters that you need (see [How to Expose Additional Workflow Parameters](#) on page 112). You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment (see [Create a Deployment](#) on page 18 for instructions).
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment (see [Run Your Workflow](#) on page 19 for instructions).

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Be sure to also perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

```
WAS_ROOT/bin/versionInfo.sh
```

Here, *WAS_ROOT* is the directory where WebSphere 8 is installed. This is the path that you specified in the WebSphere Install Location parameter.

2. Validate that the profile has been created and is running by doing the following:

- a. View the *WAS_ROOT/profiles/PROFILE_NAME/logs/AboutThisProfile.txt* file. This file is created after the creation of the profile and contains specific information about the profile.

Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.

- b. Change to the *WAS_ROOT/profiles/PROFILE_NAME/logs/CELL_NAME* directory, and tail the *SystemOut.log* file. Look for the following line:

```
Server CELL_NAME open for e-business
```

Here, *CELL_NAME* is the name of the WebSphere 8 cell to which this profile pertains. This is the name that you specified in the Cell Name parameter.

Sample Scenario

This topic shows you typical parameter values used for the [Provision Websphere 8 Standalone Profile From Existing Install](#) workflow.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see [How to Use a Policy to Specify Parameter Values](#) on page 113).

Standalone Profile on Existing Install – Parameter Value Examples

Parameter Name	Example Value	Description
Admin Password	password	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Admin User	wasadmin	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }.
Cell Name	DevStandAlone1Cell	Unique cell name that does not contain any of the following special characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	true	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	DevStandAlone1Node	Unique node name that cannot contain any of the following special characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.

Standalone Profile on Existing Install – Parameter Value Examples (continued)

Parameter Name	Example Value	Description
Profile Name	StandAlone1	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Server Name	server1	Name of the application server that will be created under the profile.
WebSphere Install Location	/opt/IBM/WebSphere8/AppServer	Fully qualified path where WebSphere will be installed.

Parameters for Provision WebSphere 8 Standalone Profile from Existing Install

The following tables describe the required and optional input parameters for this workflow. Most of these parameters are not initially visible in a deployment (see [How to Expose Additional Workflow Parameters](#) on page 112). For most parameters, if you do not specify a value for a parameter, a default value is assigned

Parameters Defined in this Step: Validate WebSphere 8 Existing Install Stand Alone Parameters

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash (-) or contain a space().
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash (-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. Defaults are: UNIX targets: <code>/opt/hp/dma/client/jython.sh</code> running as root Windows targets: <code>jython</code> running as Administrator
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Default Ports	false	optional	Provides the option to assign default ports to a profile. Valid values are true or false. If true, the WebSphere Application Server default ports will be used, and the Ports File and Starting Port parameters should not have values. If false, the workflow will increment the default port until it finds a free port. The default value is false.
Developer Server	no default	optional	Use this parameter for development environments only to help with start up time. Valid value is true. Do not use in production environments.

Parameters Defined in this Step: Validate WebSphere 8 Existing Install Stand Alone Parameters (continued)

Parameter Name	Default Value	Required	Description
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Omit Action	no default	optional	Enables you to prevent certain optional features from being installed. Valid values are deployAdminConsole or defaultAppDeployAndConfig. You may only specify one of these options.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmalab-example.com,OU=WAS7LabCell,OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.

Parameters Defined in this Step: Validate WebSphere 8 Existing Install Stand Alone Parameters (continued)

Parameter Name	Default Value	Required	Description
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_adminhost=9060). This option should be used with the Validate Ports option.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? < > & % ' " [] # \$ ^ { }.
Profile Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation.
Server Name	no default	required	Name of the application server that will be created under the profile.
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: CN=dmalab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.
Starting Port	no default	optional	Starting port number that the profile will use to generate and assign port values. Port values are assigned sequentially from the Starting Port. Do not specify this parameter if you specify Default Ports or Ports File.
Validate Ports	false	optional	Indicates that the ports should be validated to ensure that they are not already in use. Valid values are true or false. You should use this option if you specify a Ports File.

Parameters Defined in this Step: Validate WebSphere 8 Existing Install Stand Alone Parameters (continued)

Parameter Name	Default Value	Required	Description
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Provision WebSphere 8 Custom Node Profile From Existing Install

Use this workflow to create a custom profile on an existing WebSphere 8 installation.

A custom profile initially contains an empty node with no servers. The workflow can add (federate) the server to the pertinent cell when the profile is created, or you can add it later yourself.

To use this workflow in your environment, see the following information:

Topic	Information Included
Prerequisites for this Workflow	List of prerequisites that must be satisfied before you can run this workflow
How this Workflow Works	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
How to Run this Workflow	Instructions for running this workflow in your environment
Sample Scenario	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere 8 Custom Node Profile From Existing Install workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically root) who can access all required files and directories.
2. Per the IBM WebSphere 7 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server version 7 on 64-bit Red Hat Linux targets:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 ksh-20080202-14 gtk2-2.10.4-20 gtk2-engines-2.8.0-3 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 rpm-build-4.4.2-37.architecture.el5 (or later) elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48
64-bit Red Hat Enterprise Linux version 6	compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 ksh-20100621-2 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 rpm-build-4.8.0-12 elfutils-0.148-1 elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13

Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.

3. This workflow will install WebSphere Application Server as root because of the following IBM documented limitations:
 - Creation of a Linux service for WebSphere Application Server
 - Native registration with the operating system

- Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 8, refer to the [WebSphere 8 Product Documentation](#) on page 106.

How this Workflow Works

This topic contains the following information about the [Provision Websphere 8 Custom Node Profile From Existing Install](#) workflow:

Overview

This workflow creates a Custom Node profile on an existing WebSphere 8 installation.

See the following topics for detailed information:

[Validation Checks Performed](#)

[Steps in this Workflow](#)

[Process Flow](#)

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks for Red Hat Linux.

The workflow first performs the following parameter checks:

1. None of the following characters are used in the Admin User, Cell Name, Node Name, or Profile Name parameters: / \ * , : ; = + ? | < > & % ' " [] # \$ ^ { }
2. If Enable Security is true, Admin Password and Admin User are specified.
3. Admin Password (if specified) does not begin with a dash or contain a space.
4. Admin User (if specified) does not begin with a dash, a period, or a space.
5. Profile Name does not begin with a period.
6. Personal CertDN and Signing CertDN do not contain spaces.
7. If Ports File is specified, Validate Ports is true.
8. All specified file names are legal file names.




The workflow then checks to make sure that all required libraries are present on the target machine (see [Prerequisites for this Workflow](#) on page 92).

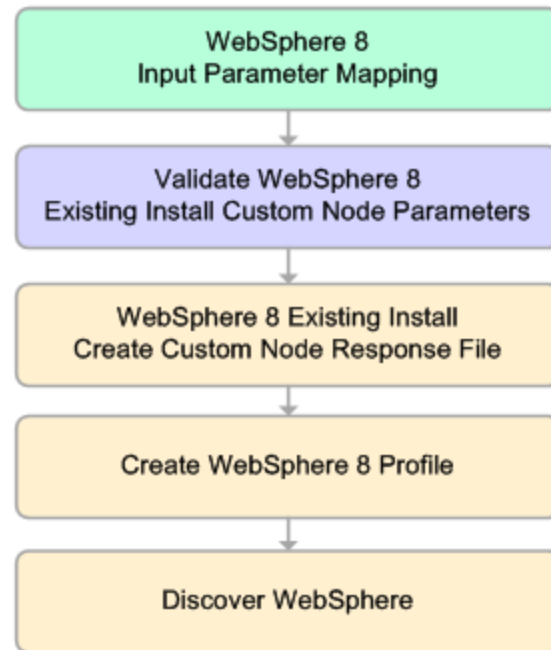
Steps Executed

The Provision WebSphere 8 Custom Node Profile From Existing Install workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.

Click each box in the diagram to view additional information about that step.

KEY:

-  Workflow preparation
-  Parameter validation
-  WebSphere specific operation



Process Flow

This workflow performs the following tasks:

1. Creates the call wrapper and determines the target server platform type.
2. Validates the parameters needed to create a Custom Node profile (see [Validation Checks Performed](#) on previous page).
3. Creates a new response file for the purpose of creating a Custom Node profile on top of the existing WebSphere 8 installation.
4. Creates a Custom Node profile on top of the WebSphere 8 installation.
5. Cleans up any files that were downloaded.
6. *Optional:* Discovers any WebSphere 8 cells, clusters, and managed servers associated with the Profile Root that you specify. If these items are found, they are added to the HP DMA environment.

How to Run this Workflow

The following instructions show you how to customize and run the [Provision Websphere 8 Custom Node Profile From Existing Install](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in [Parameters for Provision Websphere 8 Custom Node Profile From Existing Install](#) on page 102.

Note: Before following this procedure, review the [Prerequisites for this Workflow](#), and ensure that all requirements are satisfied.

To use the Provision Websphere 8 Custom Node Profile From Existing Install workflow:

1. Create a deployable copy of the workflow (see [Create a Deployable Workflow](#) on page 17).
2. Determine the values that you will specify for the following parameters: show

Parameters Defined in This Step: Validate WebSphere 8 Existing Install Custom Node Parameters

Parameter Name	Default Value	Required	Description
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	no default	optional	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Dmgr Admin User	no default	optional	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Dmgr HostName	no default	optional	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later).

Parameters Defined in This Step: Validate WebSphere 8 Existing Install Custom Node Parameters (continued)

Parameter Name	Default Value	Required	Description
Dmgr Port	no default	optional	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later).
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Parameters Defined in this Step: Discover WebSphere

Parameter Name	Default Value	Required	Description
Known Profile Roots	no default	optional	Comma delimited list of any known (or suspected) PROFILE_ROOTs. Use this to discover WebSphere cells which aren't currently running.
Trust SSL Certificates	False	optional	If "True", this step will trust any SSL used to connect to the DMA Web Service.

Parameters Defined in this Step: Discover WebSphere (continued)

Parameter Name	Default Value	Required	Description
Web Service Password	no default	required	Password for the discovery web service API.
Web Service URL	see description	required	URL for the discovery web service API. The default is: <code>https://host:8443/dma</code>
Web Service User	administrator	required	User capable of modifying the managed environment through the discovery web service API.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your provisioning objectives.

See [Parameters for Provision Websphere 8 Custom Node Profile From Existing Install](#) on page 102 for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see [How to Use a Policy to Specify Parameter Values](#) on page 113).

3. In the workflow editor, expose any additional parameters that you need (see [How to Expose Additional Workflow Parameters](#) on page 112). You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment (see [Create a Deployment](#) on page 18 for instructions).
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment (see [Run Your Workflow](#) on page 19 for instructions).

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Be sure to also perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

```
WAS_ROOT/bin/versionInfo.sh
```

Here, *WAS_ROOT* is the directory where WebSphere 8 is installed. This is the path that you specified in the WebSphere Install Location parameter.

2. Validate that the profile has been created and is running by doing the following:

- a. View the *WAS_ROOT/profiles/PROFILE_NAME/logs/AboutThisProfile.txt* file. This file is created after the creation of the profile and contains specific information about the profile.

Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.

- b. Change to the *WAS_ROOT/profiles/PROFILE_NAME/logs/CELL_NAME* directory, and tail the *SystemOut.log* file. Look for the following line:

```
Server CELL_NAME open for e-business
```

Here, *CELL_NAME* is the name of the WebSphere 8 cell to which this profile pertains. This is the name that you specified in the Cell Name parameter.

Sample Scenario

This topic shows you typical parameter values used for the [Provision Websphere 8 Custom Node Profile From Existing Install](#) workflow.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see [How to Use a Policy to Specify Parameter Values](#) on page 113).

Custom Node Profiles on Existing Install – Parameter Value Examples

Parameter Name	Example Value	Description
Cell Name	Dev NodeCell	Unique cell name that does not contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	password	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Dmgr Admin User	wasadmin	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Dmgr HostName	testserver.mycompany.com	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later).
Dmgr Port	8879	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later).

Custom Node Profiles on Existing Install – Parameter Value Examples (continued)

Parameter Name	Example Value	Description
Enable Security	true	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Node Name	DevNode1	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	DevNode1	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
WebSphere Install Location	/opt/IBM/WebSphere8/AppServer	Fully qualified path where WebSphere will be installed.

Parameters for Provision WebSphere 8 Custom Node Profile From Existing Install

The following tables describe the required and optional input parameters for this workflow. Most of these parameters are not initially visible in a deployment (see [How to Expose Additional Workflow Parameters](#) on page 112). For most parameters, if you do not specify a value for a parameter, a default value is assigned

Input Parameters Defined in this Step: Validate WebSphere 8 Existing Install Custom Node Parameters

Parameter Name	Default Value	Required	Description
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. Defaults are: UNIX targets: <code>/opt/hp/dma/client/jython.sh</code> running as root Windows targets: <code>jython</code> running as Administrator
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters <code>/ \ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> . If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	no default	optional	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Dmgr Admin User	no default	optional	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters <code>/ \ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> .
Dmgr HostName	no default	optional	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later).

Input Parameters Defined in this Step: Validate WebSphere 8 Existing Install Custom Node Parameters (continued)

Parameter Name	Default Value	Required	Description
Dmgr Port	no default	optional	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later).
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Install Manager Install Location	no default	required	Fully qualified path where Install Manager will be installed.
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmalab-example.com,OU=WAS7LabCell,OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.

Input Parameters Defined in this Step: Validate WebSphere 8 Existing Install Custom Node Parameters (continued)

Parameter Name	Default Value	Required	Description
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_adminhost=9060). This option should be used with the Validate Ports option.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Profile Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation.
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: CN=dmalab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Parameters Defined in this Step: Discover WebSphere

Parameter Name	Default Value	Required	Description
Known Profile Roots	no default	optional	Comma delimited list of any known (or suspected) PROFILE_ROOTs. Use this to discover WebSphere cells which aren't currently running.
Trust SSL Certificates	False	optional	If "True", this step will trust any SSL used to connect to the DMA Web Service.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service URL	see description	required	URL for the discovery web service API. The default is: <code>https://host:8443/dma</code>
Web Service User	administrator	required	User capable of modifying the managed environment through the discovery web service API.

Chapter 3

Reference Information

This chapter contains the following information:

Topic	Description
WebSphere 8 Product Documentation	Links to product documentation for the database products that these workflows support Links to the hardware and software requirements, as well as supported platforms for WebSphere 8,
HP DMA Documentation	Links to additional HP DMA documentation

WebSphere 8 Product Documentation

For the current list of hardware and software requirements, as well as supported platforms for WebSphere 8, see:

<http://www.ibm.com/software/webervers/appserv/doc/latest/prereq.html>

For WebSphere 8 product documentation, see:

<http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp>

For IBM Red Book resources for WebSphere 8, see:

<http://publib-b.boulder.ibm.com/Redbooks.nsf/portals/WebSphere>

HP DMA Documentation

For information about using the HP DMA web interface, see the *HP DMA User Guide* and the *HP DMA Administrator Guide* (version 10.00 or later).

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>

Chapter 4

Tips and Best Practices

This portion of the document contains a collection of tips and best practices that will enable you to use HP DMA more effectively. It contains the following topics:

[How this Solution is Organized](#) on next page

[How to Expose Additional Workflow Parameters](#) on page 112

[How to Use a Policy to Specify Parameter Values](#) on page 113

[How to Import a File into the Software Repository](#) on page 116

How this Solution is Organized

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 solution pack contains one or more related workflow templates.

Each workflow template has a Documentation tab that provides detailed information about that workflow.

The screenshot displays the HP Database & Middleware Automation console. The top navigation bar includes 'Home', 'Automation', 'Reports', 'Environment', 'Solutions', and 'Setup'. Below this, a secondary bar shows 'Workflows', 'Steps', 'Functions', 'Policies', 'Deployments', 'Run', 'Console', and 'History'. The main content area is titled 'Provision WebSphere 8 and StandAlone' and features tabs for 'Documentation', 'Workflow', 'Deployments', and 'Roles'. The 'Documentation' tab is active, showing the following details:

- Name:** Provision WebSphere 8 and StandAlone
- Tags:**
- Type:** OS
- Target level:** Server

The 'Documentation' section contains three main sections:

- Purpose:** This workflow installs a new instance of IBM WebSphere Application Server V8.0 and creates a Standalone Agent profile.
- Platforms:** This workflow installs the IBM WebSphere Application Server V8.0 ND core product binaries on the following operating system platforms:
 - Red Hat Enterprise Linux
 - AIX
 - Solaris
 - Windows Server
- Parameters:** The following characters cannot be used in the Admin User, Cell Name, Node Name, or Profile Name parameters: / \ * , ; : = + ? [< > & % ' " [] > # \$ ^ { }

At the bottom of the console, there is a footer bar with 'Copy', 'EXPORT', and 'EXTRACT POLICY' buttons, and a link to the 'HP DMA APPLICATION SERVER PROVISIONING SOLUTION PACK'.

A workflow consists of a sequence of steps. Each step performs a very specific task. Each step includes a documentation panel that briefly describes its function. Steps can be shared among workflows.

The screenshot shows the 'Create WebSphere 8 Profile' step in the 'Database & Middleware Automation' console. The interface includes a top navigation bar with tabs like Home, Automation, Reports, Environment, Solutions, and Setup. Below this is a sub-navigation bar with tabs like Workflows, Steps, Functions, Policies, Deployments, Run, Console, and History. The main content area is titled 'Create WebSphere 8 Profile' and has several sub-tabs: General, Action, Parameters, History, Workflows, Solutions, and Roles. The 'General' tab is selected, showing the 'Properties' and 'Documentation' sections. The 'Properties' section lists: Name: Create WebSphere 8 Profile, Tags: standalone, responsefile, WebSphere, Type: OS, and Category: Script. The 'Documentation' section contains a description: 'Create a profile on top of an existing WebSphere Application Server V8.0 installation.', Dependencies: None, and Return Code: 0 = Step ran successfully, 1 = Step failed. At the bottom, there is a 'Copy' button and a status indicator 'THIS STEP IS READ ONLY'.

Steps can have input and output parameters. Output parameters from one step often serve as input parameters to another step.

Parameter descriptions are displayed on the Workflow tab for each workflow.

The screenshot shows the 'Validate WebSphere 8 Stand Alone Parameters / Admin Password' step in the 'Database & Middleware Automation' console. The interface includes a top navigation bar with tabs like Home, Automation, Reports, Environment, Solutions, and Setup. Below this is a sub-navigation bar with tabs like Workflows, Steps, Functions, Policies, Deployments, Run, Console, and History. The main content area is titled 'Validate WebSphere 8 Stand Alone Parameters / Admin Password' and has several sub-tabs: General, Action, Parameters, History, Workflows, Solutions, and Roles. The 'General' tab is selected, showing the 'Properties' and 'Documentation' sections. The 'Properties' section lists: Name: Validate WebSphere 8 Stand Alone Parameters / Admin Password, Tags: standalone, responsefile, WebSphere, Type: OS, and Category: Script. The 'Documentation' section contains a description: 'Optional: When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().', Dependencies: None, and Return Code: 0 = Step ran successfully, 1 = Step failed. At the bottom, there is a 'Copy' button and a status indicator 'THIS STEP IS READ ONLY'. A red arrow points to the 'Optional: When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().' text, with the label 'To see parameter description here'.

Parameter descriptions are displayed on the Parameters tab for each step in the workflow.

Database & Middleware Automation
Home Automation Reports Environment Solutions Setup
Workflows Steps Functions Policies Deployments Run Console History

Validate WebSphere 8 Stand Alone Parameters
General Action Parameters History Workflows Solutions Roles

Input parameters

Name	Value	Description
Admin Password		Optional: When Enable Security is set to true, this p
Admin User		Optional: When Enable Security is set to true, this p
Call Wrapper		Required: Command that will execute the step as a
Cell Name		Required: Unique cell name that does not contain ar
Default Ports		Optional: Provides the option to assign default ports
Developer Server		Optional: Use this parameter for development enviro
Enable Security		Required: Enables administrative security. Must be :
Host Name		Required: Hostname or IP address of the target mac
Install Manager Binary Location		Required: Fully qualified path to the compressed Ins
Install Manager Extract Location		Required: Fully qualified path where the compressed
Install Manager Install Location		Required: Fully qualified path where Install Manager
Keystore Password		Optional: Sets the password for all keystore files cre
License Acceptance		Required: Acknowledges that the end user agrees to
Node Name		Required: Unique node name that cannot contain an
Omit Action		Optional: Enables you to prevent certain optional fea
Personal CertDN		Optional: Distinguished name of the personal certifi
Personal CertValidity Period		Optional: Amount of time in years that the personal
Ports File		Optional: Fully qualified path to a file that defines po

Parameter descriptions are also displayed on the Parameters tab in the deployment (organized by step).

The screenshot shows the HP Database & Middleware Automation console interface. At the top is a navigation bar with tabs: Home, Automation, Reports, Environment, Solutions, Setup, Workflows, Steps, Functions, Policies, Deployments, Run, Console, and History. Below this is a section titled 'Example Deployment' with three sub-tabs: Targets, Parameters, and Roles. The 'Parameters' tab is active, displaying a list of parameters for 'Validate WebSphere 8 Stand Alone Parameters'. Each parameter has a text input field, a dropdown menu set to 'Text', and a detailed description of its requirements and constraints.

Parameter Name	Requirement/Description
Admin Password:	Optional: When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Admin User:	Optional: When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period (.), or a space(). It cannot contain any of the following characters: / \ * , ; : = + ? [< > & % ' " [] > # \$ ^ { }.
Cell Name:	Required: Unique cell name that does not contain any of the following special characters: / \ * , ; : = + ? [< > & % ' " [] > # \$ ^ { } . If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security:	Required: Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Install Manager Binary Location:	Required: Fully qualified path to the compressed Install Manager software package on the target machine.
Install Manager Extract Location:	Required: Fully qualified path where the compressed software will be extracted on the target machine.

All parameters used by the workflows in this solution pack are described in the "Parameters" topic associated with each workflow.

Note: The workflow templates included in this solution pack are read-only and cannot be deployed. To use a workflow template, you must first create a copy of the template and then customize that copy for your environment (see [Create a Deployable Workflow](#) on page 17).

How to Expose Additional Workflow Parameters

Each workflow in this solution pack has a set of input parameters. Some are required and some are optional. To run a workflow in your environment, you must specify values for a subset of these parameters when you create a deployment.

By default, only a few of the input parameters for each workflow are visible on the Deployment page, and the rest are hidden. In order to specify a value for a parameter that is currently hidden, you must first expose that parameter by changing its mapping in the workflow editor.

To expose a hidden workflow parameter:

1. In the HP DMA web interface, go to Automation > Workflows.
2. From the list of workflows, select a deployable workflow.
3. Go to the Workflow tab.
4. In the list of steps below the workflow diagram, click the ► (blue arrow) to the immediate left of the pertinent step name. This expands the list of input parameters for this step.
5. For the parameter that you want to expose, select - User Selected - from the drop-down list.
For example:

Step	Name	Required Result	Next
▼ 1	Gather Parameters for Oracle Compliance		2
	Compliance Type:	- User selected -	ⓘ
	Excluded Compliance Checks:	- User selected -	ⓘ
	Inventory Files:	- User selected -	ⓘ

6. Repeat steps 4 and 5 for all the parameters that you would like to specify in the deployment.
7. Click **Save** in the lower right corner.

How to Use a Policy to Specify Parameter Values

It is sometimes advantageous to provide parameter values by using a policy rather than explicitly specifying the values in a deployment. This approach has the following advantages:

- The policy can be used in any deployment.
- It is faster and less error-prone than specifying parameter values manually.
- For parameter values that change frequently—for example, passwords that must be changed regularly—you only need to update them in one place.

To establish a policy, you can either [Create a Policy](#) or [Extract a Policy](#) from a workflow.

After you establish the policy, you must [Reference the Policy in the Deployment](#).

For more information, see the *HP DMA User Guide*. This document is available on the HP Software Product Manuals web site: <http://h20230.www2.hp.com/selfsolve/manuals>

Create a Policy

The first step in this approach is to create a policy that provides parameter values. There are two ways to do this: (1) create a new policy, and define all attributes manually (as shown here) or (2) extract a policy from a workflow (see [Extract a Policy](#) on next page).

To create a policy that provides parameter values:

1. In the HP DMA web UI, go to Automation > Policies.
2. Click **New Policy**.
3. In the **Name** box, specify the name of the policy
4. For each parameter value that you want to provide using this policy, perform the following actions on the Attributes tab:
 - a. From the drop-down list, select the type of attribute:
 - A Text attribute contains simple text that users can view while deploying and running workflows.
 - A List attribute contains a comma-separated list of values (or a large amount of text not suitable for a Text attribute).
 - A Password attribute contains simple text, but the characters are masked so that users cannot see the text.
 - b. In the text box to the left of the Add button, specify the name of the attribute.

For your convenience, this name should be similar to the parameter name used in the pertinent workflow (or workflows).
 - c. Click **Add**.
 - d. In the new text box to the right of the attribute's name, enter a value for this attribute.

To remove an attribute, click the **Remove** button.
5. On the Roles tab, grant Read and Write permission to any additional users and groups who will

be using this policy. By default, any groups to which you belong have Read and Write permission.

6. Click the **Save** button (lower right corner).

Extract a Policy

An alternative to creating your own policy one attribute at a time is to extract the policy. This automatically creates a reusable policy that provides values for all input parameters associated with a workflow. This is a convenient way to create a policy.

To extract a policy:

1. Go to Automation > Workflows.
2. Select the Workflow that you want to work with.
3. Click the Extract Policy link at the bottom of the screen.
4. Specify values for each attribute listed.
5. *Optional:* Remove any attributes that you do not want to use.
6. *Optional:* Add any new attributes that you want to use.
7. *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).
8. Click **Save**.

Reference the Policy in the Deployment

After you create a policy, you can reference its attributes in a deployment.

To reference policy attributes in a deployment:

1. Create or access the deployment.
See “Deployments” in the *HP DMA User Guide* for details.
2. On the Parameters tab, perform the following steps for each parameter whose value you want to provide by referencing a policy attribute:
 - a. In the drop-down menu for that parameter, select **Policy Attribute**.
 - b. In the text box for that parameter, type any character. A drop-down list of policy attributes appears. For example:

Admin Pwd: Policy Attribute ▼

MS SQL: Provisioning.Virtual Server Name
MyParameterValues.MyAdminPassword
MyParameterValues.MyAdminUser
MyParameterValues.MyDBUser
MyParameterValues.MyDBUserPassword
Oracle Compliance.Oracle Mandatory Checks
Oracle Compliance.Oracle Recommended Checks
Oracle Provisioning.Additional Groups
Oracle Provisioning.Backup Directory
Oracle Provisioning.Base
Oracle Provisioning.Binaries Host
Oracle Provisioning.Bit Mode

- c. From the drop-down list, select the attribute that you want to reference. For example:

Admin Pwd: Policy Attribute ▼

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

How to Import a File into the Software Repository

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

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

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

To import a file into the HP SA Software Library:

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

By default, the HP SA Client is located in Start → All Programs → HP Software → HP Server Automation Client

If the HP SA Client is not installed locally, follow the instructions under “Download and Install the HP SA Client Launcher” in the *HP Server Automation Single-Host Installation Guide*.
2. In the navigation pane in the HP SA Client, select Library → By Folder.
3. Select (or create) the folder where you want to store the file.
4. From the Actions menu, select **Import Software**.
5. In the Import Software dialog, click the **Browse** button to the right of the File(s) box.
6. In the Open dialog:
 - a. Select the file (or files) to import.
 - b. Specify the character encoding to be used from the Encoding drop-down list. The default encoding is English ASCII.
 - c. Click **Open**. The Import Software dialog reappears.
7. From the Type drop-down list, select **Unknown**.
8. If the folder where you want to store the files does not appear in the Folder box, follow these steps:
 - a. Click the **Browse** button to the right of the Folder box.
 - b. In the Select Folder window, select the import destination location, and click **Select**. The Import Software dialog reappears.
9. From the Platform drop-down list, select all the operating systems listed.
10. Click **Import**.

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

Chapter 5

Troubleshooting

These topics can help you address problems that might occur when you install and run the workflows in this solution pack:

- [Target Type](#) below
- [User Permissions and Related Requirements](#) below
- [Discovery in HP DMA](#) on next page

Target Type

In your deployment, make sure that you have specified the correct type of target. The workflow type and the target type must match. A workflow designed to run against an instance target, for example, cannot run against a server target.

User Permissions and Related Requirements

Roles define access permissions for organizations, workflows, steps, policies, and deployments. Users are assigned to roles, and they gain access to these automation items according to the permissions and capabilities defined for their roles.

Roles are assigned by your server management tool administrator. They are then registered in HP DMA by your HP DMA administrator.

Your HP DMA administrator will ensure that the users in your environment are assigned roles that grant them the permissions and capabilities they need to accomplish their tasks. For example:

- To create a workflow, your role must have Workflow Creator capability.
- To view a workflow, your role must have Read permission for that workflow.
- To edit a workflow, your role must have Write permission for that workflow.
- To view a deployment, your role must have Read permission for that deployment.
- To modify a deployment, your role must have Write permission for that deployment.
- To run a deployment, your role must have Execute permission for that deployment and Deploy permission for the organization where it will run.

Capabilities determine what features and functions are available and active in the HP DMA UI for each user role.

For more information, see the *HP DMA Administrator Guide*. This document is available on the HP Software Product Manuals web site: <http://h20230.www2.hp.com/selfsolve/manuals>

Discovery in HP DMA

HP DMA uses a process called “discovery” to find information about the servers, networks, and database instances on target machines in your managed environment.

You must explicitly initiate the process of discovery—it is not automatic. See the *HP DMA User Guide* for instructions. This document is available on the HP Software Product Manuals web site: <http://h20230.www2.hp.com/selfsolve/manuals>

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.

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.

destination

In a database refresh scenario, the contents of a database dump file are loaded into the DESTINATION database.

DESTINATION

In a database refresh scenario, the contents of a database dump file are loaded into the DESTINATION database.

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

Oracle Data Pump

Oracle Data Pump is a utility that enables you to move data or metadata from one database to another. You can use Data Pump to move a complete database or a subset of a database.

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.

Recovery Manager (RMAN)

Oracle Recovery Manager (RMAN) is a backup and recovery tool included in Oracle Database Enterprise Edition (and related products). RMAN enables you to efficiently backup and restore data files, control files, server parameter files, and archived redo log files. It provides block-level corruption detection during both the backup and restore phases. It is optimized for performance and space consumption.

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

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.

source

In a database refresh scenario, the contents of the SOURCE database are extracted and stored in a file (or multiple files).

SOURCE

In a database refresh scenario, the contents of the SOURCE database are extracted and stored in a file (or multiple files).

source database

In the context of MS SQL database refresh, the "source database" is the database from which the backup file is created.

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.