

HP Database and Middleware Automation Solution Packs

For the Linux, Solaris, AIX, HP-UX, and Windows operating systems

Software Version: 9.14

Application Server Provisioning - WebSphere 8 Workflows

Document Release Date: June 2012

Software Release Date: June 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 2012 Hewlett-Packard Development Company, L.P.

Trademark Notices

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

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

<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.

Support

Visit the HP Software Support Online web site at:

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

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

Application Server Provisioning - WebSphere 8 Workflows	1
Contents	5
About HP DMA Solution Packs	8
Quick Start Tutorial	9
Install the Solution Pack	9
Create a Deployable Workflow	10
Create a Deployment	11
Run Your Workflow	12
View the Results	12
About this Solution	14
Audience	15
Supported Products and Platforms	15
Prerequisites	16
How this Solution is Organized	17
Additional Resources	22
How to Use this Solution	23
How to Expose Additional Workflow Parameters	24
Provision WebSphere 8 and StandAlone	25
Prerequisites for this Workflow	26
How this Workflow Works	28
How to Run this Workflow	32
Sample Scenario	36
Provision WebSphere 8 and Deployment Manager	38
Prerequisites for this Workflow	39
How this Workflow Works	41
How to Run this Workflow	45
Sample Scenario	49

Provision WebSphere 8 and Custom Node	51
Prerequisites for this Workflow	52
How this Workflow Works	54
How to Run this Workflow	58
Sample Scenario	63
Provision Websphere 8 Standalone Profile From Existing Install	66
Prerequisites for this Workflow	67
How this Workflow Works	69
How to Run this Workflow	71
Sample Scenario	75
Provision Websphere 8 Custom Node Profile From Existing Install	77
Prerequisites for this Workflow	78
How this Workflow Works	80
How to Run this Workflow	82
Sample Scenario	86
Reference Information	88
Parameter Information	89
Parameters for Provision WebSphere 8 and StandAlone	90
Parameters for Provision WebSphere 8 and Custom Node	95
Parameters for Provision WebSphere 8 and Deployment Manager	100
Parameters for Provision WebSphere 8 Standalone Profile from Existing Install	105
Parameters for Provision Websphere 8 Custom Node Profile From Existing Install	109
Step Information	113
Steps for Provision WebSphere 8 and StandAlone	114
Steps for Provision WebSphere 8 and Custom Node	115
Steps for Provision WebSphere 8 and Deployment Manager	116
Steps for Provision WebSphere 8 Standalone Profile from Existing Install	117
Steps for Provision WebSphere 8 Custom Node Profile from Existing Install	118
All WebSphere 8 Provisioning Steps	119
WebSphere 8 Input Parameter Mapping	122
Validate WebSphere 8 Stand Alone Parameters	123
Validate WebSphere 8 Deployment Manager Parameters	131

Validate WebSphere 8 Custom Node Parameters	138
Validate WebSphere 8 Existing Install Stand Alone Parameters	145
Validate WebSphere 8 Existing Install Custom Node Parameters	151
OS Prerequisite Check for WebSphere 8	157
WebSphere 8 Check File Download	159
WebSphere 8 Extract Archive	160
Create IBM Install Manager And WebSphere 8 Response File	162
Create WebSphere 8 Stand Alone Response File	164
Create WebSphere 8 Deployment Manager Response File	168
Create WebSphere 8 Custom Node Response File	172
WebSphere 8 Existing Install Create Custom Node Response File	176
Install IBM Install Manager And WebSphere 8	180
Create WebSphere 8 Profile	182
WebSphere 8 StandAlone Start Server	184
WebSphere 8 Deployment Manager Start Server	185
WebSphere 8 Cleanup Downloaded Files	186
Discover WebSphere	188
Other Reference Information	190
WebSphere 8 Product Documentation	190
Using this Solution Pack With HP Server Automation	190
Tips and Best Practices	191
Using a Policy to Specify Parameter Values	191
Create a Policy	191
Extract a Policy	192
Reference the Policy in the Deployment	193
Troubleshooting	194
Target Type	194
User Permissions and Related Requirements	194
Discovery in HP Server Automation	195
Glossary	196

About HP DMA Solution Packs

HP Database and Middleware Automation (HP DMA) software automates administrative tasks like provisioning and configuration, compliance, patching, and release management for databases and application servers. When performed manually, these day-to-day operations are error-prone, time consuming, and difficult to scale.

HP DMA automates these daily, mundane, and repetitive administration tasks that take up 60-70% of a database or application server administrator's day. Automating these tasks enables greater efficiency and faster change delivery with higher quality and better predictability.

HP DMA provides role-based access to automation content. This enables you to better utilize resources at every level:

- End-users can deliver routine, yet complex, DBA and middleware tasks.
- Operators can execute expert level tasks across multiple servers including provisioning, patching, configuration, and compliance checking.
- Subject matter experts can define, enforce, and audit full stack automation across network, storage, server, database, & middleware.

An HP DMA workflow performs a specific automated task—such as provisioning database or application servers, patching database or application servers, or checking a database or application server for compliance with a specific standard. You specify environment-specific information that the workflow requires by configuring its parameters.

Related HP DMA workflows are grouped together in solution packs. When you purchase or upgrade HP DMA content, you are granted access to download specific solution packs.

Chapter 6

Quick Start Tutorial

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

1. [Install the Solution Pack below](#)
2. [Create a Deployable Workflow on next page](#)
3. [Create a Deployment on page 11](#)
4. [Run Your Workflow on page 12](#)
5. [View the Results on page 12](#)

This tutorial provides a simplified demonstration using the Provision WebSphere 8 and StandAlone workflow. Default values are supplied for most input parameters. Before executing these procedures, make sure that these default values are suitable for your environment.

Note: See the [Reference Information](#) included in this guide for descriptions of all available input parameters for this 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: For information about other automation scenarios, see [How To Use This Solution](#).

Install the Solution Pack

The following instructions assume that you have purchased the Application Server Provisioning solution pack.

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).
4. On the system where you downloaded the solution pack, open a web browser, and log in to the HP DMA server using an account with administrative privileges.

For instructions, see “Getting Started” in the *User Guide: Database and Middleware Automation*. This guide is included in the HP Server Automation documentation library (SA version 9.10 and later).

5. On the Solutions > Installed tab, click the **Browse** button in the lower right corner. The Choose File dialog opens.
6. Locate and select the ZIP file that you extracted in step 3, and click **Open**.
7. 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:

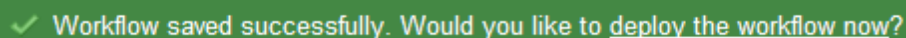


Read-only workflows are not deployable. You can create a deployable workflow by making a copy of a workflow template.

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 Provision WebSphere 8 and StandAlone workflow template.
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 – Must be OS
 - Target level – Must be a Server
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.

For more information about creating and working with workflows, see “Workflows” in the *User Guide: Database and Middleware Automation*. This guide is included in the HP Server Automation documentation library (SA version 9.10 and later).

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 (in this case, a Server).

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 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 *User Guide: Database and Middleware Automation*. This guide is included in the HP Server Automation documentation library (SA version 9.10 and later).

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 [Reference Information](#) included in this guide for descriptions of all available input parameters for this 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 [Using a Policy to Specify Parameter Values on page 191](#)).
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 area.
 - b. In the list of WORKFLOWS on the left side, select the workflow that you created.
 - c. In the list of DEPLOYMENTS in the center, double-click 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.

For more information about bridged execution workflows, see the *User Guide: Database and Middleware Automation*. This guide is included in the HP Server Automation documentation library (SA version 9.10 and later).

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 deployments that have run on this HP DMA server during the time period specified in the Filter box.

While the workflow is running, the History page shows nothing in the status column. A workflow that results in the FINISHED state also shows nothing in the status column on this page.

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 7

About this Solution

The HP Database and Middleware Automation Solution Packs Application Server Provisioning solution contains the following workflows:

- [Provision WebSphere 8 and StandAlone on page 25](#)
- [Provision WebSphere 8 and Deployment Manager on page 38](#)
- [Provision WebSphere 8 and Custom Node on page 51](#)
- [Provision Websphere 8 Standalone Profile From Existing Install on page 66](#)
- [Provision Websphere 8 Custom Node Profile From Existing Install on page 77](#)

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

The workflows perform extensive validation checks prior to provisioning WebSphere 8. All parameter values are validated to ensure that they do not contain any prohibited characters (see the [Reference Information on page 88](#) for details). Additional validation checks are performed at the operating system level. These include file system space checks and RPM checks (on Red Hat Linux platforms). All three workflows determine whether the pertinent files exist on the target machine; if they do not, the files are downloaded from the HP Server Automation core.

Although minimal WebSphere 8 knowledge is required to run this workflow using its default settings, the workflow is highly customizable and can support complex environment-specific deployment scenarios.

Note: For additional information about provisioning IBM WebSphere Application Server version 7, see the [HP DMA Application Server Provisioning Solution Pack version 9.10 User Guide](#).

The remaining topics in this chapter provide the following contextual information about this workflow:

- [Audience on next page](#)
- [Supported Products and Platforms on next page](#)
- [Prerequisites on page 16](#)
- [How this Solution is Organized on page 17](#)
- [Additional Resources on page 22](#)

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 190](#)).

Supported Products and Platforms

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

Operating Systems

For specific operating system versions supported, see the *HP Database and Middleware Automation Solution Packs version 9.14 Support Matrix* available in the HP Software product manuals library located here: <http://h20230.www2.hp.com/selfsolve/manuals>

Hardware Requirements

- If you are using HP Server Automation, see the *HP Server Automation Quick Reference: SA Installation Requirements* or the *HP Server Automation Standard/Advanced Installation Guide*.
- If you are using Database and Middleware Automation Solution Packs version 1.00, see the *HP Database and Middleware Automation Solution Packs Installation Guide*.
- For WebSphere 8 hardware and software requirements, see the [WebSphere 8 Product Documentation on page 190](#).

HP Software Requirements

This solution can be used with the following HP products:

- HP Server Automation version 9.11 (or later)
- HP Database and Middleware Automation Web Server version 6.0.17 (or later)

Bridged execution workflows can only be used with HP Server Automation version 9.11 (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.

How this Solution is Organized

In HP DMA, a workflow executes a process —such as installing a software product or creating a database.

A solution pack contains one or more related workflow templates. This solution contains the following workflow templates:

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.

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.

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.

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.

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.

What's Inside

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'. The 'Automation' tab is active, showing sub-tabs for 'Workflows', 'Steps', 'Functions', 'Policies', 'Deployments', 'Run', 'Console', and 'History'. The main content area is titled 'Provision WebSphere 8 and StandAlone' and has tabs for 'Documentation', 'Workflow', 'Deployments', and 'Roles'. The 'Documentation' tab is selected, showing the following details:

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

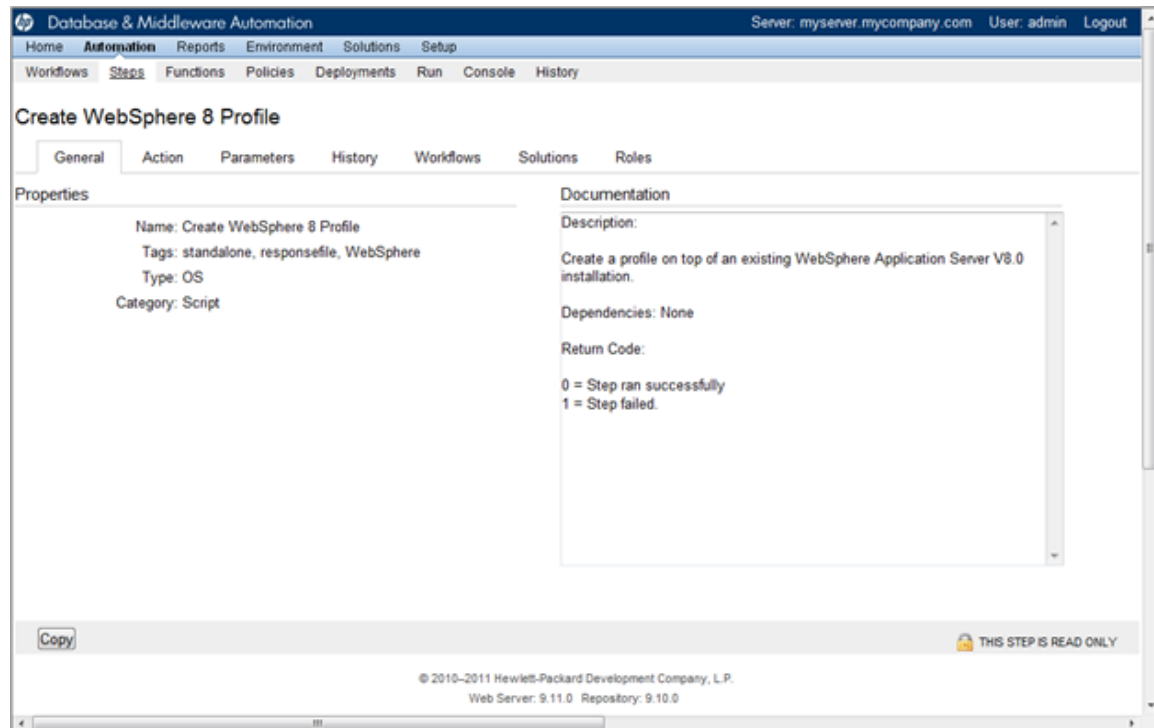
Documentation:

- 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

For a list of the specific OS versions supported, refer to the User Guide for this solution pack (see Additional Documentation below).
- Parameters**
The following characters cannot be used in the Admin User, Cell Name, Node Name, or Profile Name parameters: / \ * , ; : = + ? [< > & % ' "] > # \$ ^ { }

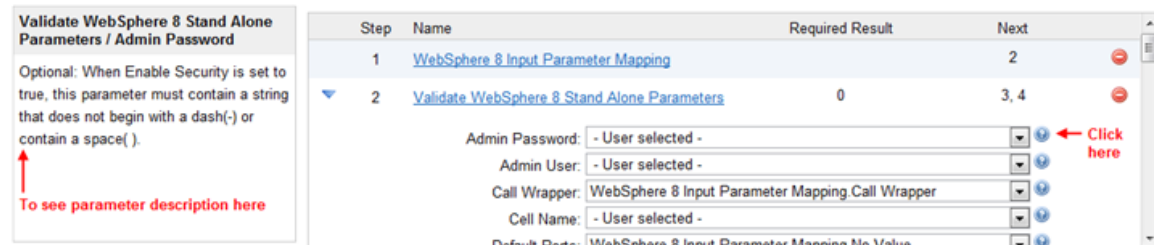
At the bottom of the console, there are buttons for 'Copy', 'EXPORT', and 'EXTRACT POLICY'. The footer includes the copyright notice: '© 2010–2011 Hewlett-Packard Development Company, L.P. Web Server: 9.11.0 Repository: 9.10.0'.

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.



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.



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

Database & Middleware Automation
Server: myserver.mycompany.com User: admin Logout

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 compressec
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. The top navigation bar includes 'Home', 'Automation', 'Reports', 'Environment', 'Solutions', and 'Setup'. The 'Automation' tab is selected, and the sub-tab 'Deployments' is active. The user is logged in as 'admin' on 'myserver.mycompany.com'. The main content area is titled 'Example Deployment' and has three sub-tabs: 'Targets', 'Parameters', and 'Roles'. The 'Parameters' tab is selected, showing a section titled 'Validate WebSphere 8 Stand Alone Parameters'. This section contains six parameters, each with a text input field, a description, and an 'Enter at runtime' checkbox.

Parameter Name	Description	Enter at runtime
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().	<input type="checkbox"/>
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: \ , ; : = + ? [< > & % ' " [] > # \$ ^ { }.	<input type="checkbox"/>
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.	<input type="checkbox"/>
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.	<input type="checkbox"/>
Install Manager Binary Location:	Required: Fully qualified path to the compressed Install Manager software package on the target machine.	<input type="checkbox"/>
Install Manager Extract Location:	Required: Fully qualified path where the compressed software will be extracted on the target machine.	<input type="checkbox"/>

All parameters used by the workflows in this solution pack are also described in the [Reference Information](#) for this solution pack.

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 10](#)).

Additional Resources

If you are using HP Server Automation version 9.10 (or later), see these documents:

- *HP Server Automation User Guide: Application Deployment Manager*
- *HP Server Automation User Guide: Database and Middleware Automation*

If you are using HP Server Automation version 9.0x, see these documents:

- *HP Database and Middleware Automation Solution Packs User Guide*
- *HP Server Automation Integration Guide*

If you are using HP Database and Middleware Automation Solution Packs version 1.00, see these documents:

- *HP Database and Middleware Automation Solution Packs Installation Guide*
- *HP Database and Middleware Automation Solution Packs User Guide*

Chapter 8

How to Use this Solution

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

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

The information presented here assumes the following: show assumptions

- HP DMA is installed and operational.
- At least one suitable target server is available (see [Supported Products and Platforms on page 15](#)).
- 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.

Note: All parameters used by each workflow in this solution are described in the [Reference Information on page 88](#).

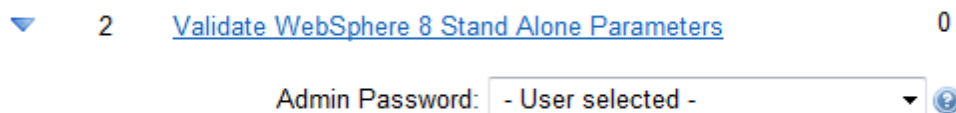
How to Expose Additional Workflow Parameters

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 (see [Create a Deployable Workflow on page 10](#)).
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:



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.

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 on next page	List of prerequisites that must be satisfied before you can run this workflow
How this Workflow Works on page 28	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
How to Run this Workflow on page 32	Instructions for running this workflow in your environment
Sample Scenario on page 36	Examples of typical parameter values for this workflow

Note: To view detailed information about the steps included in this workflow, see [Steps for Provision WebSphere 8 and StandAlone on page 114](#).

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 190](#).

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 HP Server Automation Core.

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. To provision WebSphere 7, see the [HP DMA Application Server Provisioning Solution Pack version 9.10 User Guide](#).

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.

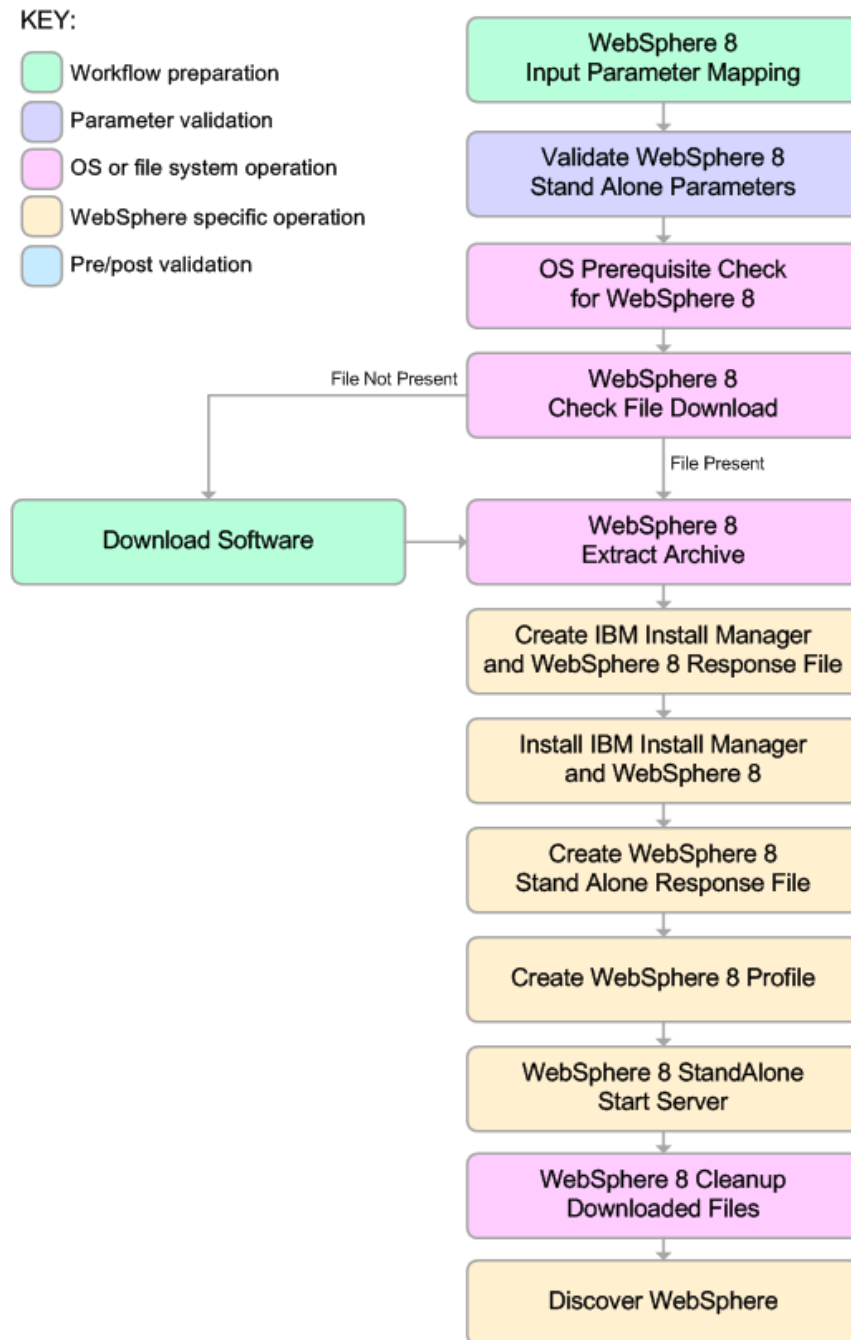
The workflow then performs the following operating system checks on the target machine:

1. All required libraries are present (see [Prerequisites for this Workflow on page 26](#)).
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 29](#)).
3. Checks the following:
 - a. Documented library requirements for WebSphere 8(see the [Prerequisites for this Workflow on page 26](#)).
 - 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 SA Core.
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 90](#)

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 10](#)).
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	true	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:4433/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 [How to Expose Additional Workflow Parameters on page 24](#)

See [Parameters for Provision WebSphere 8 and StandAlone on page 90](#) for detailed descriptions of all input parameters for this workflow, including default values.

Note: To avoid entering passwords in clear text, see [Using a Policy to Specify Parameter Values on page 191](#).

3. In the workflow editor, expose any additional parameters that you need (see [How to Expose Additional Workflow Parameters on page 24](#)). 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 11](#) 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 12](#) for instructions).

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an invalid parameter value is specified, an 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.

Note: To avoid entering passwords in clear text, see [Using a Policy to Specify Parameter Values on page 191](#).

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	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.

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.

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 on next page	List of prerequisites that must be satisfied before you can run this workflow
How this Workflow Works on page 41	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
How to Run this Workflow on page 45	Instructions for running this workflow in your environment
Sample Scenario on page 49	Examples of typical parameter values for this workflow

Note: To view detailed information about the steps included in this workflow, see [Steps for Provision WebSphere 8 and Deployment Manager on page 116](#).

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 190](#).

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 HP Server Automation Core.

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. To provision WebSphere 7, see the [HP DMA Application Server Provisioning Solution Pack version 9.10 User Guide](#).

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:

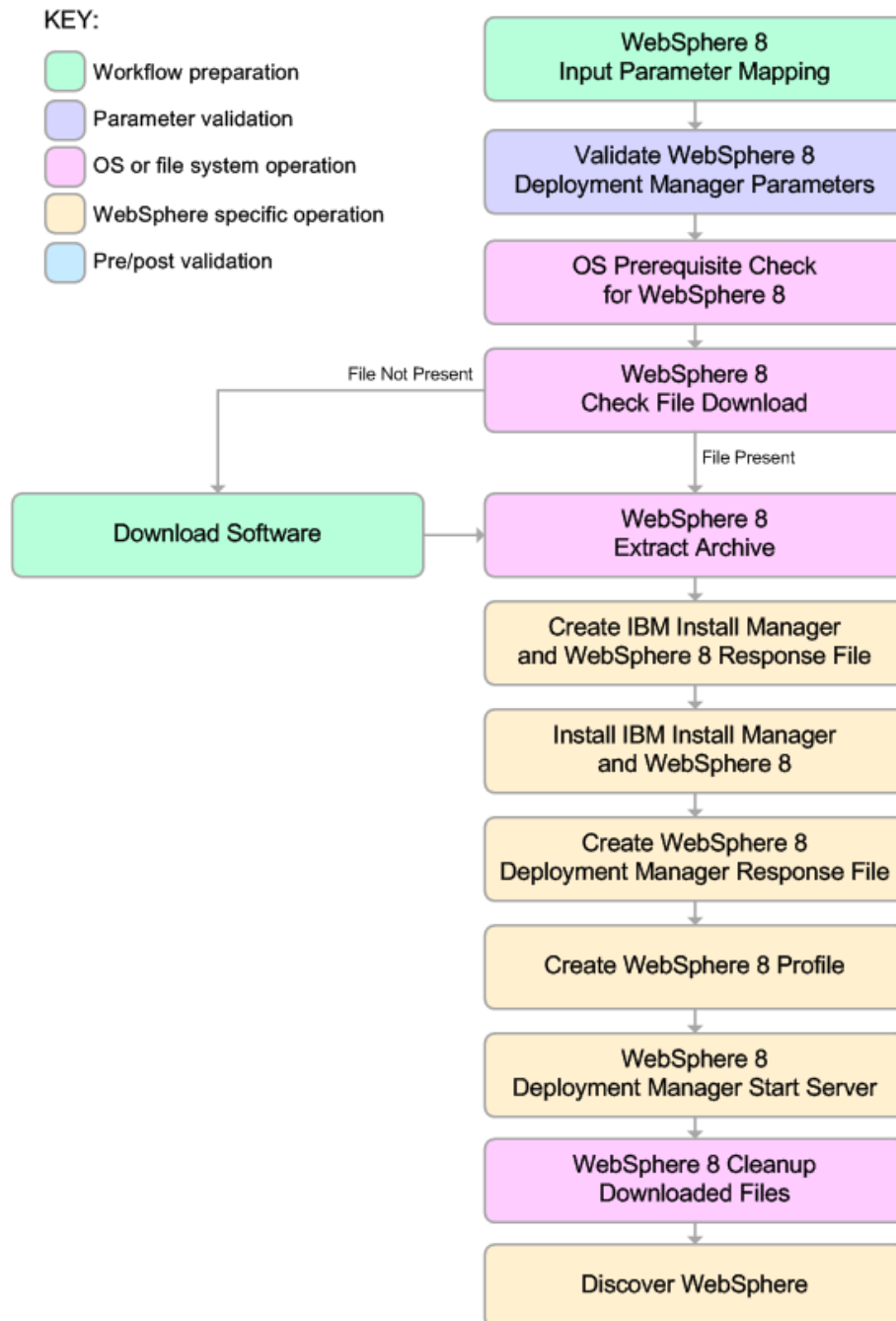
1. None of the following characters are used in the Admin User, Cell Name, Node Name, or Profile Name parameters: / \ * , ; = + ? | < > & % ' " [] > # \$ ^ { }
2. If Enable Security is true, Admin Password and Admin User are specified.
3. Admin Password (if specified) does not begin with a dash or contain 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 39](#)).
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 42](#)).
3. Checks the following:
 - a. Documented library requirements for WebSphere 8(see the [Prerequisites for this Workflow on page 39](#)).
 - 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 SA Core.
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 100](#)

Note: Before following this procedure, review the [Prerequisites for this Workflow on page 39](#), 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 10](#)).
2. Determine the values that you will specify for the following 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	true	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.

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:4433/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 [How to Expose Additional Workflow Parameters on page 24](#)

See [Parameters for Provision WebSphere 8 and Deployment Manager on page 100](#) for detailed descriptions of all input parameters for this workflow, including default values.

Note: To avoid entering passwords in clear text, see [Using a Policy to Specify Parameter Values on page 191](#).

3. In the workflow editor, expose any additional parameters that you need (see [How to Expose Additional Workflow Parameters on page 24](#)). 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 11](#) 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 12](#) for instructions).

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an invalid parameter value is specified, an 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.

Note: To avoid entering passwords in clear text, see [Using a Policy to Specify Parameter Values on page 191](#).

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.

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.

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 on next page	List of prerequisites that must be satisfied before you can run this workflow
How this Workflow Works on page 54	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
How to Run this Workflow on page 58	Instructions for running this workflow in your environment
Sample Scenario on page 63	Examples of typical parameter values for this workflow

Note: To view detailed information about the steps included in this workflow, see the [Steps for Provision WebSphere 8 and Custom Node on page 115](#).

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 190](#).

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 HP Server Automation Core.

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. To provision WebSphere 7, see the [HP DMA Application Server Provisioning Solution Pack version 9.10 User Guide](#).

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.

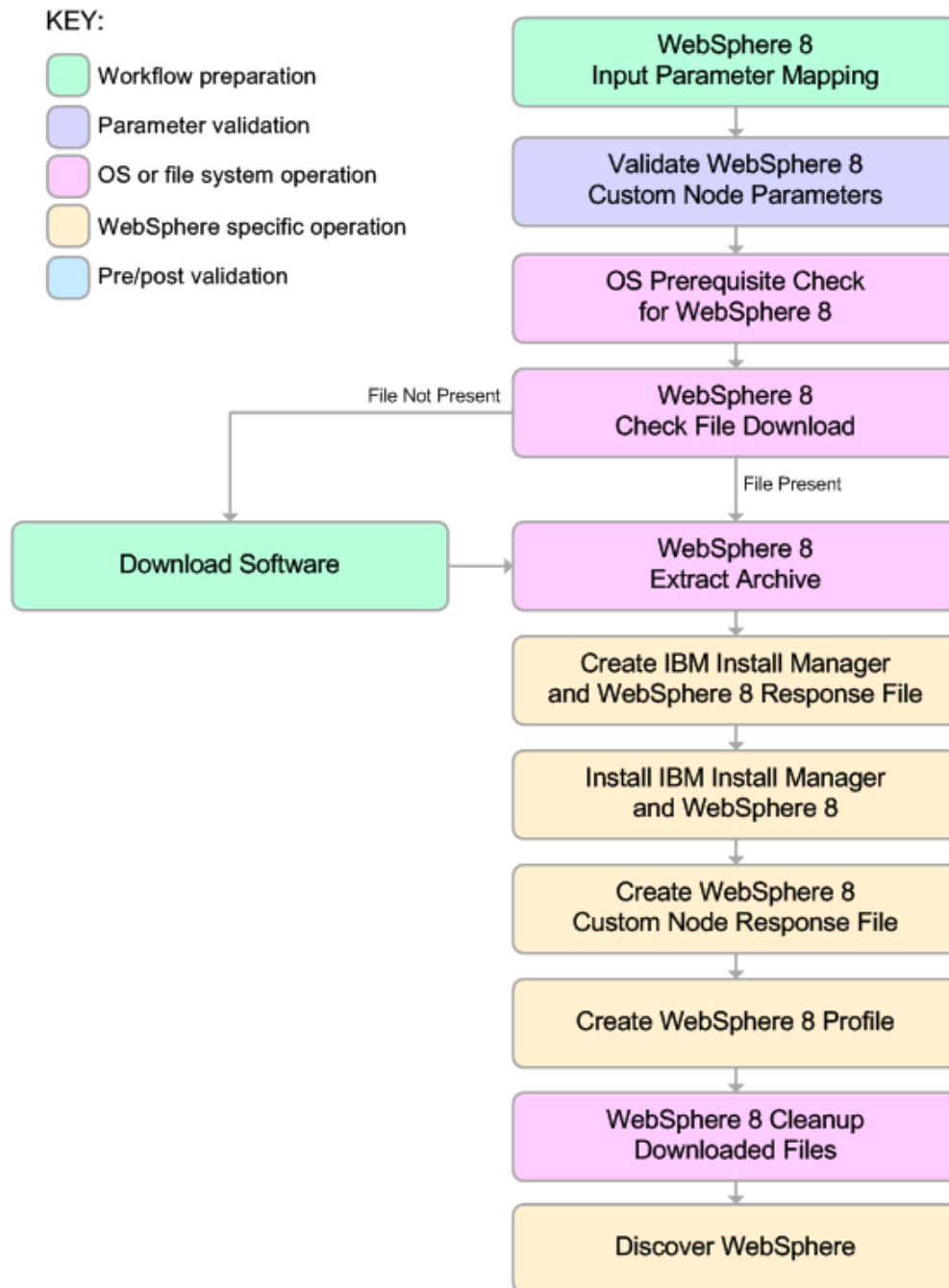
The workflow then performs the following operating system checks on the target machine:

1. All required libraries are present (see [Prerequisites for this Workflow on page 52](#)).
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 55](#)).
3. Checks the following:
 - a. Documented library requirements for WebSphere 8(see the [Prerequisites for this Workflow on page 52](#)).
 - 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 SA Core.
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 95](#)

Note: Before following this procedure, review the [Prerequisites for this Workflow on page 52](#), 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 10](#)).
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	true	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:4433/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 [How to Expose Additional Workflow Parameters on page 24](#)

See [Parameters for Provision WebSphere 8 and Custom Node on page 95](#) for detailed descriptions of all input parameters for this workflow, including default values.

Note: To avoid entering passwords in clear text, see [Using a Policy to Specify Parameter Values on page 191](#).

3. In the workflow editor, expose any additional parameters that you need (see [How to Expose Additional Workflow Parameters on page 24](#)). 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 11](#) 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 12](#) for instructions).

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an invalid parameter value is specified, an 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.

Note: To avoid entering passwords in clear text, see [Using a Policy to Specify Parameter Values on page 191](#).

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).

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 true, the new custom node will be federated during profile creation. If false, you must federate it later 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.
WebSphere Extract Location	/opt/IBM/wasv8	Fully qualified path where the compressed software will be extracted on the target machine.

Parameter Name	Example Value	Description
WebSphere Install Location	/opt/IBM/WebSphere8/AppServer	Fully qualified path where WebSphere will be installed.
Windows Administrator Password		This is the Administrator password. Required for Windows targets.
Windows Administrator User		This is the Administrator user. Required for Windows targets.

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 on next page	List of prerequisites that must be satisfied before you can run this workflow
How this Workflow Works on page 69	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
How to Run this Workflow on page 71	Instructions for running this workflow in your environment
Sample Scenario on page 75	Examples of typical parameter values for this workflow

Note: To view detailed information about the steps included in this workflow, see the [Steps for Provision WebSphere 8 Standalone Profile from Existing Install on page 117](#)

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 190](#).

How this Workflow Works

This topic contains the following information about the [Provision Websphere 8 Standalone Profile From Existing Install on page 66](#) 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 67](#)).

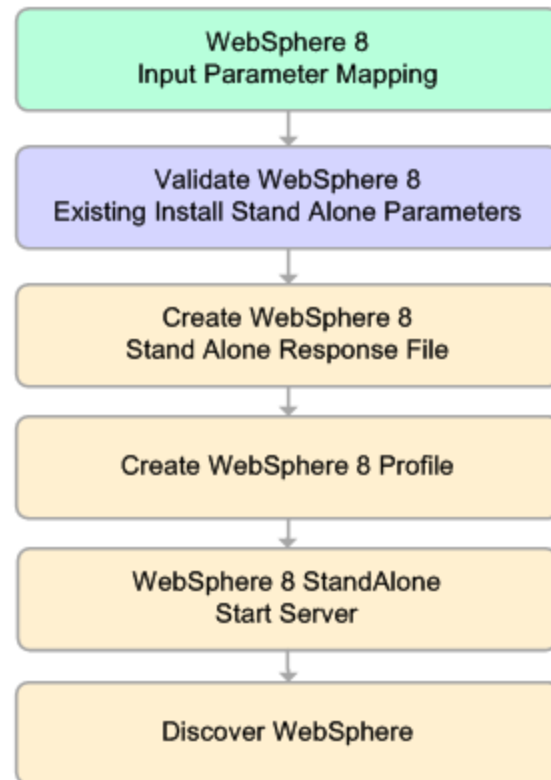
Steps Executed

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 Custom Node Profile From Existing Install on page 109](#)

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 10](#)).
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	true	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:4433/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 [How to Expose Additional Workflow Parameters on page 24](#)

See [Parameters for Provision Websphere 8 Custom Node Profile From Existing Install on page 109](#) for detailed descriptions of all input parameters for this workflow, including default values.

Note: To avoid entering passwords in clear text, see [Using a Policy to Specify Parameter Values on page 191](#).

3. In the workflow editor, expose any additional parameters that you need (see [How to Expose Additional Workflow Parameters on page 24](#)). 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 11](#) 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 12](#) for instructions).

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an invalid parameter value is specified, an 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.

Note: To avoid entering passwords in clear text, see [Using a Policy to Specify Parameter Values on page 191](#).

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.
Profile Name	StandAlone1	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; ; = + ? < > & % ' " [] > # \$ ^ { }.

Parameter Name	Example Value	Description
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.

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 on next page	List of prerequisites that must be satisfied before you can run this workflow
How this Workflow Works on page 80	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
How to Run this Workflow on page 82	Instructions for running this workflow in your environment
Sample Scenario on page 86	Examples of typical parameter values for this workflow

Note: To view detailed information about the steps included in this workflow, see [Steps for Provision WebSphere 8 Custom Node Profile from Existing Install on page 118](#).

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 190](#).

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 78](#)).

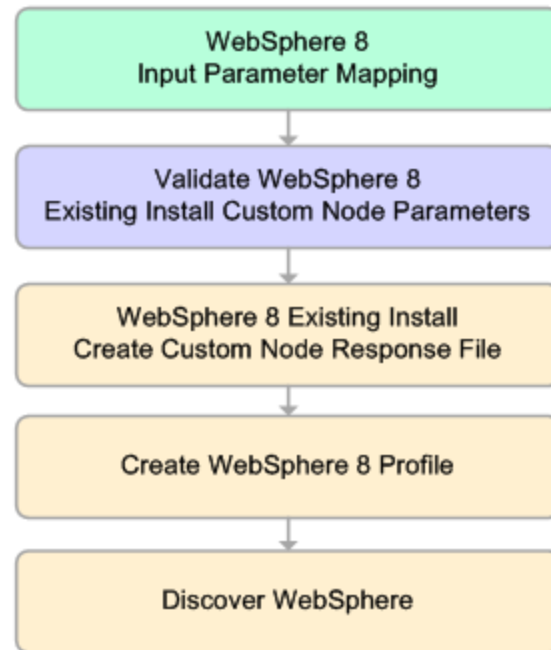
Steps Executed

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 109](#)

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 10](#)).
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	true	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:4433/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 [How to Expose Additional Workflow Parameters on page 24](#)

See [Parameters for Provision Websphere 8 Custom Node Profile From Existing Install on page 109](#) for detailed descriptions of all input parameters for this workflow, including default values.

Note: To avoid entering passwords in clear text, see [Using a Policy to Specify Parameter Values on page 191](#).

3. In the workflow editor, expose any additional parameters that you need (see [How to Expose Additional Workflow Parameters on page 24](#)). 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 11](#) 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 12](#) for instructions).

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an invalid parameter value is specified, an 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.

Note: To avoid entering passwords in clear text, see [Using a Policy to Specify Parameter Values on page 191](#).

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).

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.
Windows Administrator Password		This is the Administrator password. Required for Windows targets.
Windows Administrator User		This is the Administrator user. Required for Windows targets.

Reference Information

This chapter contains the following information:

Parameter Information

- [Parameters for Provision WebSphere 8 and StandAlone on page 90](#)
- [Parameters for Provision WebSphere 8 and Custom Node on page 95](#)
- [Parameters for Provision WebSphere 8 and Deployment Manager on page 100](#)
- [Parameters for Provision WebSphere 8 Standalone Profile from Existing Install on page 105](#)
- [Parameters for Provision Websphere 8 Custom Node Profile From Existing Install on page 109](#)
- [WebSphere 8 Product Documentation on page 190](#)

Step Information

- [Steps for Provision WebSphere 8 and StandAlone on page 114](#)
- [Steps for Provision WebSphere 8 and Custom Node on page 115](#)
- [Steps for Provision WebSphere 8 and Deployment Manager on page 116](#)
- [Steps for Provision WebSphere 8 Standalone Profile from Existing Install on page 117](#)
- [Steps for Provision WebSphere 8 Custom Node Profile from Existing Install on page 118](#)

Other Information

- [WebSphere 8 Product Documentation on page 190](#)
- [Using this Solution Pack With HP Server Automation on page 190](#)

Chapter 9

Parameter Information

The following provides detailed information about the parameters used by the WebSphere 8 provisioning workflows in this solution pack:

- [Parameters for Provision WebSphere 8 and StandAlone on next page](#)
- [Parameters for Provision WebSphere 8 and Custom Node on page 95](#)
- [Parameters for Provision WebSphere 8 and Deployment Manager on page 100](#)
- [Parameters for Provision WebSphere 8 Standalone Profile from Existing Install on page 105](#)
- [Parameters for Provision Websphere 8 Custom Node Profile From Existing Install on page 109](#)

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 24](#)). For most parameters, if you do not specify a value for a parameter, a default value is assigned.

For information about which steps use which parameters, see [How this Workflow Works on page 28](#).

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	no default	required	Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are : UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code> Windows targets: <code>jython</code> running as Administrator Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.
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.

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

Parameter Name	Default Value	Required	Description
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	true	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	no default	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.

Parameters Defined in this Step: Validate WebSphere 8 Stand Alone 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 / \ * , : ; = + ? < > & % ' " [] > # \$ ^ { }.
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.

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

Parameter Name	Default Value	Required	Description
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	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:4433/dma</code>

Parameters Defined in this Step: Discover WebSphere (continued)

Parameter Name	Default Value	Required	Description
Web Service User	administrator	required	User capable of modifying the managed environment through the discovery web service API.

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 24](#)). For most parameters, if you do not specify a value for a parameter, a default value is assigned.

For information about which steps use which parameters, see [How this Workflow Works on page 54](#).

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

Parameter Name	Default Value	Required	Description
Call Wrapper	no default	required	Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are : UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code> Windows targets: <code>jython</code> running as Administrator Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.
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 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	true	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 true, the new custom node will be federated during profile creation. If false, you must federate it later by using the addNode command.
File List	no default	optional	List of files required for download, Install Manager and WebSphere
Host Name	no default	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.

Input 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.
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 / \ * , ; = + ? < > & % ' " [] > # \$ ^ { }.
Profile Path	no default	required	Fully qualified path to the profile. For example: /opt/IBM/WebSphere/AppServer/profiles/AppServer1
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.
Profile Type	no default	required	Because this workflow creates a Custom Node profile, the value must be custom.
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.

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

Parameter Name	Default Value	Required	Description
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.
Template Path	no default	optional	Path to the profile templates in the WebSphere8 installation.
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:4433/dma</code>
Web Service User	administrator	required	User capable of modifying the managed environment through the discovery web service API.

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 24](#)). For most parameters, if you do not specify a value for a parameter, a default value is assigned

For information about which steps use which parameters, see [How this Workflow Works on page 41](#).

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	no default	required	<p>Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are :</p> <p>UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code></p> <p>Windows targets: <code>jython</code> running as Administrator</p> <p>Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.</p>
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.

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

Parameter Name	Default Value	Required	Description
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	true	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.
File List	no default	optional	List of files required for download, Install Manager and WebSphere
Host Name	no default	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.

Input Parameters Defined in this Step: Validate WebSphere 8 Deployment Manager 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.
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.
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 Path	no default	required	Fully qualified path to the profile. For example: /opt/IBM/WebSphere/AppServer/ profiles/AppServer1
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.

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

Parameter Name	Default Value	Required	Description
Profile Type	management	required	Because this workflow creates a Deployment Manager profile, the value must be management.
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 Type	DEPLOYMENT_MANAGER	required	Required: Specifies the type of management profile. The value is DEPLOYMENT_MANAGER for a deployment manager server.
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.
Template Path	no default	optional	Path to the profile templates in the WebSphere8 installation.
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.

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

Parameter Name	Default Value	Required	Description
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:4433/dma</code>
Web Service User	administrator	required	User capable of modifying the managed environment through the discovery web service API.

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 24](#)). For most parameters, if you do not specify a value for a parameter, a default value is assigned.

For information about which steps use which parameters, see [How this Workflow Works on page 69](#).

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 / \ * , ; = + ? < > & % ' " [] > # \$ ^ { }.
Binary Archive	no default	required	Fully qualified path to the compressed software package on the target machine.
Call Wrapper	no default	required	Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are : UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code> Windows targets: <code>jython</code> running as Administrator Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.
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.

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

Parameter Name	Default Value	Required	Description
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	true	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.
Extract Dir	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
File List	no default	optional	List of files required for download, Install Manager and WebSphere
Host Name	no default	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.

Parameters Defined in this Step: Validate WebSphere 8 Existing Install Stand Alone 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 / \ * , : ; = + ? < > & % ' " [] > # \$ ^ { }.
Profile Path	no default	required	Fully qualified path to the profile. For example: /opt/IBM/WebSphere/AppServer/ profiles/AppServer1
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.
Profile Type	no default	required	Required: Because this workflow creates a stand-alone profile, the value must be standAlone.
Server Name	no default	required	Name of the application server that will be created under the profile.

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

Parameter Name	Default Value	Required	Description
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.
Template Path	no default	optional	Path to the profile templates in the WebSphere8 installation.
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.
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 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 24](#)). For most parameters, if you do not specify a value for a parameter, a default value is assigned

For information about which steps use which parameters, see [How this Workflow Works on page 80](#).

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

Parameter Name	Default Value	Required	Description
Call Wrapper	no default	required	Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are : UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code> Windows targets: <code>jython</code> running as Administrator Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.
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	true	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.
File List	no default	optional	List of files required for download, Install Manager and WebSphere
Host Name	no default	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=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.
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 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.
Profile Type	no default	required	Because this workflow creates a Custom Node profile, the value must be custom.
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.
Template Path	no default	optional	Path to the profile templates in the WebSphere8 installation.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.

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

Parameter Name	Default Value	Required	Description
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:4433/dma</code>
Web Service User	administrator	required	User capable of modifying the managed environment through the discovery web service API.

Chapter 10

Step Information

The following topics provide detailed information about the steps used by the WebSphere 8 provisioning workflows in this solution pack:

- [Steps for Provision WebSphere 8 and StandAlone on next page](#)
- [Steps for Provision WebSphere 8 and Custom Node on page 115](#)
- [Steps for Provision WebSphere 8 and Deployment Manager on page 116](#)
- [Steps for Provision WebSphere 8 Standalone Profile from Existing Install on page 117](#)
- [Steps for Provision WebSphere 8 Custom Node Profile from Existing Install on page 118](#)

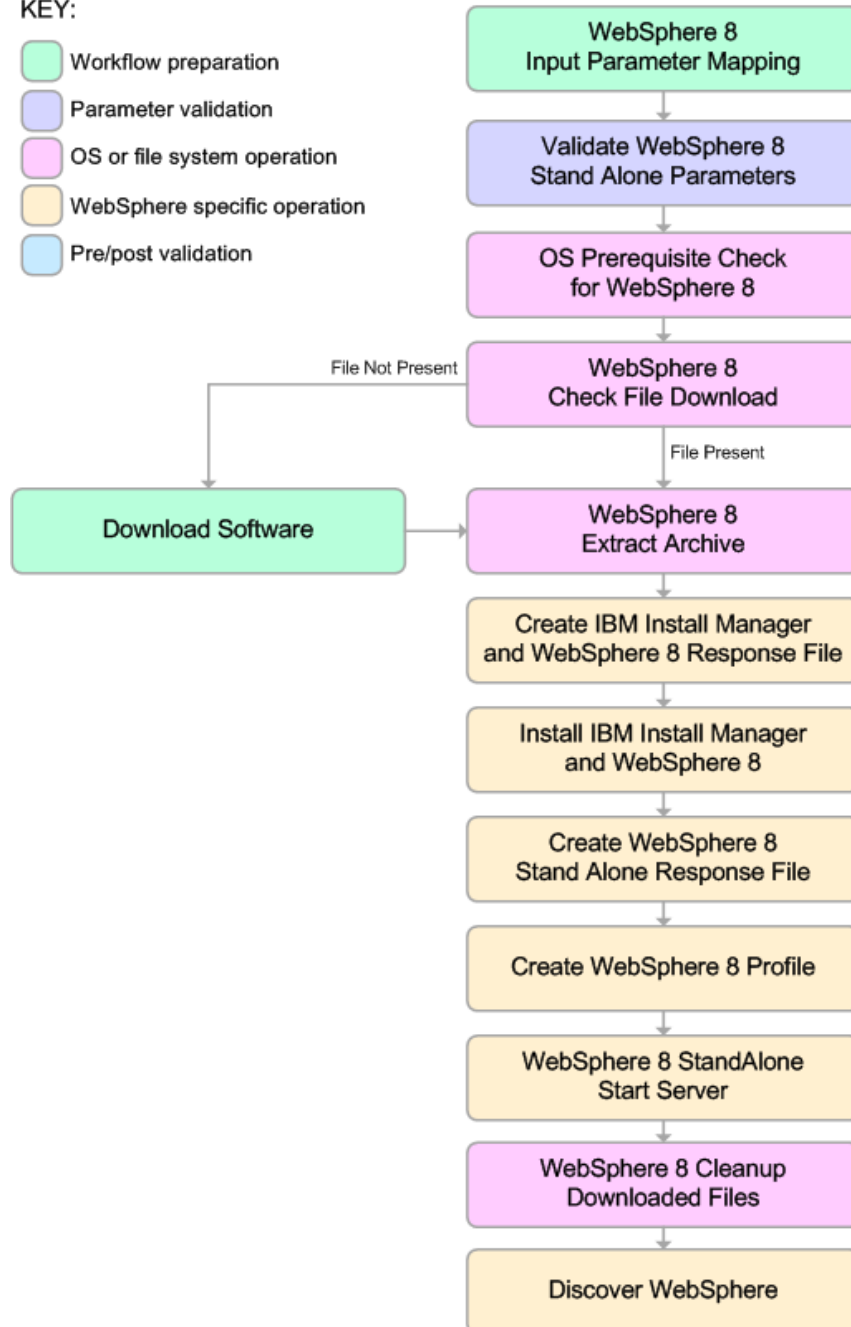
The following topic lists all the steps used by the WebSphere 8 provisioning workflows in this solution pack: [All WebSphere 8 Provisioning Steps on page 119](#)

Steps for Provision WebSphere 8 and StandAlone

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.

KEY:

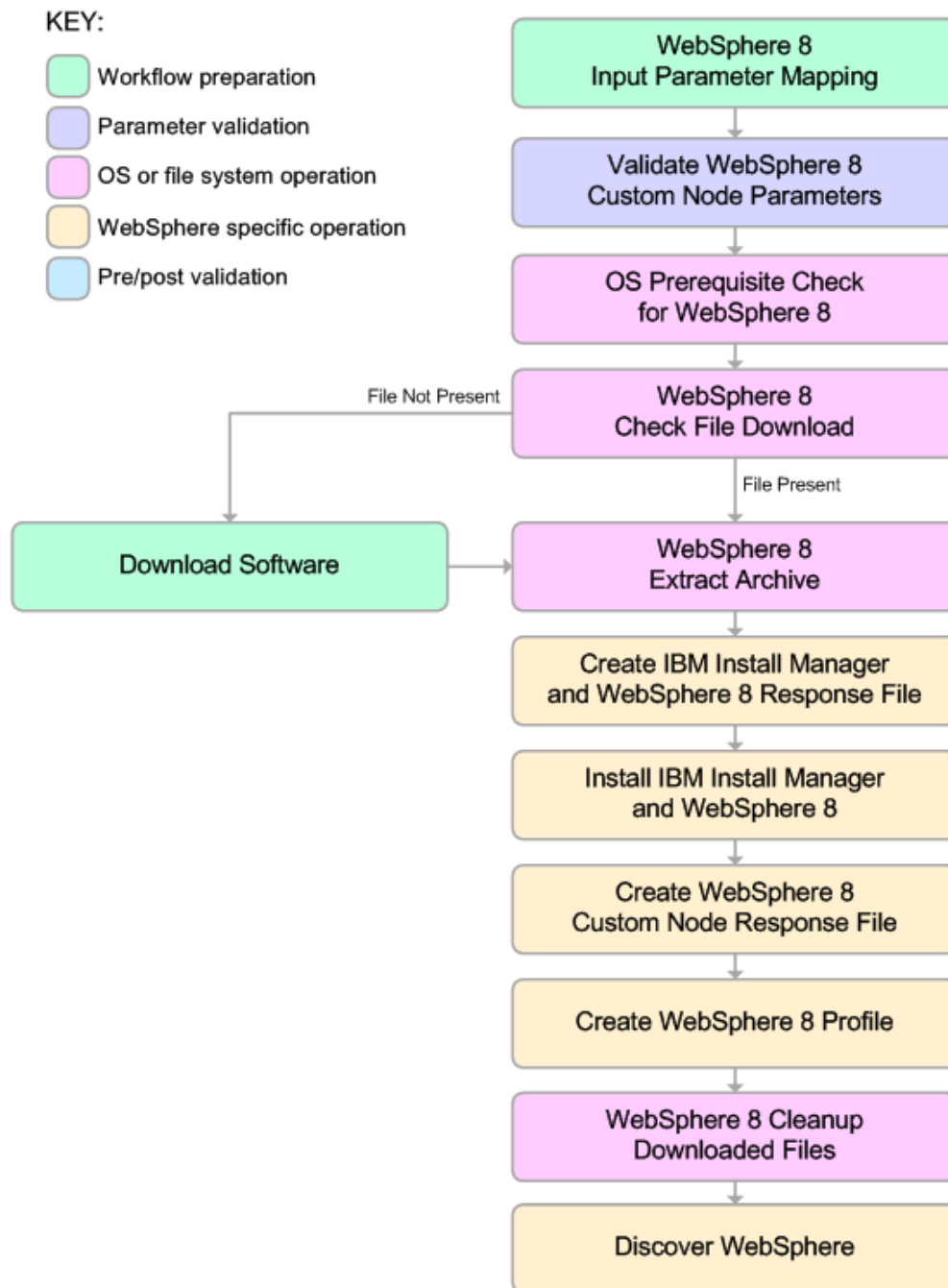
- Workflow preparation
- Parameter validation
- OS or file system operation
- WebSphere specific operation
- Pre/post validation



For parameter descriptions and defaults, see [Parameters for Provision WebSphere 8 and StandAlone on page 90](#).

Steps for Provision WebSphere 8 and Custom Node

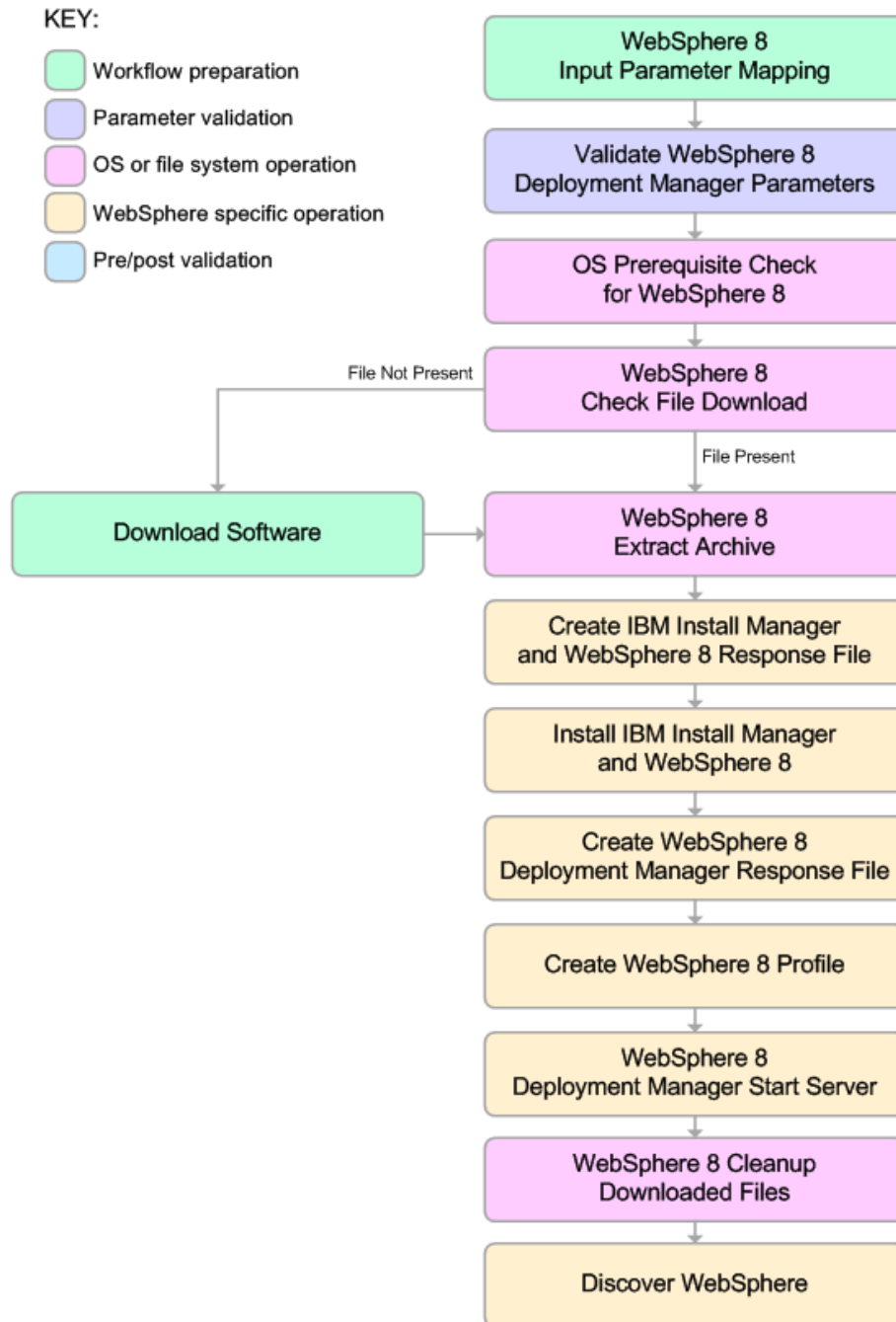
The [Provision WebSphere 8 and Custom Node on page 51](#) workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



For parameter descriptions and defaults, see [Parameters for Provision WebSphere 8 and Custom Node on page 95](#).

Steps for Provision WebSphere 8 and Deployment Manager

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.






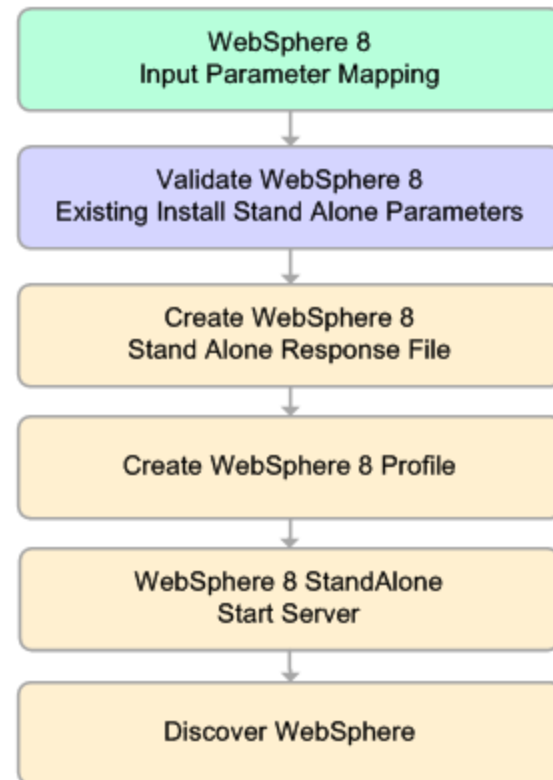
For parameter descriptions and defaults, see [Parameters for Provision WebSphere 8 and Deployment Manager](#) on page 100.

Steps for Provision WebSphere 8 Standalone Profile from Existing Install

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.

KEY:

-  Workflow preparation
-  Parameter validation
-  WebSphere specific operation






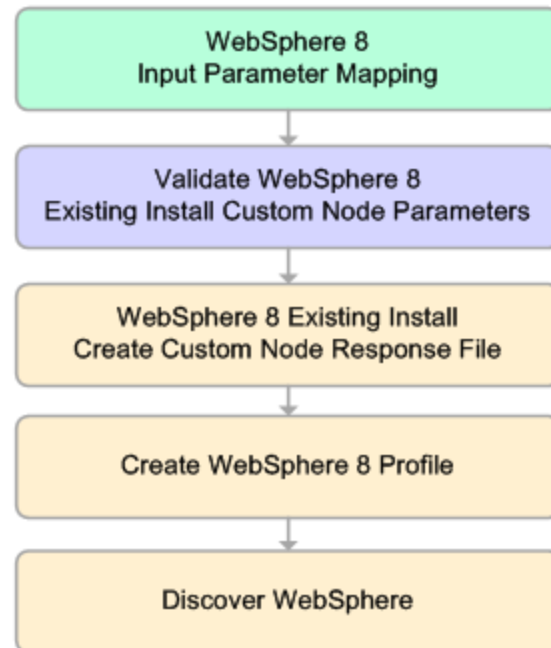
For parameter descriptions and defaults, see [Parameters for Provision WebSphere 8 Standalone Profile from Existing Install](#) on page 105.

Steps for Provision WebSphere 8 Custom Node Profile from Existing Install

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.

KEY:

-  Workflow preparation
-  Parameter validation
-  WebSphere specific operation



For parameter descriptions and defaults, see [Parameters for Provision Websphere 8 Custom Node Profile From Existing Install](#) on page 109.

All WebSphere 8 Provisioning Steps

The following topics provide detailed information about the steps used by the WebSphere 8 provisioning workflows in this solution pack:

Prepare Workflow Steps:

Step	Description
WebSphere 8 Input Parameter Mapping on page 122	This step creates the call wrapper and determines the target server platform type.
OS Prerequisite Check for WebSphere 8 on page 157	This step checks the following: <ol style="list-style-type: none">1. Documented library requirements for WebSphere 8.2. File system space requirements where WebSphere 8 will be installed.3. Temporary space requirements where the compressed software will be extracted before it is installed.

Parameter Validation Steps

Step	Description
Validate WebSphere 8 Stand Alone Parameters on page 123	This step validates the parameters needed to install WebSphere 8 and create a stand-alone profile.
Validate WebSphere 8 Deployment Manager Parameters on page 131	This step validates the parameters needed to install WebSphere 8 and create a Deployment Manager profile.
Validate WebSphere 8 Custom Node Parameters on page 138	This step validates the parameters needed to install WebSphere 8 and create a custom profile.
Validate WebSphere 8 Existing Install Stand Alone Parameters on page 145	This step prepares the parameters needed to create a stand-alone profile on an existing WebSphere 8 installation.
Validate WebSphere 8 Existing Install Custom Node Parameters on page 151	This step prepares the parameters needed to create a Custom Node profile on an existing WebSphere 8 installation.

File Management Steps

Step	Description
WebSphere 8 Check File Download on page 159	This step checks for the existence of a file on the target machine before downloading that file from the SA Core. For each file in the list, it performs the following actions: <ol style="list-style-type: none"> 1. Determines whether the file is in the expected location on the target machine. 2. If the file is not in the expected location, adds that file to a list of files that need to be downloaded.
WebSphere 8 Extract Archive on page 160	This step first checks to ensure that the archive file exists. Then, based on the archive extension, extracts the archive to the specified directory.

Installation Steps

Step	Description
Create IBM Install Manager And WebSphere 8 Response File on page 162	This step creates a response file for the purpose of installing a new instance of WebSphere 8.
Create WebSphere 8 Stand Alone Response File on page 164	This step creates a new response file for the purpose of creating a stand-alone profile on top of an existing WebSphere 8 installation.
Create WebSphere 8 Deployment Manager Response File on page 168	This step creates a new response file for the purpose of creating a Deployment Manager profile on top of an existing WebSphere 8 installation.
Create WebSphere 8 Custom Node Response File on page 172	This step creates a new response file for the purpose of creating a custom profile on top of an existing WebSphere 8 installation.
WebSphere 8 Existing Install Create Custom Node Response File on page 176	This step creates a new response file for the purpose of creating a Custom Node profile on top of an existing WebSphere 8 installation.
Install IBM Install Manager And WebSphere 8 on page 180	This step installs a new instance of WebSphere 8.

Post-Installation Steps

Step	Description
Create WebSphere 8 Profile on page 182	This step creates a profile on top of an existing WebSphere 8 installation..

Step	Description
WebSphere 8 StandAlone Start Server on page 184	This step starts the stand-alone application server.
WebSphere 8 Deployment Manager Start Server on page 185	This step starts the Deployment Profile application server.
WebSphere 8 Cleanup Downloaded Files on page 186	This step removes all downloaded files and archives. It must run as the owner of the pertinent files and directories.
Discover WebSphere on page 188	This step audits the target server's physical environment looking for WebSphere 8 cells, clusters, and managed servers associated with the Known Profile Roots that you specify. When any of these items is found, it is added to HP DMA environment.

WebSphere 8 Input Parameter Mapping

Purpose

This step creates the call wrapper and determines the target server platform type.

Input Parameters

There are no input parameters for this step.

Output Parameters

Parameter Name	Description
Call Wrapper	<p>Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are :</p> <p>UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code></p> <p>Windows targets: <code>jython</code> running as Administrator</p> <p>Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.</p>
No Value	Used to hide unused parameters in later steps.

Return Codes

0 = No errors occurred during the execution of this step.

1 = One or more errors occurred.

Used By Workflows

- [Provision WebSphere 8 and StandAlone on page 25](#)
- [Provision WebSphere 8 and Deployment Manager on page 38](#)
- [Provision WebSphere 8 and Custom Node on page 51](#)
- [Provision Websphere 8 Standalone Profile From Existing Install on page 66](#)
- [Provision Websphere 8 Custom Node Profile From Existing Install on page 77](#)

Validate WebSphere 8 Stand Alone Parameters

Purpose

This step validates the parameters needed to install WebSphere 8 and create a stand-alone profile.

Input Parameters for 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 <code>/ \ * , ; = + ? < > & % ' " [] > # \$ ^ { }</code> .
Call Wrapper	no default	required	Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are : UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code> Windows targets: <code>jython</code> running as Administrator Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.
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.
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	true	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.

Input Parameters for Validate WebSphere 8 Stand Alone Parameters (continued)

Parameter Name	Default Value	Required	Description
Host Name	no default	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=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.

Input Parameters for 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.
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.

Input Parameters for Validate WebSphere 8 Stand Alone Parameters (continued)

Parameter Name	Default Value	Required	Description
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.

Output Parameters for Validate WebSphere 8 Stand Alone Parameters

Parameter Name	Description
Admin 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	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> .
Binary Archive	Fully qualified path to the compressed WebSphere 8 software package on the target machine.
Call Wrapper	<p>Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are :</p> <p>UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code></p> <p>Windows targets: <code>jython</code> running as Administrator</p> <p>Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.</p>

Output Parameters for Validate WebSphere 8 Stand Alone Parameters (continued)

Parameter Name	Description
Cell Name	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	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	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	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.
Extract Dir	Fully qualified path where the compressed software will be extracted on the target machine.
File List	Comma-separated list of files that need to be downloaded.
Host Name	Hostname or IP address of the target machine.
Install Location	Fully qualified path where WebSphere Application Server will be installed. For example: /opt/IBM/WebSphere/AppServer
Install Manager Binary Location	Fully qualified path to the compressed Install Manager software package on the target machine.
Install Manager Extract Location	Fully qualified path where the compressed software will be extracted on the target machine.
Install Manager Install Location	Fully qualified path where Install Manager will be installed.
Keystore Password	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	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.

Output Parameters for Validate WebSphere 8 Stand Alone Parameters (continued)

Parameter Name	Description
Node Name	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	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	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.
Personal CertValidity Period	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	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	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? < > & % ' " [] > # \$ ^ { }.
Profile Path	Fully qualified path to the profile. For example: /opt/IBM/WebSphere/AppServer/profiles/AppServer1
Profile Response File	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation.
Profile Type	Because this workflow creates a stand-alone profile, the value is standAlone.
Response File	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	Name of the application server that will be created under the profile.

Output Parameters for Validate WebSphere 8 Stand Alone Parameters (continued)

Parameter Name	Description
Signing CertDN	Distinguished name of the signing certificate. For example: CN=dmlab-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	Amount of time in years that the root certificate is valid. Default is 15 years.
Starting Port	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.
Template Path	Path to the profile templates in the WebSphere8 installation.
Validate Ports	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	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Extract Location	Fully qualified path where the compressed software will be extracted on the target machine.
WebSphere Install Location	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	The Windows Administrator password. Required for Windows.
Windows Administrator User	This is the Windows Administrator user. Required for Windows.

Return Codes

0 = No errors occurred during the execution of this step.

1 = One or more errors occurred.

Used By Workflows

- [Provision WebSphere 8 and StandAlone on page 25](#)
- [Provision Websphere 8 Standalone Profile From Existing Install on page 66](#)

Validate WebSphere 8 Deployment Manager Parameters

Purpose

This step validates the parameters needed to install WebSphere 8 and create a Deployment Manager profile.

Input Parameters for 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 <code>/ \ * , ; = + ? < > & % ' " [] > # \$ ^ { }</code> .
Call Wrapper	no default	required	Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are : UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code> Windows targets: <code>jython</code> running as Administrator Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.
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.
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	true	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	no default	required	Hostname or IP address of the target machine.

Input Parameters for 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 <code>/ \ * , ; : = + ? < > & % ' " [] > # \$ ^ { }</code> . 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 <code>deployAdminConsole</code> or <code>defaultAppDeployAndConfig</code> . 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.

Input Parameters for Validate WebSphere 8 Deployment Manager 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.
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.
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	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.

Input Parameters for Validate WebSphere 8 Deployment Manager Parameters (continued)

Parameter Name	Default Value	Required	Description
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.

Output Parameters for Validate WebSphere 8 Deployment Manager Parameters

Parameter Name	Description
Admin 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	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	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	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	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.
File List	Comma-separated list of files that need to be downloaded.
Host Name	Hostname or IP address of the target machine.

**Output Parameters for Validate WebSphere 8 Deployment Manager Parameters
(continued)**

Parameter Name	Description
Install Manager Binary Location	Fully qualified path to the compressed Install Manager software package on the target machine.
Install Manager Extract Location	Fully qualified path where the compressed software will be extracted on the target machine.
Install Manager Install Location	Fully qualified path where Install Manager will be installed.
Keystore Password	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	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	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	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	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.
Personal CertValidity Period	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	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.

**Output Parameters for Validate WebSphere 8 Deployment Manager Parameters
(continued)**

Parameter Name	Description
Profile Name	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] > # \$ ^ { }.
Profile Path	Fully qualified path to the profile. For example: /opt/IBM/WebSphere/AppServer/profiles/AppServer1
Profile Response File	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation.
Profile Type	Because this workflow creates a Deployment Manager profile, the value must be management.
Response File	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 Type	Required: Specifies the type of management profile. The value is DEPLOYMENT_MANAGER for a deployment manager server.
Signing CertDN	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	Amount of time in years that the root certificate is valid. Default is 15 years.
Starting Port	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.
Template Path	Path to the profile templates in the WebSphere8 installation.
Validate Ports	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	Fully qualified path to the compressed WebSphere software package on the target machine.

**Output Parameters for Validate WebSphere 8 Deployment Manager Parameters
(continued)**

Parameter Name	Description
WebSphere Extract Location	Fully qualified path where the compressed software will be extracted on the target machine.
WebSphere Install Location	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	The Windows Administrator password. Required for Windows.
Windows Administrator User	This is the Windows Administrator user. Required for Windows.

Return Codes

0 = No errors occurred during the execution of this step.

1 = One or more errors occurred.

Used By Workflows

[Provision WebSphere 8 and Deployment Manager on page 38](#)

Validate WebSphere 8 Custom Node Parameters

Purpose

This step validates the parameters needed to install WebSphere 8 and create a custom profile.

Input Parameters for Validate WebSphere 8 Custom Node Parameters

Parameter Name	Default Value	Required	Description
Call Wrapper	no default	required	Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are : UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code> Windows targets: <code>jython</code> running as Administrator Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.
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 for Validate WebSphere 8 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	true	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 true, the new custom node will be federated during profile creation. If false, you must federate it later by using the addNode command.
Host Name	no default	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 for 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=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.
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 Path	no default	required	Fully qualified path to the profile. For example: /opt/IBM/WebSphere/AppServer/ profiles/AppServer1
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=dmlab-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 for 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.

Output Parameters for Validate WebSphere 8 Custom Node Parameters

Parameter Name	Description
Call Wrapper	<p>Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are :</p> <p>UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code></p> <p>Windows targets: <code>jython</code> running as Administrator</p> <p>Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.</p>
Cell Name	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	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().

Output Parameters for Validate WebSphere 8 Custom Node Parameters (continued)

Parameter Name	Description
Dmgr Admin User	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).
Enable Security	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	If true, the new custom node will be federated during profile creation. If false, you must federate it later by using the addNode command.
File List	List of files required for download, Install Manager and WebSphere
Host Name	Hostname or IP address of the target machine.
Install Manager Binary Location	Fully qualified path to the compressed Install Manager software package on the target machine.
Install Manager Extract Location	Fully qualified path where the compressed software will be extracted on the target machine.
Install Manager Install Location	Fully qualified path where Install Manager will be installed.
Keystore Password	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	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.

Output Parameters for Validate WebSphere 8 Custom Node Parameters (continued)

Parameter Name	Description
Node Name	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	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.
Personal CertValidity Period	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	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	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? < > & % ' " [] > # \$ ^ { }.
Profile Path	Fully qualified path to the profile. For example: /opt/IBM/WebSphere/AppServer/ profiles/AppServer1
Profile Response File	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation.
Profile Type	Because this workflow creates a Custom Node profile, the value must be custom.
Response File	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	Distinguished name of the signing certificate. For example: CN=dmlab-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.

Output Parameters for Validate WebSphere 8 Custom Node Parameters (continued)

Parameter Name	Description
Signing CertValidity Period	Amount of time in years that the root certificate is valid. Default is 15 years.
Template Path	Path to the profile templates in the WebSphere8 installation.
WebSphere Binary Location	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Extract Location	Fully qualified path where the compressed software will be extracted on the target machine.
WebSphere Install Location	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	The Windows Administrator password. Required for Windows.
Windows Administrator User	This is the Windows Administrator user. Required for Windows.

Return Codes

0 = No errors occurred during the execution of this step.

1 = One or more errors occurred.

Used By Workflows

- [Provision WebSphere 8 and Custom Node on page 51](#)
- [Provision Websphere 8 Custom Node Profile From Existing Install on page 77](#)

Validate WebSphere 8 Existing Install Stand Alone Parameters

Purpose

This step prepares the parameters needed to create a stand-alone profile on an existing WebSphere 8 installation.

Input Parameters for 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	no default	required	Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are : UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code> Windows targets: <code>jython</code> running as Administrator Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.
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.

Input Parameters for Validate WebSphere 8 Existing Install Stand Alone Parameters (continued)

Parameter Name	Default Value	Required	Description
Enable Security	true	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	no default	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.
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.

Input Parameters for Validate WebSphere 8 Existing Install Stand Alone Parameters (continued)

Parameter Name	Default Value	Required	Description
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	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 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.

Output Parameters for Validate WebSphere 8 Existing Install Stand Alone Parameters

Parameter Name	Description
Admin 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	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 / \ * , ; : = + ? < > & % ' " [] > # \$ ^ { }.
Binary Archive	Fully qualified path to the compressed WebSphere 8 software package on the target machine.
Call Wrapper	<p>Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are :</p> <p>UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code></p> <p>Windows targets: <code>jython</code> running as Administrator</p> <p>Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.</p>
Cell Name	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	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	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	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.
Extract Dir	Fully qualified path where the compressed software will be extracted on the target machine.
File List	Comma-separated list of files that need to be downloaded.
Host Name	Hostname or IP address of the target machine.

Output Parameters for Validate WebSphere 8 Existing Install Stand Alone Parameters (continued)

Parameter Name	Description
Keystore Password	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	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	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	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	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.
Personal CertValidity Period	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	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	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? < > & % ' " [] > # \$ ^ { }.
Profile Path	Fully qualified path to the profile. For example: /opt/IBM/WebSphere/AppServer/profiles/AppServer1
Profile Response File	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation.
Profile Type	Because this workflow creates a stand-alone profile, the value is standAlone.
Server Name	Name of the application server that will be created under the profile.

Output Parameters for Validate WebSphere 8 Existing Install Stand Alone Parameters (continued)

Parameter Name	Description
Signing CertDN	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	Amount of time in years that the root certificate is valid. Default is 15 years.
Starting Port	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.
Template Path	Path to the profile templates in the WebSphere8 installation.
Validate Ports	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 Install Location	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	The Windows Administrator password. Required for Windows.
Windows Administrator User	This is the Windows Administrator user. Required for Windows.

Return Codes

0 = No errors occurred during the execution of this step.

1 = One or more errors occurred.

Used By Workflows

[Provision Websphere 8 Standalone Profile From Existing Install on page 66](#)

Validate WebSphere 8 Existing Install Custom Node Parameters

Purpose

This step prepares the parameters needed to create a Custom Node profile on an existing WebSphere 8 installation.

Input Parameters for Validate WebSphere 8 Existing Install Custom Node Parameters

Parameter Name	Default Value	Required	Description
Call Wrapper	no default	required	Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are : UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code> Windows targets: <code>jython</code> running as Administrator Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.
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 for 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	true	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	no default	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.
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.
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 / \ * , ; : = + ? < > & % ' " [] > # \$ ^ { }.

Input Parameters for Validate WebSphere 8 Existing Install Custom Node Parameters (continued)

Parameter Name	Default Value	Required	Description
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=dmlab-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.

Output Parameters for Validate WebSphere 8 Existing Install Custom Node Parameters

Parameter Name	Description
Call Wrapper	<p>Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are :</p> <p>UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code></p> <p>Windows targets: <code>jython</code> running as Administrator</p> <p>Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.</p>

Output Parameters for Validate WebSphere 8 Existing Install Custom Node Parameters (continued)

Parameter Name	Description
Cell Name	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	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	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).
Enable Security	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.
File List	List of files required for download, Install Manager and WebSphere
Host Name	Hostname or IP address of the target machine.
Install Manager Install Location	Fully qualified path where Install Manager will be installed.
Keystore Password	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	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.

Output Parameters for Validate WebSphere 8 Existing Install Custom Node Parameters (continued)

Parameter Name	Description
Personal CertDN	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	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	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	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] > # \$ ^ { }.
Profile Path	Fully qualified path to the profile. For example: /opt/IBM/WebSphere/AppServer/ profiles/AppServer1
Profile Response File	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation.
Profile Type	Because this workflow creates a Custom Node profile, the value must be custom.
Signing CertDN	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	Amount of time in years that the root certificate is valid. Default is 15 years.
Template Path	Path to the profile templates in the WebSphere8 installation.

Output Parameters for Validate WebSphere 8 Existing Install Custom Node Parameters (continued)

Parameter Name	Description
WebSphere Install Location	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	The Windows Administrator password. Required for Windows.
Windows Administrator User	This is the Windows Administrator user. Required for Windows.

Return Codes

0 = No errors occurred during the execution of this step.

1 = One or more errors occurred.

Used By Workflows

[Provision Websphere 8 Custom Node Profile From Existing Install on page 77](#)

OS Prerequisite Check for WebSphere 8

Purpose

Checks the following:

1. Documented library requirements for WebSphere 8(see the [Prerequisites on page 16](#)).
2. File system space requirements where WebSphere 8 will be installed.
3. Temporary space requirements where the compressed software will be extracted before it is installed.

For current operating system and hardware requirements, see

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

Input Parameters for OS Prerequisite Check for WebSphere 8

Parameter Name	Default Value	Required	Description
Call Wrapper	no default	required	Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are : UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code> Windows targets: <code>jython</code> running as Administrator Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.
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.
Skip Validation	no default	optional	If true, no OS kernel level validations and library checking for Red Hat Enterprise Linux 5 will be performed.

Input Parameters for OS Prerequisite Check for WebSphere 8 (continued)

Parameter Name	Default Value	Required	Description
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.

Output Parameters

This step has no output parameters.

Return Codes

0 = No errors occurred during the execution of this step.

1 = One or more errors occurred.

Used By Workflows

- [Provision WebSphere 8 and StandAlone on page 25](#)
- [Provision WebSphere 8 and Deployment Manager on page 38](#)
- [Provision WebSphere 8 and Custom Node on page 51](#)
- [Provision Websphere 8 Standalone Profile From Existing Install on page 66](#)
- [Provision Websphere 8 Custom Node Profile From Existing Install on page 77](#)

WebSphere 8 Check File Download

Purpose

This step checks for the existence of a file on the target machine before downloading that file from the SA Core. For each file in the list, it performs the following actions:

1. Determines whether the file is in the expected location on the target machine.
2. If the file is not in the expected location, adds that file to a list of files that need to be downloaded.

Input Parameters

Parameter Name	Default Value	Required	Description
File List	no default	optional	Comma-separated list of files that need to be downloaded.

Output Parameters

Parameter Name	Description
Download List	Comma-separated list of files in the File List that were not found on the target machine.
File List	Comma-separated list of files that need to be downloaded.
Present List	Comma-separated list of files in the File List that were found on the target machine.
Target Directory	Directory name of the first file in the File List that was not found.

Return Codes

0 = No errors occurred during the execution of this step.

1 = Errors occurred while checking files.

9 = One or more files was not found.

Used By Workflows

- [Provision WebSphere 8 and StandAlone on page 25](#)
- [Provision WebSphere 8 and Deployment Manager on page 38](#)
- [Provision WebSphere 8 and Custom Node on page 51](#)
- [Provision Websphere 8 Standalone Profile From Existing Install on page 66](#)
- [Provision Websphere 8 Custom Node Profile From Existing Install on page 77](#)

WebSphere 8 Extract Archive

Purpose

This step first checks to ensure that the archive file exists. Then, based on the archive extension, extracts the archive to the specified directory.

Input Parameters

Parameter Name	Default Value	Required	Description
Call Wrapper	no default	required	Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are : UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code> Windows targets: <code>jython</code> running as Administrator Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.
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 Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.

Output Parameters

This step has no output parameters.

Return Codes

0 = Step ran successfully.

1 = Step failed.

Used By Workflows

- [Provision WebSphere 8 and StandAlone on page 25](#)
- [Provision WebSphere 8 and Deployment Manager on page 38](#)
- [Provision WebSphere 8 and Custom Node on page 51](#)

Create IBM Install Manager And WebSphere 8 Response File

Purpose

This step creates a response file for the purpose of installing a new instance of WebSphere 8.

Input Parameters

Parameter Name	Default Value	Required	Description
Call Wrapper	no default	required	Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are : UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code> Windows targets: <code>jython</code> running as Administrator Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.
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.
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.
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.

Output Parameters

This step has no output parameters.

Return Codes

0 = No errors occurred during the execution of this step.

1 = One or more errors occurred.

Used By Workflows

- [Provision WebSphere 8 and StandAlone on page 25](#)
- [Provision WebSphere 8 and Deployment Manager on page 38](#)
- [Provision WebSphere 8 and Custom Node on page 51](#)

Create WebSphere 8 Stand Alone Response File

Purpose

This step creates a new response file for the purpose of creating a stand-alone profile on top of an existing WebSphere 8 installation.

Input Parameters for Create WebSphere 8 Deployment Manager Response File

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	no default	required	Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are : UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code> Windows targets: <code>jython</code> running as Administrator Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.
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.

Input Parameters for Create WebSphere 8 Deployment Manager Response File (continued)

Parameter Name	Default Value	Required	Description
Enable Security	true	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	no default	required	Hostname or IP address of the target machine.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: <code>/opt/IBM/WebSphere/AppServer</code>
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 <code>/ \ * , ; = + ? < > & % ' " [] > # \$ ^ { }</code> . 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 <code>deployAdminConsole</code> or <code>defaultAppDeployAndConfig</code> . You may only specify one of these options.
Password	no default	required	The Windows Administrator password. Required for Windows.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: <code>CN=dmalab-example.com,OU=WAS7LabCell,OU=WAS7LabDmgrManager,O=IBM,C=US</code> The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal Cert-Validity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.

Input Parameters for Create WebSphere 8 Deployment Manager Response File (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 Path	no default	required	Fully qualified path to the profile. For example: <code>/opt/IBM/WebSphere/AppServer/profiles/AppServer1</code>
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 Cert-Validity 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.
Template Path	no default	required	Path to the profile templates in the WebSphere8 installation.
Username	no default	required	This is the Windows Administrator user. Required for Windows.

Input Parameters for Create WebSphere 8 Deployment Manager Response File (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.

Output Parameters for Create WebSphere 8 Deployment Manager Response File

Parameter Name	Description
Response File	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.

Return Codes

0 = No errors occurred during the execution of this step.

1 = One or more errors occurred.

Used By Workflows

- [Provision WebSphere 8 and StandAlone on page 25](#)
- [Provision Websphere 8 Standalone Profile From Existing Install on page 66](#)

Create WebSphere 8 Deployment Manager Response File

Purpose

This step creates a new response file for the purpose of creating a Deployment Manager profile on top of an existing WebSphere 8 installation.

Input Parameters for Create WebSphere 8 Deployment Manager Response File

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	no default	required	Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are : UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code> Windows targets: <code>jython</code> running as Administrator Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.
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.

Input Parameters for Create WebSphere 8 Deployment Manager Response File (continued)

Parameter Name	Default Value	Required	Description
Enable Security	true	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	no default	required	Hostname or IP address of the target machine.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: <code>/opt/IBM/WebSphere/AppServer</code>
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 <code>/ \ * , ; = + ? < > & % ' " [] > # \$ ^ { }</code> . 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 <code>deployAdminConsole</code> or <code>defaultAppDeployAndConfig</code> . You may only specify one of these options.
Password	no default	required	The Windows Administrator password. Required for Windows.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: <code>CN=dmalab-example.com,OU=WAS7LabCell,OU=WAS7LabDmgrManager,O=IBM,C=US</code> The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal Cert-Validity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.

Input Parameters for Create WebSphere 8 Deployment Manager Response File (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 Path	no default	required	Fully qualified path to the profile. For example: <code>/opt/IBM/WebSphere/AppServer/profiles/AppServer1</code>
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 Type	DEPLOYMENT_MANAGER	required	Required: Specifies the type of management profile. The value is DEPLOYMENT_MANAGER for a deployment manager server.
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 Cert-Validity 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.
Template Path	no default	required	Path to the profile templates in the WebSphere8 installation.

Input Parameters for Create WebSphere 8 Deployment Manager Response File (continued)

Parameter Name	Default Value	Required	Description
User-name	no default	required	This is the Windows Administrator user. Required for Windows.
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.

Output Parameters for Create WebSphere 8 Deployment Manager Response File

Parameter Name	Description
Response File	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.

Return Codes

0 = No errors occurred during the execution of this step.

1 = One or more errors occurred.

Used By Workflows

[Provision WebSphere 8 and Deployment Manager on page 38](#)

Create WebSphere 8 Custom Node Response File

Purpose

This step creates a new response file for the purpose of creating a custom profile on top of an existing WebSphere 8 installation.

Input Parameters for Create WebSphere 8 Custom Node Response File

Parameter Name	Default Value	Required	Description
Call Wrapper	no default	required	Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are : UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code> Windows targets: <code>jython</code> running as Administrator Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.
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 for Create WebSphere 8 Custom Node Response File (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	true	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 true, the new custom node will be federated during profile creation. If false, you must federate it later by using the addNode command.
Host Name	no default	required	Hostname or IP address of the target machine.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: <code>/opt/IBM/WebSphere/AppServer</code>
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 <code>/ \ * , : ; = + ? < > & % ' " [] > # \$ ^ { }</code> . 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: <code>CN=dmalab-example.com,OU=WAS7LabCell,OU=WAS7LabDmgrManager,O=IBM,C=US</code> The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal Cert-Validity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.

Input Parameters for Create WebSphere 8 Custom Node Response File (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 Path	no default	required	Fully qualified path to the profile. For example: /opt/IBM/WebSphere/AppServer/profiles/AppServer1
Profile Type	no default	required	Because this workflow creates a Custom Node profile, the value must be custom.
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=dmlab-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 Cert-Validity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.
Template Path	no default	required	Path to the profile templates in the WebSphere8 installation.

Output Parameters for Create WebSphere 8 Custom Node Response File

Parameter Name	Description
Response File	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.

Return Codes

0 = No errors occurred during the execution of this step.

1 = One or more errors occurred.

Used By Workflows

- [Provision Websphere 8 Custom Node Profile From Existing Install on page 77](#)
- [Provision WebSphere 8 and Custom Node on page 51](#)

WebSphere 8 Existing Install Create Custom Node Response File

Purpose

This step creates a new response file for the purpose of creating a Custom Node profile on top of an existing WebSphere 8 installation.

Input Parameters for WebSphere 8 Existing Install Create Custom Node Response File

Parameter Name	Default Value	Required	Description
Call Wrapper	no default	required	Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are : UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code> Windows targets: <code>jython</code> running as Administrator Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.
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 for WebSphere 8 Existing Install Create Custom Node Response File (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	true	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	no default	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.
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.
Password	no default	required	The Windows Administrator password. Required for Windows.
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.
Personal Cert-Validity 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.

Input Parameters for WebSphere 8 Existing Install Create Custom Node Response File (continued)

Parameter Name	Default Value	Required	Description
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 Path	no default	required	Fully qualified path to the profile. For example: /opt/IBM/WebSphere/AppServer/profiles/AppServer1
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.
Signing Cert-Validity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.
Template Path	no default	required	Path to the profile templates in the WebSphere8 installation.
Username	no default	required	This is the Windows Administrator user. Required for Windows.

Output Parameters for WebSphere 8 Existing Install Create Custom Node Response File

Parameter Name	Description
Response File	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.

Return Codes

0 = No errors occurred during the execution of this step.

1 = One or more errors occurred.

Used By Workflows

[Provision Websphere 8 Custom Node Profile From Existing Install on page 77](#)

Install IBM Install Manager And WebSphere 8

Purpose

This step installs a new instance of WebSphere 8.

Input Parameters

Parameter Name	Default Value	Required	Description
Call Wrapper	no default	required	Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are : UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code> Windows targets: <code>jython</code> running as Administrator Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.
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.
Password	no default	required	The Windows Administrator password. Required for Windows.
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.
Username	no default	required	This is the Windows Administrator user. Required for Windows.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.

Output Parameters

This step has no output parameters.

Return Codes

0 = No errors occurred during the execution of this step.

1 = One or more errors occurred.

Used By Workflows

- [Provision WebSphere 8 and StandAlone on page 25](#)
- [Provision WebSphere 8 and Deployment Manager on page 38](#)
- [Provision WebSphere 8 and Custom Node on page 51](#)

Create WebSphere 8 Profile

Purpose

This step creates a profile on top of an existing WebSphere 8 installation..

Input Parameters for Create WebSphere 8 Profile

Parameter Name	Default Value	Required	Description
Call Wrapper	no default	required	Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are : UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code> Windows targets: <code>jython</code> running as Administrator Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: <code>/opt/IBM/WebSphere/AppServer</code>
Node Name	no default	required	Unique node name that cannot contain any of the following special characters <code>/ \ * , ; ; = + ? < > & % ' " [] > # \$ ^ { }</code> . If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Password	no default	required	The Windows Administrator password. Required for Windows.
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 Type	no default	required	Because this workflow creates a Custom Node profile, the value must be custom.
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.
Username	no default	required	This is the Windows Administrator user. Required for Windows.

Output Parameters

This step has no output parameters.

Return Codes

0 = No errors occurred during the execution of this step.

1 = One or more errors occurred.

Used By Workflows

- [Provision WebSphere 8 and StandAlone on page 25](#)
- [Provision WebSphere 8 and Deployment Manager on page 38](#)
- [Provision WebSphere 8 and Custom Node on page 51](#)
- [Provision Websphere 8 Standalone Profile From Existing Install on page 66](#)
- [Provision Websphere 8 Custom Node Profile From Existing Install on page 77](#)

WebSphere 8 StandAlone Start Server

Purpose

This step starts the stand-alone application server.

Input Parameters

Parameter Name	Default Value	Required	Description
Call Wrapper	no default	required	Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are : UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code> Windows targets: <code>jython</code> running as Administrator Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.
Profile Path	no default	required	Fully qualified path to the profile. For example: <code>/opt/IBM/WebSphere/AppServer/profiles/AppServer1</code>
Server Name	no default	required	Name of the application server that was created under the profile.

Output Parameters

This step has no output parameters.

Return Codes

0 = No errors occurred during the execution of this step.

1 = One or more errors occurred.

Used By Workflows

- [Provision WebSphere 8 and StandAlone on page 25](#)
- [Provision Websphere 8 Standalone Profile From Existing Install on page 66](#)

WebSphere 8 Deployment Manager Start Server

Purpose

This step starts the Deployment Profile application server.

Input Parameters

Parameter Name	Default Value	Required	Description
Call Wrapper	no default	required	Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are : UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code> Windows targets: <code>jython</code> running as Administrator Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.
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 Type	management	required	Because this workflow creates a Deployment Manager profile, the value must be management.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.

Output Parameters

This step has no output parameters.

Return Codes

0 = No errors occurred during the execution of this step.

1 = One or more errors occurred.

Used By Workflows

[Provision WebSphere 8 and Deployment Manager on page 38](#)

WebSphere 8 Cleanup Downloaded Files

Purpose

This step removes all downloaded files and archives. It must run as the owner of the pertinent files and directories.

Input Parameters

Parameter Name	Default Value	Required	Description
Call Wrapper	no default	required	Name of the interpreter specified in the command that will execute each step as a specific user. Defaults are : UNIX targets: <code>sudo -u root /opt/opsware/dma/jython/jython.sh</code> Windows targets: <code>jython</code> running as Administrator Note that these examples pertain to an HP Server Automation 9.x environment, where both the default user and the user who initiates the call wrapper is root. In HP DMA (6.0.x) environments, the user who is running the DMA process initiates the call wrapper.
Do Not Remove List	no default	optional	List of directories that should not be removed.
Download File List	no default	optional	List of files that were downloaded.
Extract Location One	no default	optional	Location where the installation binaries were extracted.
Extract Location Two	no default	optional	Second location (if any) where files were extracted.
File List	no default	optional	Comma-separated list of files that need to be removed.

Output Parameters

This step has no output parameters.

Return Codes

0 = No errors occurred during the execution of this step.

1 = One or more errors occurred.

Used By Workflows

- [Provision WebSphere 8 and StandAlone on page 25](#)
- [Provision WebSphere 8 and Deployment Manager on page 38](#)
- [Provision WebSphere 8 and Custom Node on page 51](#)
- [Provision Websphere 8 Standalone Profile From Existing Install on page 66](#)
- [Provision Websphere 8 Custom Node Profile From Existing Install on page 77](#)

Discover WebSphere

Purpose

This step audits the target server's physical environment looking for WebSphere 8 cells, clusters, and managed servers associated with the Known Profile Roots that you specify. When any of these items is found, it is added to HP DMA environment.

Note: The discovery process is ONLY additive. It will not remove instances or databases that currently exist in your HP DMA environment. It is your responsibility to delete items that are no longer in use.

Note: WebSphere discovery is currently supported on Linux and AIX platforms.

Input Parameters

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:4433/dma</code>
Web Service User	administrator	required	User capable of modifying the managed environment through the discovery web service API.

Optional Custom Field Inputs

Custom Field Name	Example Value	Required	Description
Server.Become Routine	sudo, su, or ssh	optional	Routine used to switch users on unix machines.

Output Parameters

This step has no output parameters.

Return Codes

0 = No errors occurred during the execution of this step.

-1, 1, 2 = One or more errors occurred.

Used By Workflows

- [Provision WebSphere 8 and StandAlone on page 25](#)
- [Provision WebSphere 8 and Deployment Manager on page 38](#)
- [Provision WebSphere 8 and Custom Node on page 51](#)
- [Provision Websphere 8 Standalone Profile From Existing Install on page 66](#)
- [Provision Websphere 8 Custom Node Profile From Existing Install on page 77](#)

Chapter 11

Other Reference Information

The following topics provide additional information pertinent to the workflows in this solution pack:

- [WebSphere 8 Product Documentation below](#)
- [Using this Solution Pack With HP Server Automation below](#)

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/webservers/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>

Using this Solution Pack With HP Server Automation

HP Database and Middleware Automation (HP DMA) version 1.00 is compatible with HP Server Automation version 9.02 (and later 9.0x versions).

For information about running HP DMA workflows from HP Server Automation versions prior to 9.10, refer to the following documents:

- *HP Server Automation Application Deployment User Guide* (version 9.02 and later 9.0x versions)
- *HP Database and Middleware Automation User Guide* (version 1.00)

HP Database and Middleware Automation version 9.10 is compatible with HP Server Automation version 9.10 (and later).

For information about running HP Database and Middleware Automation workflows from HP Server Automation version 9.10 (and later), refer to the following documents:

- *User Guide: Application Deployment Manager*
- *User Guide: Database and Middleware Automation User Guide*

These guides are included in the HP Server Automation documentation library (version 9.10 and later).

Chapter 12

Tips and Best Practices

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

[Using a Policy to Specify Parameter Values below](#)

Using 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:

- Passwords are obfuscated (not displayed in clear text).
- The policy can be used in any deployment.
- It is faster and less error-prone than specifying parameter values manually.

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](#).

If you are using HP Server Automation, see the *User Guide: Database and Middleware Automation*. This guide is included in the HP Server Automation documentation library (SA version 9.10 and later).

If you are using HP DMA 1.00, see "Policies" in the *HP Database and Middleware Automation User Guide* for more information.

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-delimited list of values (or a large amount of text not suitable for a Text attribute).
 - A Password attribute contains simple text, but it is obfuscated 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.

Note: Extracted policies only use Text type attributes. Therefore, passwords are not obfuscated when you specify them in an extracted policy. You can, however, delete an automatically extracted attribute and then add a new one of type Password.

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 *User Guide: Database and Middleware Automation* for details. This guide is included in the HP Server Automation documentation library (SA version 9.10 and later).

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 text box to the right of the parameter name, type the first few characters of the policy name.

A drop-down list of policy attributes appears.
 - b. From the drop-down list, select the attribute that you want to reference.
3. Click **Save** to save your changes to the deployment.

Chapter 13

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 Server Automation on next page](#)

For additional information, refer to the “Troubleshooting” chapter in the *HP Server Automation User Guide: Database and Middleware Automation*.

If you are using HP Database and Middleware Automation version 1.00, see the *HP Database and Middleware Automation Installation Guide*.

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 (Read or Write) permissions for organizations, workflows, steps, policies, and deployments. Deployments have an extra permission: Execute. Users are assigned to roles, and they gain access to these items according to the permissions defined for their roles.

Note: The following information pertains only to HP DMA 1.00:

Roles can be defined in one of two ways: native or LDAP groups.

- Native roles define groups of HP DMA users in the repository.
- LDAP groups are retrieved from the LDAP server configured in the Setup > Expert Engine area. No user information is stored in the repository for LDAP groups. This allows you to use your corporate directory for defining users and their permissions making security audits easier.

Roles are assigned on the Roles tab of the Setup page. See “Roles” in the *HP Database and Middleware Automation User Guide* (version 1.00) for more information.

Make sure that the HP DMA users in your environment are assigned roles that grant them the permissions they need to accomplish their tasks. For example:

- To view a workflow, your role must have Read permission for that workflow.
- To view a deployment, your role must have Read permission for that deployment.

- To edit a workflow, your role must have Write permission for that workflow.
- To run a deployment, your role must have Execute permission for that deployment.

Permissions determine what features and functions are available and active in the HP DMA UI. For a detailed breakdown, see the HP Database and Middleware Automation *User Guide*.

Note: In HP Server Automation, roles and permissions work differently. Both roles and permissions are assigned by the SA administrator. See the HP Server Automation *Administration Guide* and the *User Guide: Database and Middleware Automation* for more information. Both guides are included in the HP Server Automation documentation library (SA version 9.10 and later).

Discovery in HP Server Automation

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

In HP DMA version 1.00, discovery is automatically activated when an agent is started on a target machine.

In HP Server Automation, you must explicitly initiate the process of discovery—it is not automatic. Refer to the *User Guide: Database and Middleware Automation* for instructions. This guide is included in the SA documentation library (version 9.10 and later).

Glossary

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 Server Automation version 9.11 (and later).

C

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.

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.

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.

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.

S

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.