HP Database and Middleware Automation

For Linux, Solaris, AIX, and Windows

Software Version: 10.20

WebSphere 8.0 and 8.5.x Provisioning

User Guide

Document Release Date: December 2013

Software Release Date: December 2013

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

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

UNIX® is a registered trademark of The Open Group.

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

Documentation Updates

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

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

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

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

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

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

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

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

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

Document Changes

Chapter	Version	Changes
Workflow Details	10.00	Synchronized parameter information to the DMA user interface. Made cosmetic and consistency changes.
Title Page Legal Notices	10.01	Updated version number, software release date, document release date, and copyright date range.
WebSphere 8 Provisioning Quick Start	10.01	Updated from 10.00 to 10.01.
Title Page Legal Notices	10.10	Updated version number, software release date, document release date, and copyright date range.
About HP DMA Solution Packs	10.10	Added overview topic: About HP DMA Solution Packs.
Workflow Details	10.10	Added new Provision IBM HTTP Server and Plug-in workflow.
Title Page Legal Notices	10.20	Updated version number, software release date, document release date, and copyright date range.

Document Changes (continued)

Chapter	Version	Changes
WebSphere 8 Provisioning Quick Start Workflow Details	10.20	Removed Quick Start chapter. In the "How to Run this Workflow" topics, pointed to the*HP DMA Quick Start Tutorial*.
Entire guide Workflow Details	10.20	Added support for WebSphere 8.5 and 8.5.5. Deprecated workflows and steps that are specific to WebSphere 8. Documented new workflows and steps that support WebSphere 8.0 and 8.5.x.

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

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, and 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.

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 versions 8.0, 8.5, and 8.5.5 (WebSphere 8.0 and 8.5.x).

To use this solution, you should be familiar with WebSphere 8.0 or 8.5.x and its requirements (see links to the WebSphere 8.0 and 8.5.x Product Documentation on page 128).

Document Map

The following table shows you how to navigate this guide:

Topic	Description
The WebSphere Provisioning Solution	General information about this solution, including what it contains and what it does.
Workflow Details	Information about the WebSphere 8.0 and 8.5.x workflows included in this solution, including: prerequisites, how it works, how to run it, sample scenarios, and a list of input parameters.
Reference Information	Links to current WebSphere 8.0 and 8.5.x product documentation and additional HP DMA documentation.
Tips and Best Practices	Simple procedures that you can use to accomplish a variety of common HP DMA tasks.
Troubleshooting	Tips for solving common problems.

Important Terms

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

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

  If you provide correct values for the input parameters that each scenario requires, the workflow will be able to accomplish its objective. Output parameters from one step often serve as input parameters to another step.
- A **solution pack** contains a collection of related workflows and the steps, functions, and policies that implement each workflow.

  More precisely, solution packs contain **workflow templates**. These are read-only versions of the workflows that cannot be deployed. To run a workflow included in a solution pack, you must first create a deployable copy of the workflow template and then customize that copy for your environment.
- A **deployment** associates a workflow with the targets (servers, instances, or databases) where the workflow will run. To run a workflow, you execute a specific deployment. A deployment is associated with one workflow; a workflow can have many deployments, each with its own targets and parameter settings.
- The umbrella term **automation items** is used to refer to those items to which role-based permissions can be assigned. Automation items include workflows, deployments, steps, and policies.

  Organizations also have role-based permissions. Servers, instances, and databases inherit their role-based permissions from the organization in which the server resides.
- The **software repository** contains any files that a workflow might need to carry out its purpose (for example, software binaries or patch archives). If the files that a workflow requires are not in the software repository, they must be stored locally on each target server.

  When you are using HP DMA with HP Server Automation (HP SA), the software repository is the HP SA Software Library.
- An **organization** is a logical grouping of servers. You can use organizations to separate development, staging, and production resources—or to separate logical business units. Because user security for running workflows is defined at the organization level, organizations should be composed with user security in mind.

Additional terms are defined in the Glossary on page 141.

Chapter 1

The WebSphere Provisioning Solution

The WebSphereprovisioning solution provides tools that you can use to provision many features of a WebSphere 8.0 or 8.5.x environment.

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

- Installing IBM Installation Manager
- Installing IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x (WebSphere 8.0 or 8.5.x)
- Creating stand-alone or custom node profiles for new or existing WebSphere 8.0 or 8.5.x installations
- Installing the IBM HTTP Server for WebSphere Application Server version 8.0 or 8.5.x and plug-in

By consistently using the tools provided in this solution, you can quickly, efficiently, and accurately set up your WebSphere 8.0 or 8.5.x environment. You maintain flexibility over the architecture by configuring environment-specific information through the input parameters.

What this Solution Includes

The Application Server Provisioning solution pack contains the following WebSphere 8.0 and 8.5.xprovisioning workflows:

Workflow Name	Purpose
Provision WebSphere and Stand-Alone	Use this workflow to install the WebSphere 8.0 or 8.5.x 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 and Deployment Manager	Use this workflow to install a new instance of the IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x and Installation Manager, and then 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 and Custom Node	Use this workflow to install the WebSphere 8.0 or 8.5.x 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 Stand-Alone Profile From Existing Install	Use this workflow to create a stand-alone profile on an existing WebSphere 8.0 or 8.5.x 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 Custom Node Profile From Existing Install	Use this workflow to create a custom profile on an existing WebSphere 8.0 or 8.5.x 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.
Provision IBM HTTP Server and Plug-in	Use this workflow to install IBM HTTP Server for WebSphere Application Server version 8.0 or 8.5.x and the plug-in on a target system and then to configure a Web server instance along with the plug-in on the same target system. IBM HTTP Server version 8.0 or 8.5.x is a Web server that will serve both static and dynamic content. Usually you will front your WebSphere Application Server environment with an IBM HTTP Server.

Deprecated WebSphere 8 Provisioning Workflows

The following workflows that are specifically for WebSphere 8 have been deprecated from the solution pack and removed from the product:

Workflow Name	Purpose
Provision WebSphere 8 and StandAlone	Use this workflow to install the WebSphere 8 Base core binaries and, optionally, create a stand-alone profile. This workflow has been replaced by the Provision WebSphere and Stand-Alone workflow that supports both WebSphere 8.0 and 8.5.x.
Provision WebSphere 8 and Deployment Manager	Use this workflow to install the WebSphere 8 Base core binaries and, optionally, create a deployment manager profile. This workflow has been replaced by the Provision WebSphere and Deployment Manager workflow that supports both WebSphere 8.0 and 8.5.x.
Provision WebSphere 8 and Custom Node	Use this workflow to install the WebSphere 8 Base core binaries and, optionally, create a custom profile. This workflow has been replaced by the Provision WebSphere and Custom Node workflow that supports both WebSphere 8.0 and 8.5.x.
Provision Websphere 8 Standalone Profile From Existing Install	Use this workflow to create a stand-alone profile on an existing WebSphere 8 installation. This workflow has been replaced by the Provision WebSphere Stand-Alone Profile From Existing Install workflow that supports both WebSphere 8.0 and 8.5.x.
Provision Websphere 8 Custom Node Profile From Existing Install	Use this workflow to create a custom profile on an existing WebSphere 8 installation. This workflow has been replaced by the Provision WebSphere Custom Node Profile From Existing Install workflow that supports both WebSphere 8.0 and 8.5.x.
Provision IBM HTTP Server 8 and Plug-In	Use this workflow to install IBM HTTP Server for WebSphere Application Server V8.0 and the plug-in on a target system and then to configure a Web server instance along with the plug-in on the same target system. This workflow has been replaced by the Provision IBM HTTP Server and Plug-in workflow that supports both WebSphere 8.0 and 8.5.x.

Tip: Documentation for deprecated workflows is available in the *HP DMA WebSphere 8 Provisioning User Guide* for HP DMA version 10.10. This document is available on the HP Software Product Manuals web site: http://h20230.www2.hp.com/selfsolve/manuals

Supported Products and Platforms

WebSphere Versions

The WebSphere provisioning workflows documented in this guide support the following versions of WebSphere: 8.0, 8.5, and 8.5.5. These versions will be referred to as WebSphere 8.0 and 8.5.x throughout.

Operating Systems

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

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

Hardware Requirements

For HP DMA server hardware requirements, see the *HP DMA Installation Guide* and the *HP DMA Release Notes*.

HP Software Requirements

This solution requires HP DMA version 10.20 (or later).

Prerequisites

The following prerequisites must be satisfied before you can run the WebSphere 8.0 and 8.5.x provisioning workflows in this solution pack:

Per the IBM WebSphere 8.0 and 8.5.x documentation, the following system libraries are required before provisioning IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x on 64-bit and 32-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 gtk2-2.10.4-29.el5 gtk2-engines-2.8.0-3.el5 ksh-20080202-14 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libstdc++-4.1.2-48 libXft-2.1.10-1.1 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5

Platform	Required Library
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 elfutils-0.148-1 elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 libstdc++-4.4.4-13 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 libXft-2.1.13-4.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5

Make sure that these libraries exist on each target server before running the WebSphere 8.0 and 8.5.x provisioning workflows. If newer versions of these libraries are available, you can install the newer versions.

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

Chapter 2

Workflow Details

The Application Server Provisioning solution pack contains the following WebSphere 8.0 and 8.5.xprovisioning workflows. You can run these workflows ad-hoc for custom WebSphere 8.0 and 8.5.x installations or create reusable deployments to standardize WebSphere 8.0 and 8.5.x installations in your environment.

Workflow Name	Purpose
Provision WebSphere and Stand-Alone	Use this workflow to install the WebSphere 8.0 or 8.5.x 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 and Deployment Manager	Use this workflow to install a new instance of the IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x and Installation Manager, and then 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 and Custom Node	Use this workflow to install the WebSphere 8.0 or 8.5.x 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 Stand-Alone Profile From Existing Install	Use this workflow to create a stand-alone profile on an existing WebSphere 8.0 or 8.5.x 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 Custom Node Profile From Existing Install	Use this workflow to create a custom profile on an existing WebSphere 8.0 or 8.5.x 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.

Workflow Name	Purpose
Provision IBM HTTP Server and Plug-in	Use this workflow to install IBM HTTP Server for WebSphere Application Server version 8.0 or 8.5.x and the plug-in on a target system and then to configure a Web server instance along with the plug-in on the same target system. IBM HTTP Server version 8.0 or 8.5.x is a Web server that will serve both static and dynamic content. Usually you will front your WebSphere Application Server environment with an IBM HTTP Server.

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

There are two steps required to customize this solution:

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

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

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

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

The information presented here assumes the following:

- HP DMA is installed and operational.
- At least one suitable target server is available (see Supported Products and Platforms on page 16).
- You are logged in to the HP DMA web interface.
- You have permission to create, edit, and deploy copies of the workflows included in this solution pack.

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

Provision WebSphere and Stand-Alone

Use this workflow to install the WebSphere 8.0 or 8.5.x Base core binaries and, optionally, create a stand-alone profile.

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

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

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

Note: The documentation for this workflow contains steps that are referred to by their base names. The names in the HP DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere and Stand-Alone 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 8.0 and 8.5.x documentation, the following system libraries are required before provisioning IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x on 64-bit and 32-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 gtk2-2.10.4-29.el5 gtk2-engines-2.8.0-3.el5 ksh-20080202-14 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libstdc++-4.1.2-48 libXft-2.1.10-1.1 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5

Platform	Required Library
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 elfutils-0.148-1 elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 libstdc++-4.4.4-13 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 libXft-2.1.13-4.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5

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 8.0 and 8.5.x, refer to the WebSphere 8.0 and 8.5.x Product Documentation on page 128.

How this Workflow Works

This topic contains the following information about the Provision WebSphere and Stand-Alone 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 8.0 or 8.5.x
3. Creates a stand-alone profile

The workflow checks to see if the WebSphere 8.0 or 8.5.x binary archive files exist on the target machine. If they do not, the files are downloaded from the software repository (for more information, see How to Import a File into the Software Repository on page 138).

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 8.0 and 8.5.x are installed.

Validation Checks Performed

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

The workflow first performs the following parameter checks:

1. Required parameters have values specified.
2. WebSphere specific names do not contain the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
3. Parameters do not contain illegal characters for the parameter type.
4. Flag parameters are set to true or false.
5. Integer parameters are set to appropriate integer values.
6. Mutually dependent parameters are specified appropriately as a set.
7. Parameters are set to one of the values if the parameter has a list of valid values.
8. License Acceptance is true (for workflows that input the License Acceptance parameter).
9. All specified file names are legal file names.
10. All specified locations are legal path names. If they do not exist they will be created.

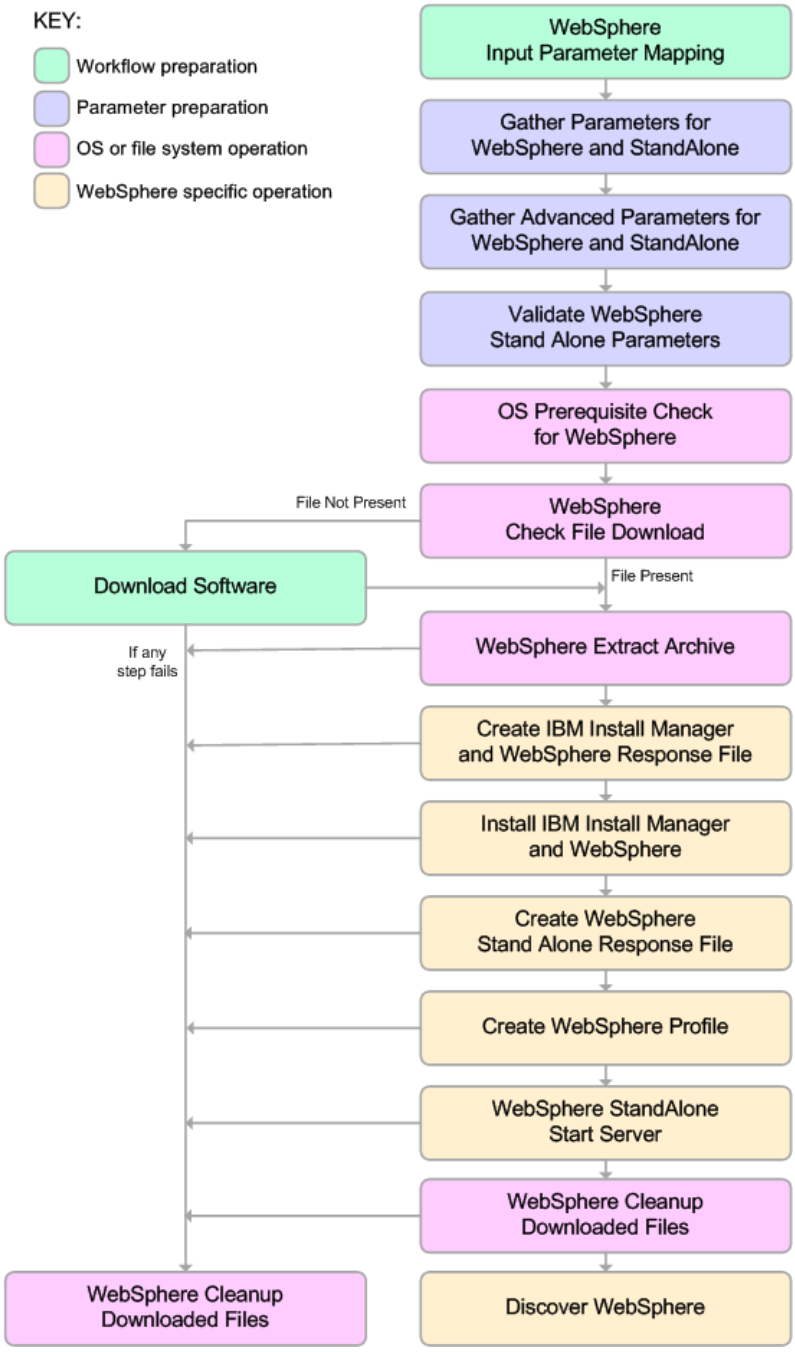
Note: For more information about valid parameter values, see Parameters for Provision WebSphere and Stand-Alone.

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 22).
2. Sufficient disk space is available to install WebSphere 8.0 or 8.5.x.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

The Provision WebSphere and Stand-Alone 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. Gathers and validates the parameters needed to install WebSphere 8.0 or 8.5.x and create a stand-alone profile (see Validation Checks Performed on page 25).
3. Checks the following:
   a. Documented library requirements for WebSphere 8.0 and 8.5.x (see the Prerequisites for this Workflow on page 22).
   b. File system space requirements where WebSphere 8.0 or 8.5.x will be installed.
   c. Temporary space requirements where the compressed software will be extracted before it is installed.
4. Determines whether the WebSphere 8.0 or 8.5.x binary archive is present on the target machine. If the archive is not present, the workflow downloads it from the software repository (see How to Import a File into the Software Repository on page 138).
5. Extracts the WebSphere 8.0 or 8.5.x binary archive to the specified directory.
6. Creates a response file for the purpose of installing a new instance of WebSphere 8.0 or 8.5.x.
7. Installs the IBM Installation Manager and a new WebSphere 8.0 or 8.5.x 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 8.0 or 8.5.x installation.
9. Creates a stand-alone profile on top of the WebSphere 8.0 or 8.5.x installation.
10. Starts the new stand-alone WebSphere 8.0 or 8.5.x application server.
11. Cleans up any files that were downloaded—for either workflow success or failure.

    Note: The parameters Cleanup on Success and Cleanup on Failure are defaulted to True. If they are set to False, the downloaded files are not cleaned up.

12. Discovers any WebSphere 8.0 or 8.5.x 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 and Stand-Alone workflow in your environment.

Tip: For detailed instructions to run HP DMA workflows—using the Run Oracle Compliance Audit workflow as an example—see *HP DMA Quick Start Tutorial*.

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 and Stand-Alone.

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 and Stand-Alone workflow:

1. Create a deployable copy of the workflow (see "Create a Deployable Workflow" in *HP DMA Quick Start Tutorial*).
2. Determine the values that you will specify for the following parameters:

   Parameters Defined in this Step: Gather Parameters for WebSphere and StandAlone

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

Parameters Defined in this Step: Gather Parameters for WebSphere and Stand-Alone (continued)

Parameter Name	Default Value	Required	Description
Install Manager Binary Download Location	`/opt/IBM/iim`	required	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For example: `/opt/IBM/iim`
Install Manager Binary Files	no default	required	Name of the compressed Install Manager software package.
Install Manager Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as WebSphere Extract Location.
Install Manager Install Location	no default	required	Fully qualified path where Install Manager will be installed. For example: `/opt/IBM/InstallManager`
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.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.

Parameters Defined in this Step: Gather Parameters for WebSphere and Stand-Alone (continued)

Parameter Name	Default Value	Required	Description
WebSphere Binary Download Location	`/opt/IBM/WAS`	required	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Files	no default	required	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
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.

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

See Parameters for Provision WebSphere and Stand-Alone for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see How to Use a Policy to Specify Parameter Values on page 135).

3. In the workflow editor, expose any additional parameters that you need (see How to Expose Additional Workflow Parameters on page 134). 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" in *HP DMA Quick Start Tutorial* 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" in *HP DMA Quick Start Tutorial* for instructions).

To verify the results:

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

Be sure to also perform the following steps:

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

   WAS_ROOT/bin/versionInfo.sh

   Here, *WAS_ROOT* is the directory where WebSphere 8.0 or 8.5.x 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 8.0 or 8.5.x 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 and Stand-Alone workflow.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see How to Use a Policy to Specify Parameter Values on page 135).

New Install with Stand-Alone Profile – Parameter Value Examples

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

New Install with Stand-Alone Profile – Parameter Value Examples (continued)

Parameter Name	Example Value	Description
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	DevNode	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	standAlone	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Server Name	Server1	Name of the application server that will be created under the profile.
Web Service Password	myWebSvcPwd	Password for the discovery web service API.
Web Service User	JohnDoe	User capable of modifying the managed environment through the discovery web service API.
WebSphere Binary Download Location	/opt/IBM/was	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Files	WAS_V8.0_disk1.zip, WAS_V8.0_disk2.zip	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	/opt/IBM/was	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
WebSphere Install Location	/opt/IBM/ WebSphere/AppServer	Fully qualified path where WebSphere will be installed.

Parameters for Provision WebSphere and Stand-Alone

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 134). For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Input Parameters Defined in this Step: Gather Parameters for WebSphere and StandAlone

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

Input Parameters Defined in this Step: Gather Parameters for WebSphere and StandAlone (continued)

Parameter Name	Default Value	Required	Description
Install Manager Binary Download Location	`/opt/IBM/iim`	required	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For example: `/opt/IBM/iim`
Install Manager Binary Files	no default	required	Name of the compressed Install Manager software package.
Install Manager Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as WebSphere Extract Location.
Install Manager Install Location	no default	required	Fully qualified path where Install Manager will be installed. For example: `/opt/IBM/InstallManager`
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.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.

Input Parameters Defined in this Step: Gather Parameters for WebSphere and StandAlone (continued)

Parameter Name	Default Value	Required	Description
WebSphere Binary Download Location	`/opt/IBM/WAS`	required	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Files	no default	required	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
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.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere and StandAlone

Parameter Name	Default Value	Required	Description
Cleanup on Failure	True	optional	Indicates whether to remove downloaded and extracted files and to clean up the installation directory in the event of workflow failure. Valid values are True and False. The default is True, which will clean up on failure.
Cleanup on Success	True	optional	Indicates whether to remove downloaded and extracted files and to clean up the installation directory in the event of workflow success. Valid values are True and False. The default is True, which will clean up on success.
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.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere and StandAlone (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.
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.
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 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.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere and StandAlone (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.
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.

Provision WebSphere and Deployment Manager

Use this workflow to install a new instance of the IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x and Installation Manager, and then create a deployment manager profile.

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

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

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

Note: The documentation for this workflow contains steps that are referred to by their base names. The names in the HP DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

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

1. This workflow requires unchallenged `sudo` access to a user (typically root) who can access all required files and directories.
2. Per the IBM WebSphere 8.0 and 8.5.x documentation, the following system libraries are required before provisioning IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x on 64-bit and 32-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 gtk2-2.10.4-29.el5 gtk2-engines-2.8.0-3.el5 ksh-20080202-14 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libstdc++-4.1.2-48 libXft-2.1.10-1.1 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5

Platform	Required Library
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 elfutils-0.148-1 elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 libstdc++-4.4.4-13 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 libXft-2.1.13-4.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5

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 8.0 and 8.5.x, refer to the WebSphere 8.0 and 8.5.x Product Documentation on page 128.

How this Workflow Works

This topic contains the following information about the Provision WebSphere 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 8.0 or 8.5.x
3. Creates a Deployment Manager profile

The workflow checks to see if the WebSphere 8.0 or 8.5.x binary archive files exist on the target machine. If they do not, the files are downloaded from the software repository (for more information, see How to Import a File into the Software Repository on page 138).

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 8.0 and 8.5.x are installed.

Validation Checks Performed

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

The workflow first performs the following parameter checks:

1. Required parameters have values specified.
2. WebSphere specific names do not contain the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
3. Parameters do not contain illegal characters for the parameter type.
4. Flag parameters are set to true or false.
5. Integer parameters are set to appropriate integer values.
6. Mutually dependent parameters are specified appropriately as a set.
7. Parameters are set to one of the values if the parameter has a list of valid values.
8. License Acceptance is true (for workflows that input the License Acceptance parameter).
9. All specified file names are legal file names.
10. All specified locations are legal path names. If they do not exist they will be created.

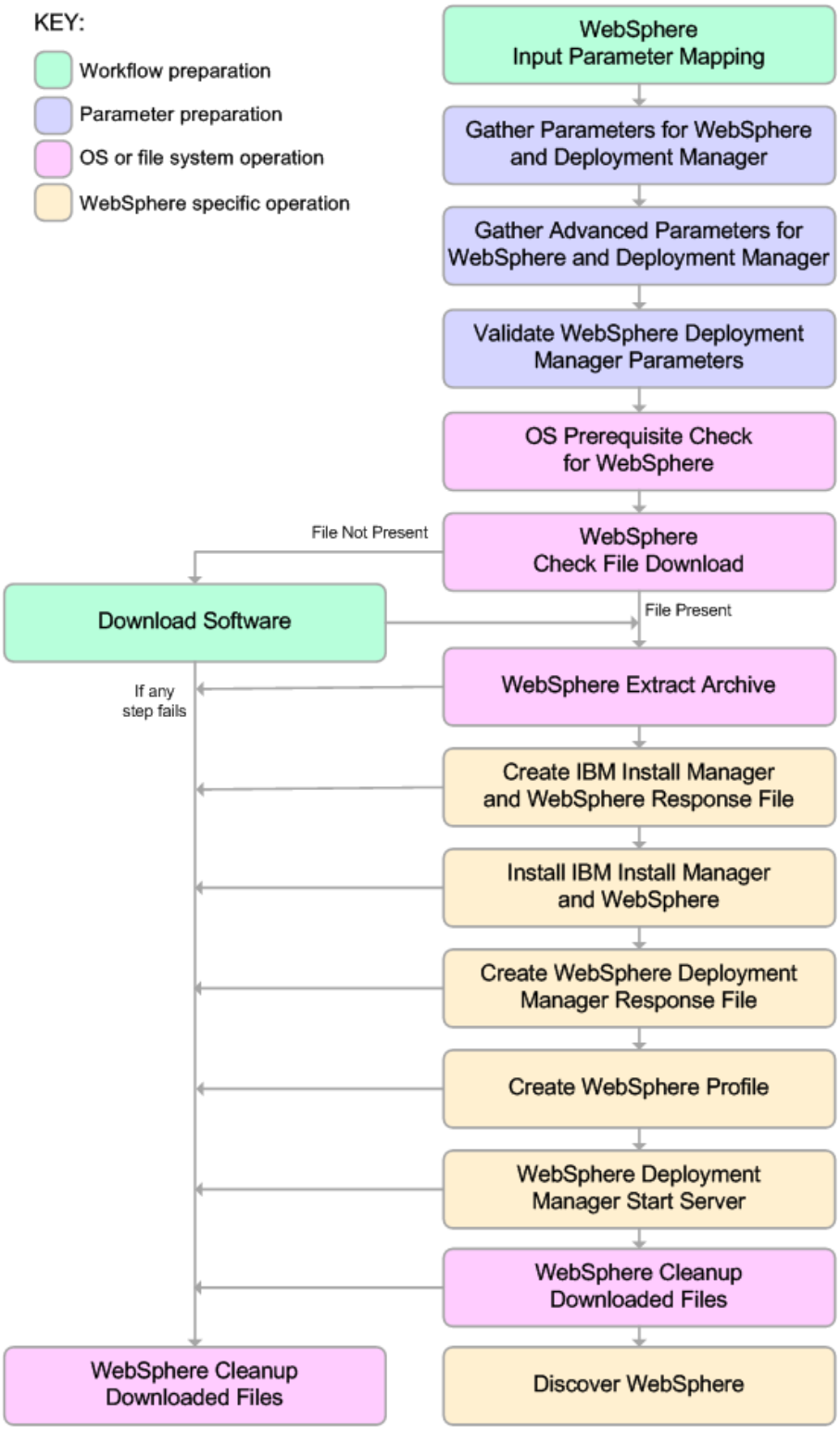
Note: For more information about valid parameter values, see Parameters for Provision WebSphere and Deployment Manager.

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

1. All required libraries are present (see Prerequisites for this Workflow).
2. Sufficient disk space is available to install WebSphere 8.0 or 8.5.x.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

The Provision WebSphere 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. Gathers and validates the parameters needed to install WebSphere 8.0 or 8.5.x and create a Deployment Manager profile (see Validation Checks Performed on page 43).
3. Checks the following:
   a. Documented library requirements for WebSphere 8.0 and 8.5.x (see the Prerequisites for this Workflow).
   b. File system space requirements where WebSphere 8.0 or 8.5.x will be installed.
   c. Temporary space requirements where the compressed software will be extracted before it is installed.
4. Determines whether the WebSphere 8.0 or 8.5.x binary archive is present on the target machine. If the archive is not present, the workflow downloads it from the software repository (see How to Import a File into the Software Repository on page 138).
5. Extracts the WebSphere 8.0 or 8.5.x binary archive to the specified directory.
6. Creates a response file for the purpose of installing a new instance of WebSphere 8.0 or 8.5.x.
7. Installs the IBM Installation Manager and a new WebSphere 8.0 or 8.5.x 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 8.0 or 8.5.x installation.
9. Creates a Deployment Manager profile on top of the WebSphere 8.0 or 8.5.x installation.
10. Starts the new Deployment Manager WebSphere 8.0 or 8.5.x application server.
11. Cleans up any files that were downloaded—for either workflow success or failure.

    Note: The parameters Cleanup on Success and Cleanup on Failure are defaulted to True. If they are set to False, the downloaded files are not cleaned up.

12. Discovers any WebSphere 8.0 or 8.5.x 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 and Deployment Manager workflow in your environment.

Tip: For detailed instructions to run HP DMA workflows—using the Run Oracle Compliance Audit workflow as an example—see *HP DMA Quick Start Tutorial*.

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 and Deployment Manager.

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 and Deployment Manager workflow:

1. Create a deployable copy of the workflow (see "Create a Deployable Workflow" in *HP DMA Quick Start Tutorial*).
2. Determine the values that you will specify for the following parameters:

   Parameters Defined in this Step: Gather Parameters for WebSphere and Deployment Manager

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.

Parameters Defined in this Step: Gather Parameters for WebSphere and Deployment Manager (continued)

Parameter Name	Default Value	Required	Description
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Install Manager Binary Download Location	`/opt/IBM/iim`	required	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For example: `/opt/IBM/iim`
Install Manager Binary Files	no default	required	Name of the compressed Install Manager software package.
Install Manager Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as WebSphere Extract Location.
Install Manager Install Location	no default	required	Fully qualified path where Install Manager will be installed. For example: `/opt/IBM/InstallManager`
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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Web Service Password	no default	required	Password for the discovery web service API.

Parameters Defined in this Step: Gather Parameters for WebSphere and Deployment Manager (continued)

Parameter Name	Default Value	Required	Description
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Binary Download Location	`/opt/IBM/WAS`	required	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Files	no default	required	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
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.

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

See Parameters for Provision WebSphere and Deployment Manager for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see How to Use a Policy to Specify Parameter Values on page 135).

3. In the workflow editor, expose any additional parameters that you need (see How to Expose Additional Workflow Parameters on page 134). 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" in *HP DMA Quick Start Tutorial* 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" in *HP DMA Quick Start Tutorial* for instructions).

To verify the results:

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

Be sure to also perform the following steps:

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

   WAS_ROOT/bin/versionInfo.sh

   Here, *WAS_ROOT* is the directory where WebSphere 8.0 or 8.5.x 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 8.0 or 8.5.x 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 and Deployment Manager workflow.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see How to Use a Policy to Specify Parameter Values on page 135).

New Install with Deployment Manager – Parameter Value Examples

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

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

Parameter Name	Example Value	Description
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	DevManager	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	DevDmgr	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Web Service Password	myWebSvcPwd	Password for the discovery web service API.
Web Service User	JohnDoe	User capable of modifying the managed environment through the discovery web service API.
WebSphere Binary Download Location	/opt/IBM/was	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Files	WAS_V8.0_disk1.zip, WAS_V8.0_disk2.zip, WAS_V8.0_disk3.zip, WAS_V8.0_disk4.zip	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	/opt/IBM/was	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
WebSphere Install Location	/opt/IBM/ WebSphere/AppServer	Fully qualified path where WebSphere will be installed.

Parameters for Provision WebSphere 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 134). For most parameters, if you do not specify a value for a parameter, a default value is assigned

Input Parameters Defined in this Step: Gather Parameters for WebSphere and Deployment Manager

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

Input Parameters Defined in this Step: Gather Parameters for WebSphere and Deployment Manager (continued)

Parameter Name	Default Value	Required	Description
Install Manager Binary Download Location	`/opt/IBM/iim`	required	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For example: `/opt/IBM/iim`
Install Manager Binary Files	no default	required	Name of the compressed Install Manager software package.
Install Manager Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as WebSphere Extract Location.
Install Manager Install Location	no default	required	Fully qualified path where Install Manager will be installed. For example: `/opt/IBM/InstallManager`
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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Binary Download Location	`/opt/IBM/WAS`	required	Fully qualified path to the compressed WebSphere software package on the target machine.

Input Parameters Defined in this Step: Gather Parameters for WebSphere and Deployment Manager (continued)

Parameter Name	Default Value	Required	Description
WebSphere Binary Files	no default	required	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
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.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere and Deployment Manager

Parameter Name	Default Value	Required	Description
Cleanup on Failure	True	optional	Indicates whether to remove downloaded and extracted files and to clean up the installation directory in the event of workflow failure. Valid values are True and False. The default is True, which will clean up on failure.
Cleanup on Success	True	optional	Indicates whether to remove downloaded and extracted files and to clean up the installation directory in the event of workflow success. Valid values are True and False. The default is True, which will clean up on success.
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.
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.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere and Deployment Manager (continued)

Parameter Name	Default Value	Required	Description
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 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.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere and Deployment Manager (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.

Provision WebSphere and Custom Node

Use this workflow to install the WebSphere 8.0 or 8.5.x Base core binaries and, optionally, create a custom profile.

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

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

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

Note: The documentation for this workflow contains steps that are referred to by their base names. The names in the HP DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere 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 8.0 and 8.5.x documentation, the following system libraries are required before provisioning IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x on 64-bit and 32-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 gtk2-2.10.4-29.el5 gtk2-engines-2.8.0-3.el5 ksh-20080202-14 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libstdc++-4.1.2-48 libXft-2.1.10-1.1 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5

Platform	Required Library
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 elfutils-0.148-1 elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 libstdc++-4.4.4-13 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 libXft-2.1.13-4.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5

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 8.0 and 8.5.x, refer to the WebSphere 8.0 and 8.5.x Product Documentation on page 128.

How this Workflow Works

This topic contains the following information about the Provision WebSphere 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 8.0 or 8.5.x
3. Creates a Custom Node profile

The workflow checks to see if the WebSphere 8.0 or 8.5.x binary archive files exist on the target machine. If they do not, the files are downloaded from the software repository (for more information, see How to Import a File into the Software Repository on page 138).

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 8.0 and 8.5.x are installed.

Validation Checks Performed

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

The workflow first performs the following parameter checks:

1. Required parameters have values specified.
2. WebSphere specific names do not contain the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
3. Parameters do not contain illegal characters for the parameter type.
4. Flag parameters are set to true or false.
5. Integer parameters are set to appropriate integer values.
6. Mutually dependent parameters are specified appropriately as a set.
7. Parameters are set to one of the values if the parameter has a list of valid values.
8. License Acceptance is true (for workflows that input the License Acceptance parameter).
9. All specified file names are legal file names.
10. All specified locations are legal path names. If they do not exist they will be created.

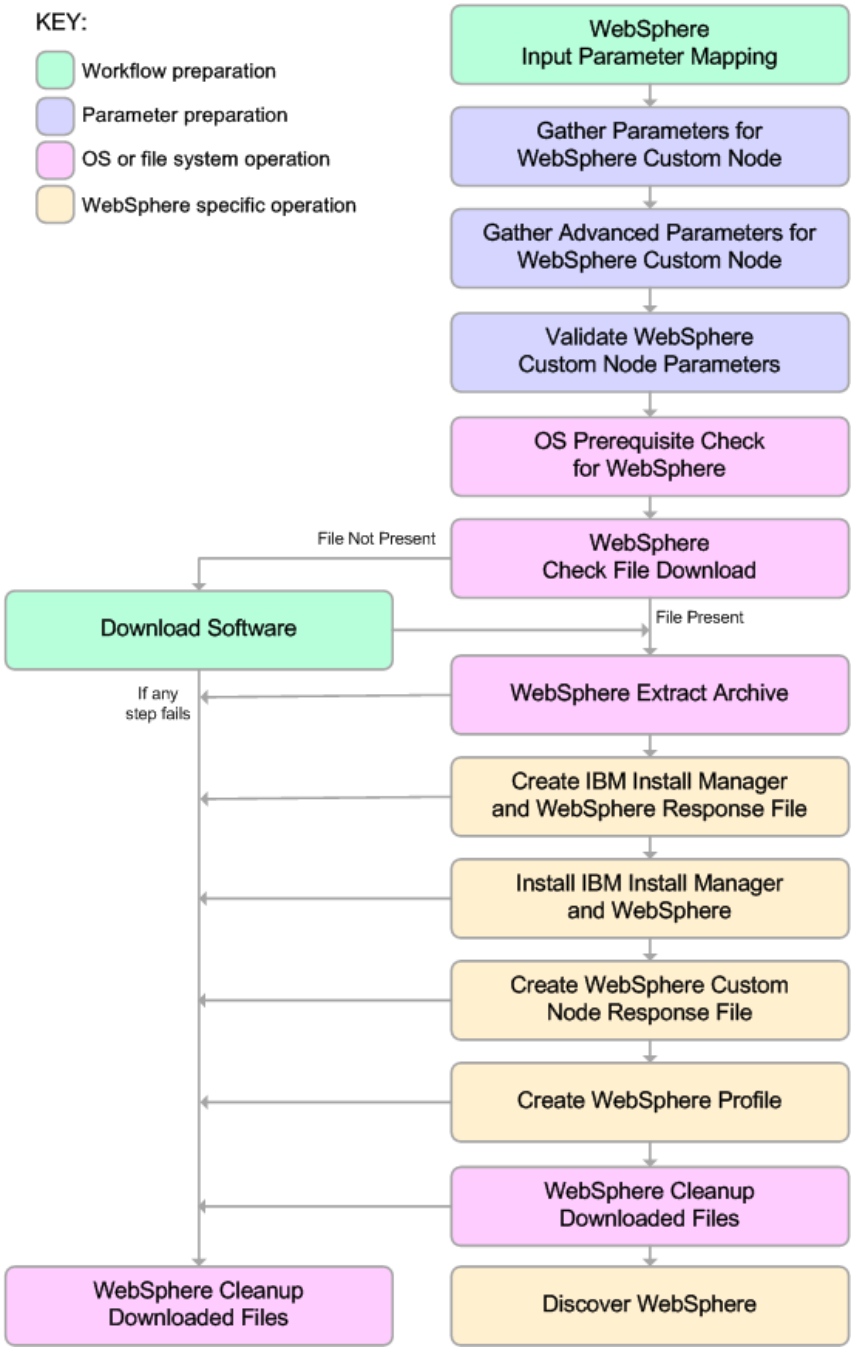
Note: For more information about valid parameter values, see Parameters for Provision WebSphere and Custom Node.

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

1. All required libraries are present (see Prerequisites for this Workflow).
2. Sufficient disk space is available to install WebSphere 8.0 or 8.5.x.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

The Provision WebSphere 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.



Process Flow

This workflow performs the following tasks:

1. Creates the call wrapper and determines the target server platform type.
2. Gathers and validates the parameters needed to install WebSphere 8.0 or 8.5.x and create a Custom Node profile (see Validation Checks Performed on page 61).
3. Checks the following:
   a. Documented library requirements for WebSphere 8.0 and 8.5.x (see the Prerequisites for this Workflow).
   b. File system space requirements where WebSphere 8.0 or 8.5.x will be installed.
   c. Temporary space requirements where the compressed software will be extracted before it is installed.
4. Determines whether the WebSphere 8.0 or 8.5.x binary archive is present on the target machine. If the archive is not present, the workflow downloads it from the software repository (see How to Import a File into the Software Repository on page 138).
5. Extracts the WebSphere 8.0 or 8.5.x binary archive to the specified directory.
6. Creates a response file for the purpose of installing a new instance of WebSphere 8.0 or 8.5.x.
7. Installs the IBM Installation Manager and a new WebSphere 8.0 or 8.5.x 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 8.0 or 8.5.x installation.
9. Creates a custom profile on top of the WebSphere 8.0 or 8.5.x installation.
10. Cleans up any files that were downloaded—for either workflow success or failure.

    Note: The parameters Cleanup on Success and Cleanup on Failure are defaulted to True. If they are set to False, the downloaded files are not cleaned up.

11. Discovers any WebSphere 8.0 or 8.5.x 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 and Custom Node workflow in your environment.

Tip: For detailed instructions to run HP DMA workflows—using the Run Oracle Compliance Audit workflow as an example—see *HP DMA Quick Start Tutorial*.

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 and Custom Node.

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

To use the Provision WebSphere and Custom Node workflow:

1. Create a deployable copy of the workflow (see "Create a Deployable Workflow" in *HP DMA Quick Start Tutorial*).
2. Determine the values that you will specify for the following parameters:

   Parameters Defined in this Step: Gather Parameters for WebSphere Custom Node

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: Gather Parameters for WebSphere Custom Node (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). Required if Federate Later is set to false.
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). Required if Federate Later is set to false.
Enable Security	no default	required	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.
Federate Later	no default	required	If false, the new custom node will be federated by the workflow during profile creation; you must specify Dmgr HostName and Dmgr Port to do this. If true, you must federate it later manually by using the addNode command.
Install Manager Binary Download Location	`/opt/IBM/iim`	required	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For example: `/opt/IBM/iim`
Install Manager Binary Files	no default	required	Name of the compressed Install Manager software package.
Install Manager Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as WebSphere Extract Location.

Parameters Defined in this Step: Gather Parameters for WebSphere Custom Node (continued)

Parameter Name	Default Value	Required	Description
Install Manager Install Location	no default	required	Fully qualified path where Install Manager will be installed. For example: `/opt/IBM/InstallManager`
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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Binary Download Location	`/opt/IBM/WAS`	required	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Files	no default	required	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.

Parameters Defined in this Step: Gather Parameters for WebSphere Custom Node (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.

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

See Parameters for Provision WebSphere and Custom Node for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see How to Use a Policy to Specify Parameter Values on page 135).

3. In the workflow editor, expose any additional parameters that you need (see How to Expose Additional Workflow Parameters on page 134). 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" in *HP DMA Quick Start Tutorial* 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" in *HP DMA Quick Start Tutorial* for instructions).

To verify the results:

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

Be sure to also perform the following steps:

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

   WAS_ROOT/bin/versionInfo.sh

   Here, *WAS_ROOT* is the directory where WebSphere 8.0 or 8.5.x 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 8.0 or 8.5.x 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 and Custom Node workflow.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see How to Use a Policy to Specify Parameter Values on page 135).

New Install with Custom Node Profile – Parameter Value Examples

Parameter Name	Example Value	Description
Cell Name	Dev NodeCell	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	wasPassWord	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). Required if Federate Later is set to false.
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). Required if Federate Later is set to false.
Enable Security	true	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.

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

Parameter Name	Example Value	Description
Federate Later	true	If false, the new custom node will be federated by the workflow during profile creation; you must specify Dmgr HostName and Dmgr Port to do this. If true, you must federate it later manually by using the addNode command.
Install Manager Binary Download Location	/opt/IBM/iim	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For example: `/opt/IBM/iim`
Install Manager Binary Files	IBM_Install_Manager_Linux.zip	Name of the compressed Install Manager software package.
Install Manager Extract Location	/opt/IBM/iim	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as WebSphere Extract Location.
Install Manager Install Location	/opt/IBM/installManager	Fully qualified path where Install Manager will be installed. For example: `/opt/IBM/InstallManager`
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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Web Service Password	myWebSvcPwd	Password for the discovery web service API.
Web Service User	JohnDoe	User capable of modifying the managed environment through the discovery web service API.

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

Parameter Name	Example Value	Description
WebSphere Binary Download Location	/opt/IBM/was	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Files	WAS_V8.0_disk1.zip, WAS_V8.0_disk2.zip	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	/opt/IBM/was	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
WebSphere Install Location	/opt/IBM/ WebSphere/AppServer	Fully qualified path where WebSphere will be installed.

Parameters for Provision WebSphere 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 134). For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Input Parameters Defined in this Step: Gather Parameters for WebSphere Custom Node

Parameter Name	Default Value	Required	Description
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. Defaults are: UNIX targets: `/opt/hp/dma/client/jython.sh` running as root Windows targets: `jython` running as Administrator **Caution:** This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.
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). Required if Federate Later is set to false.

Input Parameters Defined in this Step: Gather Parameters for WebSphere Custom Node (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). Required if Federate Later is set to false.
Enable Security	no default	required	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.
Federate Later	no default	required	If false, the new custom node will be federated by the workflow during profile creation; you must specify Dmgr HostName and Dmgr Port to do this. If true, you must federate it later manually by using the addNode command.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Install Manager Binary Download Location	`/opt/IBM/iim`	required	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For example: `/opt/IBM/iim`
Install Manager Binary Files	no default	required	Name of the compressed Install Manager software package.
Install Manager Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as WebSphere Extract Location.
Install Manager Install Location	no default	required	Fully qualified path where Install Manager will be installed. For example: `/opt/IBM/InstallManager`
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: Gather Parameters for WebSphere Custom Node (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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Binary Download Location	`/opt/IBM/WAS`	required	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Files	no default	required	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
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.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere Custom Node

Parameter Name	Default Value	Required	Description
Cleanup on Failure	True	optional	Indicates whether to remove downloaded and extracted files and to clean up the installation directory in the event of workflow failure. Valid values are True and False. The default is True, which will clean up on failure.
Cleanup on Success	True	optional	Indicates whether to remove downloaded and extracted files and to clean up the installation directory in the event of workflow success. Valid values are True and False. The default is True, which will clean up on success.
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.
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 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.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere Custom Node (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.

Provision WebSphere Stand-Alone Profile From Existing Install

Use this workflow to create a stand-alone profile on an existing WebSphere 8.0 or 8.5.x installation.

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

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

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

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere Stand-Alone 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 8.0 and 8.5.x documentation, the following system libraries are required before provisioning IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x on 64-bit and 32-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 gtk2-2.10.4-29.el5 gtk2-engines-2.8.0-3.el5 ksh-20080202-14 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libstdc++-4.1.2-48 libXft-2.1.10-1.1 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5

Platform	Required Library
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 elfutils-0.148-1 elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 libstdc++-4.4.4-13 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 libXft-2.1.13-4.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5

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 8.0 and 8.5.x, refer to the WebSphere 8.0 and 8.5.x Product Documentation on page 128.

How this Workflow Works

This topic contains the following information about the Provision WebSphere Stand-Alone Profile From Existing Install workflow:

Overview

This workflow creates a stand-alone profile on an existing WebSphere 8.0 or 8.5.x 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 (on Red Hat Linux platforms only).

The workflow first performs the following parameter checks:

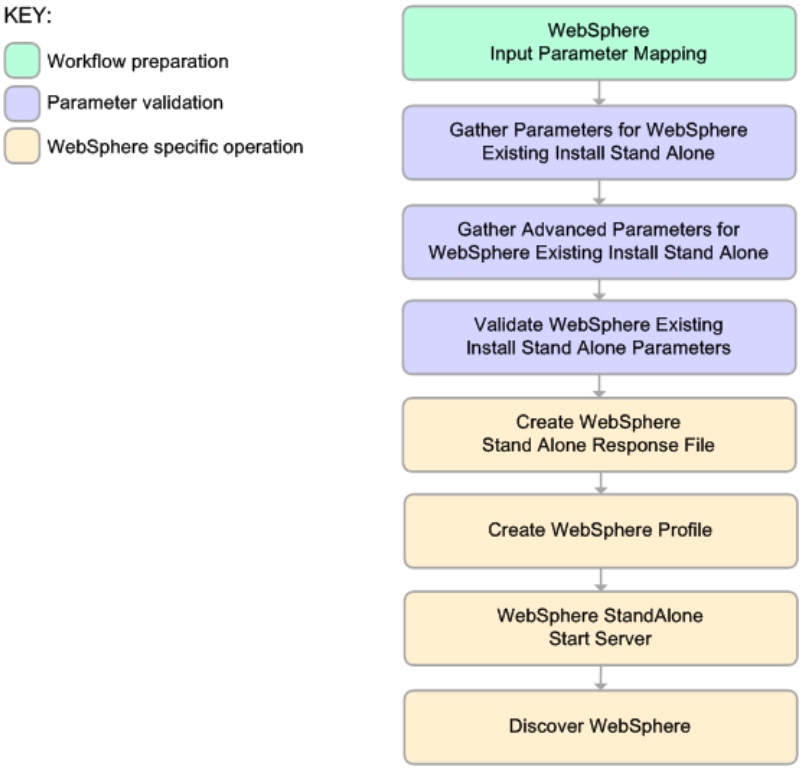
1. Required parameters have values specified.
2. WebSphere specific names do not contain the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
3. Parameters do not contain illegal characters for the parameter type.
4. Flag parameters are set to true or false.
5. Integer parameters are set to appropriate integer values.
6. Mutually dependent parameters are specified appropriately as a set.
7. Parameters are set to one of the values if the parameter has a list of valid values.
8. License Acceptance is true (for workflows that input the License Acceptance parameter).
9. All specified file names are legal file names.
10. All specified locations are legal path names. If they do not exist they will be created.

Note: For more information about valid parameter values, see Parameters for Provision WebSphere Stand-Alone Profile from Existing Install.

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

Steps Executed

The Provision WebSphere Stand-Alone 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.



Process Flow

This workflow performs the following tasks:

1. Creates the call wrapper and determines the target server platform type.
2. Gathers and 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 8.0 or 8.5.x installation.
4. Creates a stand-alone profile on top of the WebSphere 8.0 or 8.5.x installation.
5. Starts the stand-alone application server.
6. Discovers any WebSphere 8.0 or 8.5.x 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 Stand-Alone Profile From Existing Install workflow in your environment.

Tip: For detailed instructions to run HP DMA workflows—using the Run Oracle Compliance Audit workflow as an example—see *HP DMA Quick Start Tutorial*.

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 Stand-Alone Profile from Existing Install.

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 Stand-Alone Profile From Existing Install workflow:

1. Create a deployable copy of the workflow (see "Create a Deployable Workflow" in *HP DMA Quick Start Tutorial*).
2. Determine the values that you will specify for the following parameters:

   Parameters Defined in this Step: Gather Parameters for WebSphere Existing Install Stand Alone

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.

Parameters Defined in this Step: Gather Parameters for WebSphere Existing Install Stand Alone (continued)

Parameter Name	Default Value	Required	Description
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
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.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
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.

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

See Parameters for Provision WebSphere Custom Node Profile From Existing Install for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see How to Use a Policy to Specify Parameter Values on page 135).

3. In the workflow editor, expose any additional parameters that you need (see How to Expose Additional Workflow Parameters on page 134). 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" in *HP DMA Quick Start Tutorial* 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" in *HP DMA Quick Start Tutorial* for instructions).

To verify the results:

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

Be sure to also perform the following steps:

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

   WAS_ROOT/bin/versionInfo.sh

   Here, *WAS_ROOT* is the directory where WebSphere 8.0 or 8.5.x 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 8.0 or 8.5.x 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 Stand-Alone Profile From Existing Install workflow.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see How to Use a Policy to Specify Parameter Values on page 135).

Stand-Alone Profile on Existing Install – Parameter Value Examples

Parameter Name	Example Value	Description
Admin Password	wasPassWord	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Admin User	wasadmin	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Cell Name	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.
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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Server Name	Server1	Name of the application server that will be created under the profile.
Web Service Password	myWebSvcPwd	Password for the discovery web service API.
Web Service User	JohnDoe	User capable of modifying the managed environment through the discovery web service API.

Stand-Alone Profile on Existing Install – Parameter Value Examples (continued)

Parameter Name	Example Value	Description
WebSphere Install Location	/opt/IBM/ WebSphere/AppServer	Fully qualified path where WebSphere will be installed.

Parameters for Provision WebSphere Stand-Alone 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 134). For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Input Parameters Defined in this Step: Gather Parameters for WebSphere Existing Install Stand Alone

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

Input Parameters Defined in this Step: Gather Parameters for WebSphere Existing Install Stand Alone (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.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
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.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere Existing Install Stand Alone

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.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere Existing Install Stand Alone (continued)

Parameter Name	Default Value	Required	Description
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.
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 Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation.
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: CN=dmalab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere Existing Install Stand Alone (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.

Provision WebSphere Custom Node Profile From Existing Install

Use this workflow to create a custom profile on an existing WebSphere 8.0 or 8.5.x installation.

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

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

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

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere 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 8.0 and 8.5.x documentation, the following system libraries are required before provisioning IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x on 64-bit and 32-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 gtk2-2.10.4-29.el5 gtk2-engines-2.8.0-3.el5 ksh-20080202-14 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libstdc++-4.1.2-48 libXft-2.1.10-1.1 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5

Platform	Required Library
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 elfutils-0.148-1 elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 libstdc++-4.4.4-13 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 libXft-2.1.13-4.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5

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 8.0 and 8.5.x, refer to the WebSphere 8.0 and 8.5.x Product Documentation on page 128.

How this Workflow Works

This topic contains the following information about the Provision WebSphere Custom Node Profile From Existing Install workflow:

Overview

This workflow creates a Custom Node profile on an existing WebSphere 8.0 or 8.5.x 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 (on Red Hat Linux platforms only).

The workflow first performs the following parameter checks:

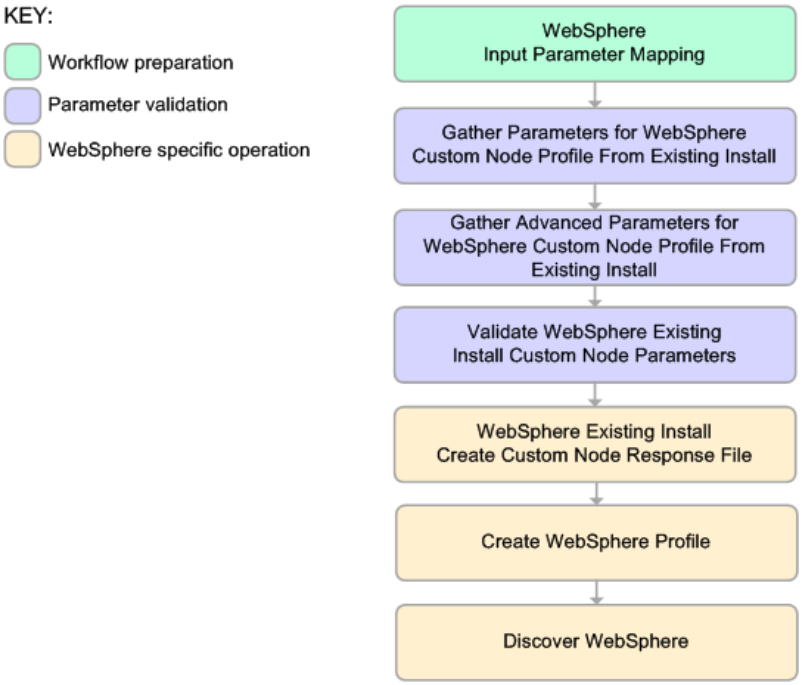
1. Required parameters have values specified.
2. WebSphere specific names do not contain the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
3. Parameters do not contain illegal characters for the parameter type.
4. Flag parameters are set to true or false.
5. Integer parameters are set to appropriate integer values.
6. Mutually dependent parameters are specified appropriately as a set.
7. Parameters are set to one of the values if the parameter has a list of valid values.
8. License Acceptance is true (for workflows that input the License Acceptance parameter).
9. All specified file names are legal file names.
10. All specified locations are legal path names. If they do not exist they will be created.

Note: For more information about valid parameter values, see Parameters for Provision WebSphere Custom Node Profile From Existing Install .

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

Steps Executed

The Provision WebSphere 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.



Process Flow

This workflow performs the following tasks:

1. Creates the call wrapper and determines the target server platform type.
2. Gathers and 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 8.0 or 8.5.x installation.
4. Creates a Custom Node profile on top of the WebSphere 8.0 or 8.5.x installation.
5. Federates into the Deployment Manager.
6. Discovers any WebSphere 8.0 or 8.5.x 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 Custom Node Profile From Existing Install workflow in your environment.

Tip: For detailed instructions to run HP DMA workflows—using the Run Oracle Compliance Audit workflow as an example—see *HP DMA Quick Start Tutorial*.

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 Custom Node Profile From Existing Install .

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

To use the Provision WebSphere Custom Node Profile from Existing Install workflow:

1. Create a deployable copy of the workflow (see "Create a Deployable Workflow" in *HP DMA Quick Start Tutorial*).
2. Determine the values that you will specify for the following parameters:

   Parameters Defined in this Step: Gather Parameters for WebSphere Custom Node Profile From Existing Install

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: Gather Parameters for WebSphere Custom Node Profile From Existing Install (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). Required if Federate Later is set to false.
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). Required if Federate Later is set to false.
Enable Security	no default	required	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr 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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.

Parameters Defined in this Step: Gather Parameters for WebSphere Custom Node Profile From Existing Install (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.

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

See Parameters for Provision WebSphere Custom Node Profile From Existing Install for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see How to Use a Policy to Specify Parameter Values on page 135).

3. In the workflow editor, expose any additional parameters that you need (see How to Expose Additional Workflow Parameters on page 134). 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" in *HP DMA Quick Start Tutorial* 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" in *HP DMA Quick Start Tutorial* for instructions).

To verify the results:

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

Be sure to also perform the following steps:

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

   WAS_ROOT/bin/versionInfo.sh

   Here, *WAS_ROOT* is the directory where WebSphere 8.0 or 8.5.x 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 8.0 or 8.5.x 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 Custom Node Profile From Existing Install workflow.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see How to Use a Policy to Specify Parameter Values on page 135).

Custom Node Profiles on Existing Install – Parameter Value Examples

Parameter Name	Example Value	Description
Cell Name	Dev NodeCell	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	wasPassWord	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). Required if Federate Later is set to false.
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). Required if Federate Later is set to false.

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

Parameter Name	Example Value	Description
Enable Security	true	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr 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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Web Service Password	myWebSvcPwd	Password for the discovery web service API.
Web Service User	JohnDoe	User capable of modifying the managed environment through the discovery web service API.
WebSphere Install Location	/opt/IBM/ WebSphere/AppServer	Fully qualified path where WebSphere will be installed.

Parameters for Provision WebSphere 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 134). For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Input Parameters Defined in this Step: Gather Parameters for WebSphere Custom Node Profile From Existing Install

Parameter Name	Default Value	Required	Description
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. Defaults are: UNIX targets: `/opt/hp/dma/client/jython.sh` running as root Windows targets: `jython` running as Administrator **Caution:** This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.
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). Required if Federate Later is set to false.

Input Parameters Defined in this Step: Gather Parameters for WebSphere Custom Node Profile From Existing Install (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). Required if Federate Later is set to false.
Enable Security	no default	required	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.
Host Name	Server.name	required	Hostname or IP address of the target machine.
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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
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.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere Custom Node Profile From Existing Install

Parameter Name	Default Value	Required	Description
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.
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 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.

Provision IBM HTTP Server and Plug-in

Use this workflow to install IBM HTTP Server for WebSphere Application Server version 8.0 or 8.5.x and the plug-in on a target system and then to configure a Web server instance along with the plug-in on the same target system.

IBM HTTP Server version 8.0 or 8.5.x is a Web server that will serve both static and dynamic content. Usually you will front your WebSphere Application Server environment with an IBM HTTP Server.

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

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

Note: The documentation for this workflow contains steps that are referred to by their base names. The names in the HP DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision IBM HTTP Server and Plug-in 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 8.0 and 8.5.x documentation, the following system libraries are required before provisioning IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x on 64-bit and 32-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 gtk2-2.10.4-29.el5 gtk2-engines-2.8.0-3.el5 ksh-20080202-14 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libstdc++-4.1.2-48 libXft-2.1.10-1.1 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5

Platform	Required Library
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 elfutils-0.148-1 elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 libstdc++-4.4.4-13 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 libXft-2.1.13-4.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5

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.

For more information about prerequisites for WebSphere 8.0 and 8.5.x, refer to the WebSphere 8.0 and 8.5.x Product Documentation on page 128.

How this Workflow Works

This topic contains the following information about the Provision IBM HTTP Server and Plug-in workflow:

Overview

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

1. Installs the IBM Install Manager
2. Installs IBM HTTP Server version 8.0 or 8.5.x and the plug-in
3. Configures a Web server instance
4. Creates a plug-in configuration for the Web server instance
5. Optionally, creates the HTTP admin instance
6. Optionally, runs all Web server instances and the HTTP admin instance as a non-root system account
7. Starts the Web server instance and, if configured, starts the HTTP admin instance
8. Discovers all IBM HTTP Server instances and populates HP DMA with the relevant configuration information

The workflow checks to see if the IBM HTTP Server version 8.0 or 8.5.x binary archive files exist on the target machine. If they do not, the files are downloaded from the software repository (for more information, see How to Import a File into the Software Repository on page 138).

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 8.0 and 8.5.x are installed.

Validation Checks Performed

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

The workflow first performs the following parameter checks:

1. Required parameters have values specified.
2. WebSphere specific names do not contain the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
3. Parameters do not contain illegal characters for the parameter type.
4. Flag parameters are set to true or false.
5. Integer parameters are set to appropriate integer values.
6. Mutually dependent parameters are specified appropriately as a set.
7. Parameters are set to one of the values if the parameter has a list of valid values.
8. License Acceptance is true (for workflows that input the License Acceptance parameter).
9. All specified file names are legal file names.
10. All specified locations are legal path names. If they do not exist they will be created.

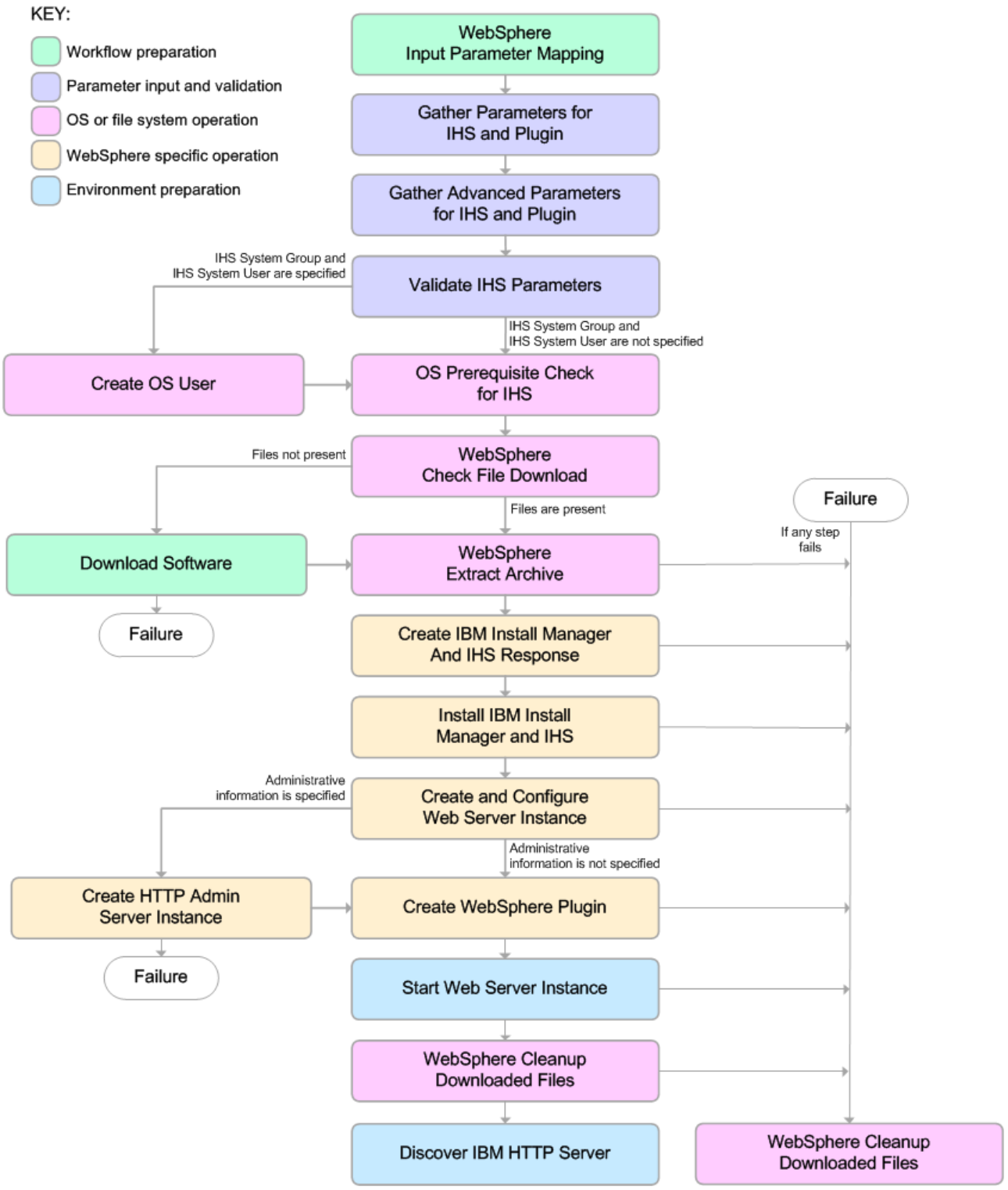
Note: For more information about valid parameter values, see Parameters for Provision IBM HTTP Server and Plug-in.

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

1. All required libraries are present (see Prerequisites for this Workflow).
2. Sufficient disk space is available to install IBM HTTP Server for WebSphere Application Server version 8.0 or 8.5.x.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

The Provision IBM HTTP Server and Plug-in 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 to facilitate the execution of subsequent steps.
2. Gathers and validates the parameters needed to install IBM HTTP Server version 8.0 or 8.5.x and the plug-in (see Validation Checks Performed on page 109).
3. *Optional:* Creates the operating system user—if IHS System User and IHS System Group are specified.
4. Checks the following:
   a. Documented library requirements for IBM HTTP Server versions 8.0 and 8.5.x (see the Prerequisites for this Workflow).
   b. File system space requirements where IBM HTTP Server version 8.0 or 8.5.x will be installed.
   c. Temporary space requirements where the compressed software will be extracted before it is installed.
5. Determines whether the IBM HTTP Server version 8.0 or 8.5.x binary archive and the Install Manager binary archive are present on the target machine. If the files are not present, the workflow downloads them from the software repository (see How to Import a File into the Software Repository on page 138).
6. Extracts the IBM HTTP Server version 8.0 or 8.5.x and Install Manager binary archives to the specified directories.
7. Creates a response file for the purpose of installing the IBM Install Manager, a new IBM HTTP Server version 8.0 or 8.5.x instance, and the WebSphere plug-in.
8. Installs the IBM Installation Manager, a new IBM HTTP Server version 8.0 or 8.5.x instance, and the WebSphere plug-in on the target server.
9. Creates a new Web server instance under the installation root of IBM HTTP Server.
10. *Optional:* Creates the HTTP Admin Web server instance—if HTTP Admin User, HTTP Admin Password, and HTTP Admin Port are specified.
11. Creates the plug-in configuration files and plug-in log directory.
12. Starts the Web server instance.
13. Cleans up any files that were downloaded—for either workflow success or failure.

    Note: The parameters Cleanup on Success and Cleanup on Failure are defaulted to True. If they are set to False, the downloaded files are not cleaned up.

14. Discovers all IBM HTTP Server instances and populates HP DMA with the relevant configuration information.

How to Run this Workflow

The following instructions show you how to customize and run the Provision IBM HTTP Server and Plug-in workflow in your environment.

Tip: For detailed instructions to run HP DMA workflows—using the Run Oracle Compliance Audit workflow as an example—see *HP DMA Quick Start Tutorial*.

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 IBM HTTP Server and Plug-in.

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

To customize and run the Provision IBM HTTP Server and Plug-in workflow:

1. Create a deployable copy of the workflow (see "Create a Deployable Workflow" in *HP DMA Quick Start Tutorial*).
2. Determine the values that you will specify for the following parameters:

Parameters Defined in this Step: Gather Parameters for IHS and Plugin

Parameter Name	Default Value	Required	Description
Http Port	80	required	The port on which the Web server will listen. Default is set to 80. If the Web server instance is run as non-root this value has to be greater than 1024.
IHS Binary Download Location	no default	required	Name of the compressed IHS software package.
IHS Binary Files	no default	required	Name of the compressed IHS software package.
IHS Extract Location	no default	required	Fully-qualified path where the compressed software will be extracted on the target machine. This cannot be the same as the Install Manager Extract Location.
IHS Install Location	no default	required	Fully-qualified path where IHS will be installed.

Parameters Defined in this Step: Gather Parameters for IHS and Plugin (continued)

Parameter Name	Default Value	Required	Description
Install Manager Binary Download Location	no default	required	Fully-qualified path to the compressed Install Manager software package on the target machine.
Install Manager Binary Files	no default	required	Name of the compressed Install Manager software package.
Install Manager Extract Location	no default	required	Fully-qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as the IHS Extract Location.
Install Manager Install Location	no default	required	Fully-qualified path where the 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 for the installation to continue.
Web Server Name	no default	required	Required: Fully-qualified name of the Web server instance. There can be no spaces in the name. For example: `myapp.hp.com`
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.

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

See Parameters for Provision IBM HTTP Server and Plug-in for detailed descriptions of all input parameters for this workflow, including default values.

> **Tip:** To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see How to Use a Policy to Specify Parameter Values on page 135).

3. In the workflow editor, expose any additional parameters that you need (see How to Expose Additional Workflow Parameters on page 134). 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" in *HP DMA Quick Start Tutorial* 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" in *HP DMA Quick Start Tutorial* for instructions).

To verify the results:

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

Be sure to also perform the following step:

After the workflow has completed, run the following command to check the version of IBM HTTP Server that was installed:

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

Here, *WAS_ROOT* is the directory where IBM HTTP Server was installed. For example:
`/opt/IBM/HTTPServer`

Sample Scenario

This topic shows you typical parameter values used for the Provision IBM HTTP Server and Plug-in workflow.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see How to Use a Policy to Specify Parameter Values on page 135).

Scenario 1:

Provision IBM HTTP Server 8 and plug-in with root - Parameter Value Examples

Parameter Name	Example Value	Description
Http Port	80	The port on which the Web server will listen. Default is set to 80. If the Web server instance is run as non-root this value has to be greater than 1024.
IHS Binary Download Location	`/opt/wasv8`	Name of the compressed IHS software package.
IHS Binary Files	`IHSbinary1.zip, IHSbinary2.zip, IHSbinary3.zip, IHSbinary4.zip,`	Name of the compressed IHS software package.
IHS Extract Location	`/opt/ihsv8`	Fully-qualified path where the compressed software will be extracted on the target machine. This cannot be the same as the Install Manager Extract Location.
IHS Install Location	`/opt/IBM/HTTPServer`	Fully-qualified path where IHS will be installed.
Install Manager Binary Download Location	`/opt/IBM/iim`	Fully-qualified path to the compressed Install Manager software package on the target machine.
Install Manager Binary Files	`IBM_Install_ Manager_Linux_ 1.5.3.zip`	Name of the compressed Install Manager software package.
Install Manager Extract Location	`/opt/IBM/iim`	Fully-qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as the IHS Extract Location.

Provision IBM HTTP Server 8 and plug-in with root - Parameter Value Examples (continued)

Parameter Name	Example Value	Description
Install Manager Install Location	`/opt/IBM/installManager`	Fully-qualified path where the 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 for the installation to continue.
Web Server Name	`example.mycompany.com`	Required: Fully-qualified name of the Web server instance. There can be no spaces in the name. For example: `myapp.hp.com`
Web Service Password	WebSrvPsWd	Password for the discovery web service API.
Web Service User	no default	User capable of modifying the managed environment through the discovery web service API.

Scenario 2:

Provision IBM HTTP Server 8 and plug-in with non-root - Parameter Value Examples

Parameter Name	Example Value	Description
Http Port	80	The port on which the Web server will listen. Default is set to 80. If the Web server instance is run as non-root this value has to be greater than 1024.
IHS Binary Download Location	`/opt/wasv8`	Name of the compressed IHS software package.
IHS Binary Files	`IHSbinary1.zip, IHSbinary2.zip, IHSbinary3.zip, IHSbinary4.zip,`	Name of the compressed IHS software package.

Provision IBM HTTP Server 8 and plug-in with non-root - Parameter Value Examples (continued)

Parameter Name	Example Value	Description
IHS Extract Location	`/opt/ihsv8`	Fully-qualified path where the compressed software will be extracted on the target machine. This cannot be the same as the Install Manager Extract Location.
IHS Install Location	`/opt/IBM/HTTPServer`	Fully-qualified path where IHS will be installed.
Install Manager Binary Download Location	`/opt/IBM/iim`	Fully-qualified path to the compressed Install Manager software package on the target machine.
Install Manager Binary Files	`IBM_Install_ Manager_Linux_ 1.5.3.zip`	Name of the compressed Install Manager software package.
Install Manager Extract Location	`/opt/IBM/iim`	Fully-qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as the IHS Extract Location.
Install Manager Install Location	`/opt/IBM/ installManager`	Fully-qualified path where the 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 for the installation to continue.
Web Server Name	`example. mycompany.com`	Required: Fully-qualified name of the Web server instance. There can be no spaces in the name. For example: `myapp.hp.com`
Web Service Password	WebSrvPsWd	Password for the discovery web service API.
Web Service User	no default	User capable of modifying the managed environment through the discovery web service API.

Provision IBM HTTP Server 8 and plug-in with non-root - Parameter Value Examples (continued)

Parameter Name	Example Value	Description
IHS System Group	webadmin	The group that owns and runs the Web server instances and the plug-in directories. If the system group account does not already exist the account will be created on the target machine.
IHS System Password	SysPsWd	The password for the user that owns and runs the Web server instances and the plug-in directories. This password will be used when creating the system user.
IHS System User	ihsadmin	The user that owns and runs the Web server instances and the plug-in directories. If the system user account does not already exist the account will be created on the target machine.

Note: For this use case you need to expose the following parameters in the Gather Advanced Parameters for IHS and Plugin step (see How to Expose Additional Workflow Parameters on page 134 for instructions):

The IHS System parameters: IHS System Group, IHS System Password, and IHS System User

Scenario 3:

Provision IBM HTTP Server 8, plug-in, and HTTP Admin Server with non-root - Parameter Value Examples

Parameter Name	Example Value	Description
Http Port	80	The port on which the Web server will listen. Default is set to 80. If the Web server instance is run as non-root this value has to be greater than 1024.
IHS Binary Download Location	`/opt/wasv8`	Name of the compressed IHS software package.
IHS Binary Files	`IHSbinary1.zip, IHSbinary2.zip, IHSbinary3.zip, IHSbinary4.zip,`	Name of the compressed IHS software package.
IHS Extract Location	`/opt/ihsv8`	Fully-qualified path where the compressed software will be extracted on the target machine. This cannot be the same as the Install Manager Extract Location.

Provision IBM HTTP Server 8, plug-in, and HTTP Admin Server with non-root - Parameter Value Examples (continued)

Parameter Name	Example Value	Description
IHS Install Location	`/opt/IBM/HTTPServer`	Fully-qualified path where IHS will be installed.
Install Manager Binary Download Location	`/opt/IBM/iim`	Fully-qualified path to the compressed Install Manager software package on the target machine.
Install Manager Binary Files	`IBM_Install_ Manager_Linux_ 1.5.3.zip`	Name of the compressed Install Manager software package.
Install Manager Extract Location	`/opt/IBM/iim`	Fully-qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as the IHS Extract Location.
Install Manager Install Location	`/opt/IBM/ installManager`	Fully-qualified path where the 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 for the installation to continue.
Web Server Name	`example. mycompany.com`	Required: Fully-qualified name of the Web server instance. There can be no spaces in the name. For example: `myapp.hp.com`
Web Service Password	WebSrvPsWd	Password for the discovery web service API.
Web Service User	no default	User capable of modifying the managed environment through the discovery web service API.
HTTP Admin Password	AdMinPsWd	Password for the HTTP Admin User. If specified, HTTP Admin Port and HTTP Admin User must also be specified. If not specified, HTTP Admin Port and HTTP Admin User must not be specified.

Provision IBM HTTP Server 8, plug-in, and HTTP Admin Server with non-root - Parameter Value Examples (continued)

Parameter Name	Example Value	Description
HTTP Admin Port	8004	Port of the IBM HTTP Server administrative server. If specified, HTTP Admin Password and HTTP Admin User must also be specified. If not specified, HTTP Admin Password and HTTP Admin User must not be specified.
HTTP Admin User	wasadmin	User name of the IBM HTTP administrative user. If specified, HTTP Admin Password and HTTP Admin Port must also be specified. If not specified, HTTP Admin Password and HTTP Admin Port must not be specified.
IHS System Group	webadmin	The group that owns and runs the Web server instances and the plug-in directories. If the system group account does not already exist the account will be created on the target machine.
IHS System Password	SysPsWd	The password for the user that owns and runs the Web server instances and the plug-in directories. This password will be used when creating the system user.
IHS System User	ihsadmin	The user that owns and runs the Web server instances and the plug-in directories. If the system user account does not already exist the account will be created on the target machine.

Note: For this use case you need to expose the following parameters in the Gather Advanced Parameters for IHS and Plugin step (see How to Expose Additional Workflow Parameters on page 134 for instructions):

- The IHS System parameters: IHS System Group, IHS System Password, and IHS System User
- The HTTP Admin parameters: HTTP Admin Password, HTTP Admin Port, and HTTP Admin User

Scenario 4:

Provision IBM HTTP Server 8, plug-in, HTTP Admin Server, and HTTP SSL with non-root - Parameter Value Examples

Parameter Name	Example Value	Description
Http Port	80	The port on which the Web server will listen. Default is set to 80. If the Web server instance is run as non-root this value has to be greater than 1024.
IHS Binary Download Location	`/opt/wasv8`	Name of the compressed IHS software package.
IHS Binary Files	`IHSbinary1.zip, IHSbinary2.zip, IHSbinary3.zip, IHSbinary4.zip,`	Name of the compressed IHS software package.
IHS Extract Location	`/opt/ihsv8`	Fully-qualified path where the compressed software will be extracted on the target machine. This cannot be the same as the Install Manager Extract Location.
IHS Install Location	`/opt/IBM/HTTPServer`	Fully-qualified path where IHS will be installed.
Install Manager Binary Download Location	`/opt/IBM/iim`	Fully-qualified path to the compressed Install Manager software package on the target machine.
Install Manager Binary Files	`IBM_Install_ Manager_Linux_ 1.5.3.zip`	Name of the compressed Install Manager software package.
Install Manager Extract Location	`/opt/IBM/iim`	Fully-qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as the IHS Extract Location.
Install Manager Install Location	`/opt/IBM/ installManager`	Fully-qualified path where the 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 for the installation to continue.

Provision IBM HTTP Server 8, plug-in, HTTP Admin Server, and HTTP SSL with non-root - Parameter Value Examples (continued)

Parameter Name	Example Value	Description
Web Server Name	`example.mycompany.com`	Required: Fully-qualified name of the Web server instance. There can be no spaces in the name. For example: `myapp.hp.com`
Web Service Password	WebSrvPsWd	Password for the discovery web service API.
Web Service User	no default	User capable of modifying the managed environment through the discovery web service API.
HTTP Admin Password	AdMinPsWd	Password for the HTTP Admin User. If specified, HTTP Admin Port and HTTP Admin User must also be specified. If not specified, HTTP Admin Port and HTTP Admin User must not be specified.
HTTP Admin Port	8004	Port of the IBM HTTP Server administrative server. If specified, HTTP Admin Password and HTTP Admin User must also be specified. If not specified, HTTP Admin Password and HTTP Admin User must not be specified.
HTTP Admin User	wasadmin	User name of the IBM HTTP administrative user. If specified, HTTP Admin Password and HTTP Admin Port must also be specified. If not specified, HTTP Admin Password and HTTP Admin Port must not be specified.
HTTP SSL Port	443	The port on which the Web server will listen for SSL requests. Typically, this is set to 443. If the Web server instance is run as non-root this value has to be greater than 1024.
IHS System Group	webadmin	The group that owns and runs the Web server instances and the plug-in directories. If the system group account does not already exist the account will be created on the target machine.
IHS System Password	SysPsWd	The password for the user that owns and runs the Web server instances and the plug-in directories. This password will be used when creating the system user.

Provision IBM HTTP Server 8, plug-in, HTTP Admin Server, and HTTP SSL with non-root - Parameter Value Examples (continued)

Parameter Name	Example Value	Description
IHS System User	ihsadmin	The user that owns and runs the Web server instances and the plug-in directories. If the system user account does not already exist the account will be created on the target machine.
SSL Key Database Password	SslKeyDbPsWd	The password that will be used to create the SSL key database used to store the Web server instance SSL certificates.

Note: For this use case you need to expose the following parameters in the Gather Advanced Parameters for IHS and Plugin step (see How to Expose Additional Workflow Parameters on page 134 for instructions):

- The IHS System parameters: IHS System Group, IHS System Password, and IHS System User
- The HTTP Admin parameters: HTTP Admin Password, HTTP Admin Port, and HTTP Admin User
- The SSL parameters: HTTP SSL Port and SSL Key Database Password

Parameters for Provision IBM HTTP Server and Plug-in

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 134). For many parameters, if you do not specify a value for a parameter, a default value is assigned

Input Parameters Defined in this Step: Gather Parameters for IHS and Plugin

Parameter Name	Default Value	Required	Description
Http Port	80	required	The port on which the Web server will listen. Default is set to 80. If the Web server instance is run as non-root this value has to be greater than 1024.
IHS Binary Download Location	no default	required	Name of the compressed IHS software package.
IHS Binary Files	no default	required	Name of the compressed IHS software package.
IHS Extract Location	no default	required	Fully-qualified path where the compressed software will be extracted on the target machine. This cannot be the same as the Install Manager Extract Location.
IHS Install Location	no default	required	Fully-qualified path where IHS will be installed.
Install Manager Binary Download Location	no default	required	Fully-qualified path to the compressed Install Manager software package on the target machine.
Install Manager Binary Files	no default	required	Name of the compressed Install Manager software package.
Install Manager Extract Location	no default	required	Fully-qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as the IHS Extract Location.
Install Manager Install Location	no default	required	Fully-qualified path where the 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 for the installation to continue.

Input Parameters Defined in this Step: Gather Parameters for IHS and Plugin (continued)

Parameter Name	Default Value	Required	Description
Web Server Name	no default	required	Required: Fully-qualified name of the Web server instance. There can be no spaces in the name. For example: `myapp.hp.com`
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for IHS and Plugin

Parameter Name	Default Value	Required	Description
Access Log File	see description	optional	Fully-qualified path for the IBM HTTP Server access log file. For example: `/opt/IBM/HTTPServer/logs` The default is based on the values of IHS Install Location and Web Server Name.
Cleanup on Failure	True	optional	Indicates whether to remove downloaded and extracted files and to clean up the installation directory in the event of workflow failure. Valid values are True and False. The default is True, which will clean up on failure.
Cleanup on Success	True	optional	Indicates whether to remove downloaded and extracted files and to clean up the installation directory in the event of workflow success. Valid values are True and False. The default is True, which will clean up on success.
Error Log File	see description	optional	Fully-qualified path for the IBM HTTP Server error log file. For example: `/opt/IBM/HTTPServer/logs` The default is based on the values of IHS Install Location and Web Server Name.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for IHS and Plugin (continued)

Parameter Name	Default Value	Required	Description
HTTP Admin Password	no default	optional	Password for the HTTP Admin User. If specified, HTTP Admin Port and HTTP Admin User must also be specified. If not specified, HTTP Admin Port and HTTP Admin User must not be specified.
HTTP Admin Port	no default	optional	Port of the IBM HTTP Server administrative server. If specified, HTTP Admin Password and HTTP Admin User must also be specified. If not specified, HTTP Admin Password and HTTP Admin User must not be specified.
HTTP Admin User	no default	optional	User name of the IBM HTTP administrative user. If specified, HTTP Admin Password and HTTP Admin Port must also be specified. If not specified, HTTP Admin Password and HTTP Admin Port must not be specified.
HTTP Configuration File	see description	optional	Fully-qualified path for the IBM HTTP Server configuration file. For example: `/opt/IBM/HTTPServer/conf/httpd.conf` The default is based on the values of IHS Install Location and Web Server Name.
HTTP SSL Port	no default	optional	The port on which the Web server will listen for SSL requests. Typically, this is set to 443. If the Web server instance is run as non-root this value has to be greater than 1024.
IHS System Group	no default	optional	The group that owns and runs the Web server instances and the plug-in directories. If the system group account does not already exist the account will be created on the target machine.
IHS System Password	no default	optional	The password for the user that owns and runs the Web server instances and the plug-in directories. This password will be used when creating the system user.
IHS System User	no default	optional	The user that owns and runs the Web server instances and the plug-in directories. If the system user account does not already exist the account will be created on the target machine.
IPaddr	see description	optional	IP address that binds the Web server to a specific IP address and ports. The default value is the IP address of `${Server.Name}`.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for IHS and Plugin (continued)

Parameter Name	Default Value	Required	Description
Plugin Install Root	see description	optional	Fully-qualified path where the WebSphere plug-in is installed. The default is based on IHS Install Location.
Response File	see description	optional	Fully-qualified path where the response file that this workflow creates will be located. This file is used to drive the installation. The default is `/tmp/installrespFile.xml`
SSL Key Database Password	no default	optional	The password that will be used to create the SSL key database used to store the Web server instance SSL certificates.

Chapter 3

Reference Information

This chapter contains the following information:

Topic	Description
WebSphere 8.0 and 8.5.x Product Documentation	Links to product documentation for the database products that these workflows support Links to the hardware and software requirements, as well as supported platforms for WebSphere 8.0 and 8.5.x,
HP DMA Documentation	Links to additional HP DMA documentation

WebSphere 8.0 and 8.5.x Product Documentation

For the current list of hardware and software requirements, as well as supported platforms for WebSphere 8.0 and 8.5.x, see:

http://www-01.ibm.com/support/docview.wss?uid=swg27006921

ForWebSphere 8.0 and 8.5.x product documentation, see:

http://pic.dhe.ibm.com/infocenter/wasinfo/v8r0/index.jsp

http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/index.jsp

For IBM Red Book resources for WebSphere 8.0 and 8.5.x, see:

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

HP DMA Documentation

For information about using the HP DMA web interface, see the *HP DMA User Guide*, the *HP DMA Administrator Guide*, and the *HP DMA Quick Start Tutorial*.

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

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

Chapter 4

Tips and Best Practices

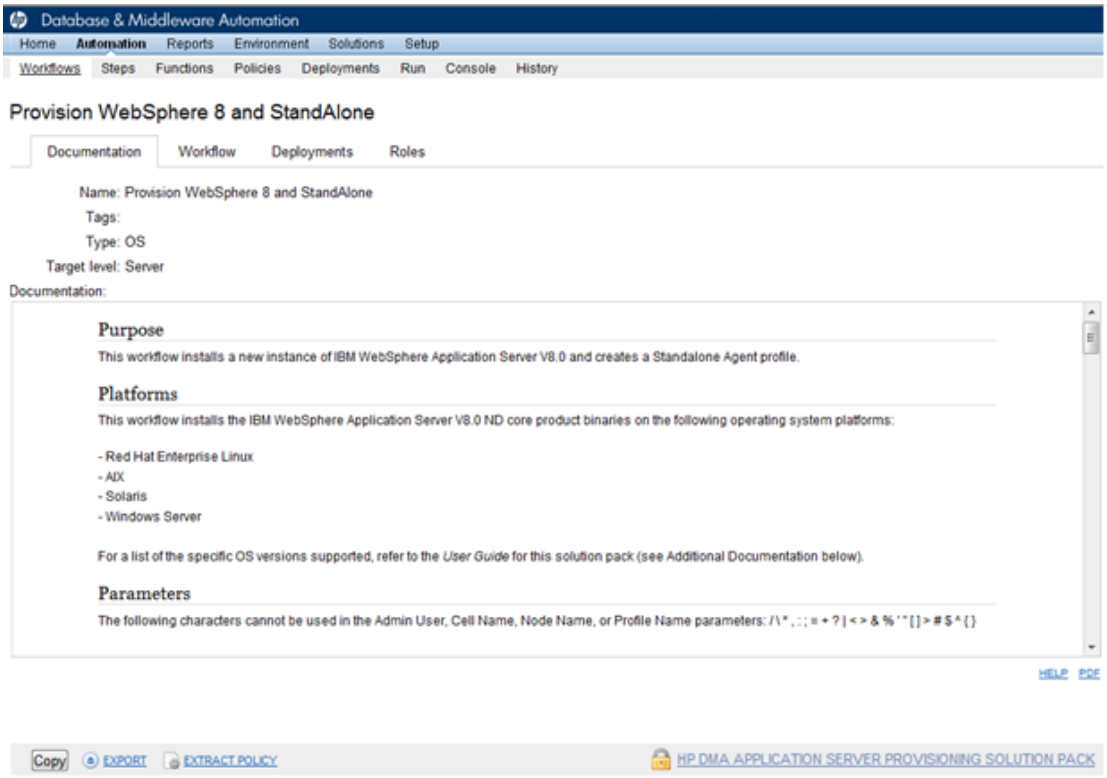
This portion of the document contains a collection of tips and best practices that will enable you to use HP DMA more effectively. It contains the following topics:

How this Solution is Organized

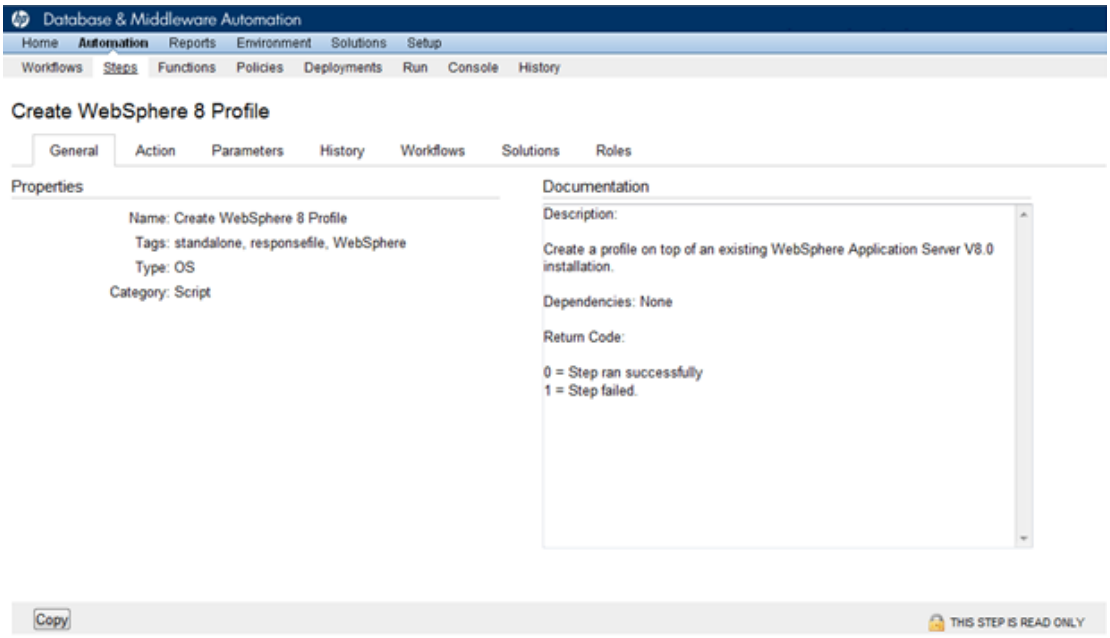
In HP DMA, a **workflow** executes a process —such as installing a software product or checking a database instance for compliance with a specific security benchmark.

A **solution pack** contains one or more related **workflow templates**.

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

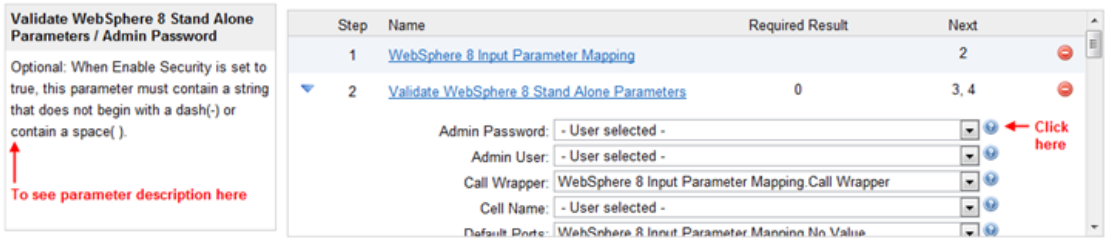


A workflow consist of a sequence of **steps**. Each step performs a very specific task. Each step includes a documentation panel that briefly describes its function. Steps can be shared among workflows.

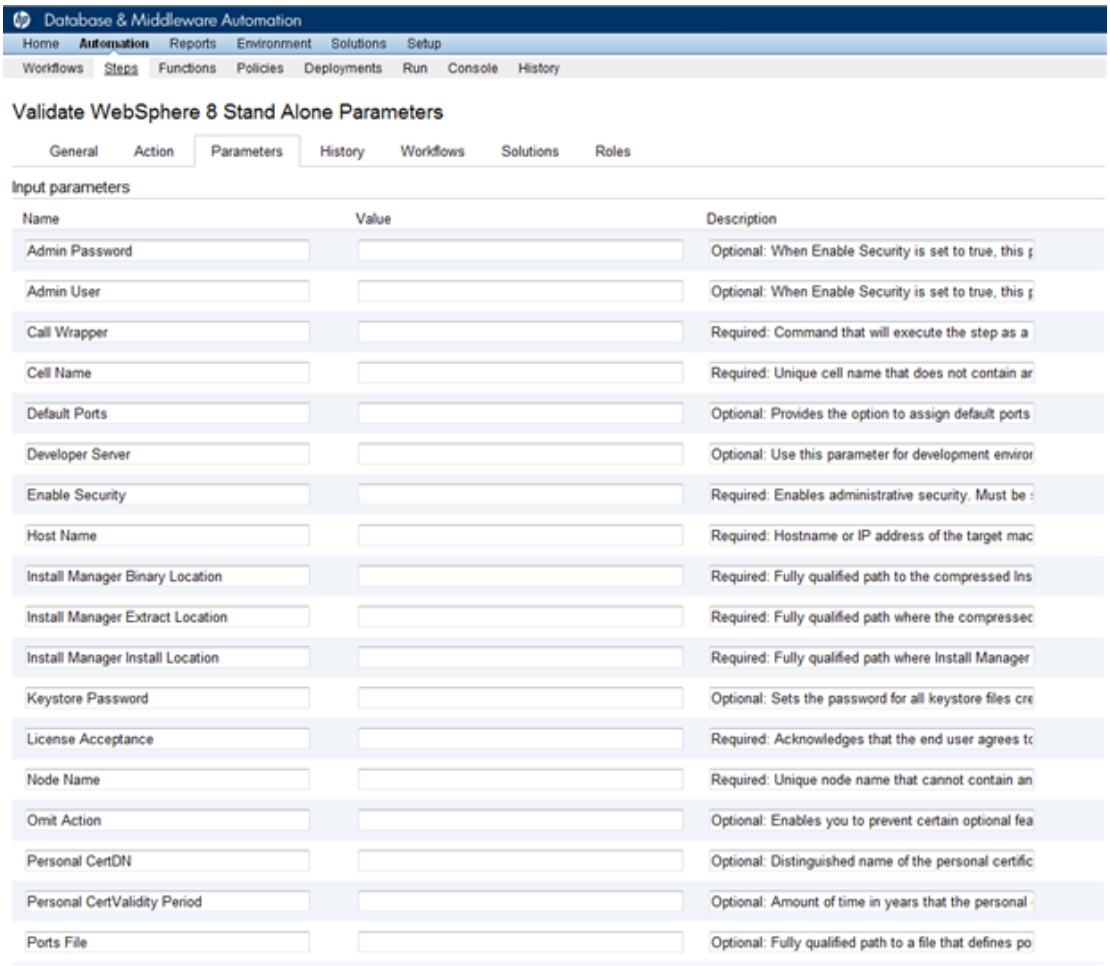


Steps can have input and output **parameters**. Output parameters from one step often serve as input parameters to another step.

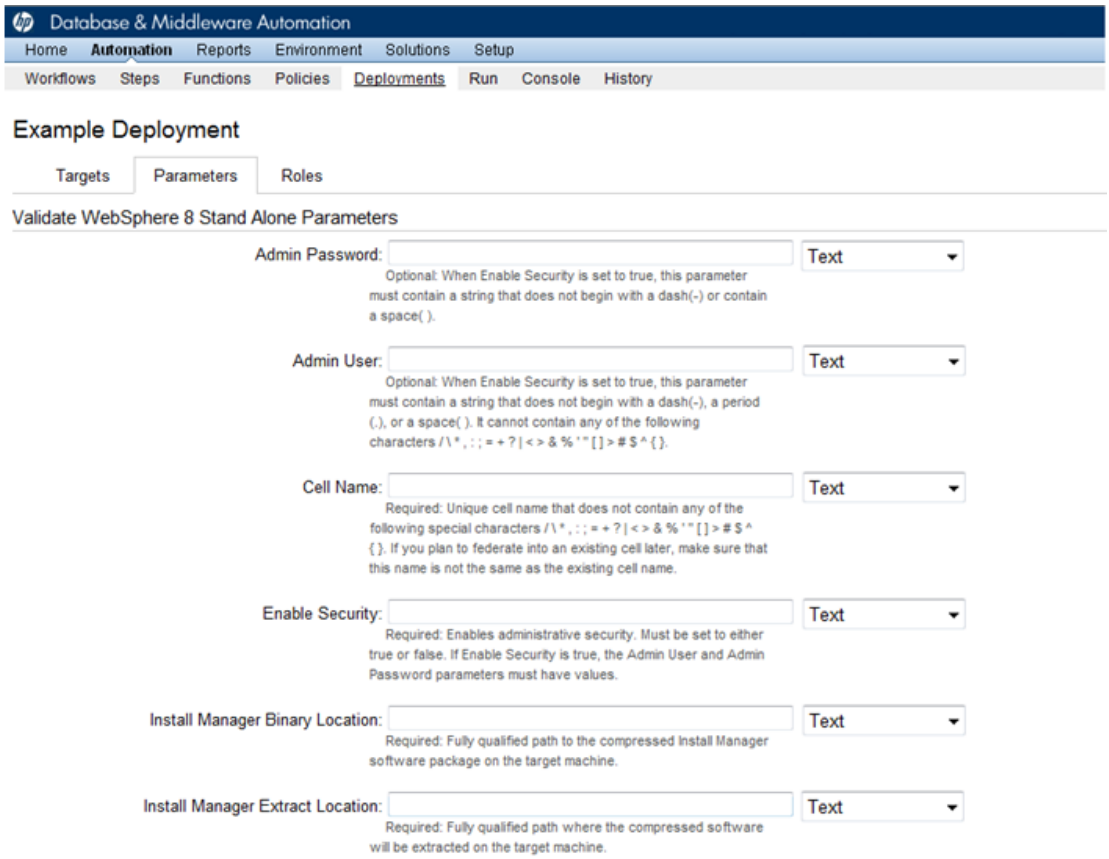
Parameter descriptions are displayed on the Workflow tab for each workflow.



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



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



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

Note: The workflow templates included in this solution pack are read-only and cannot be deployed. To use a workflow template, you must first create a copy of the template and then customize that copy for your environment (see the *HP DMA Quick Start Tutorial* for instructions).

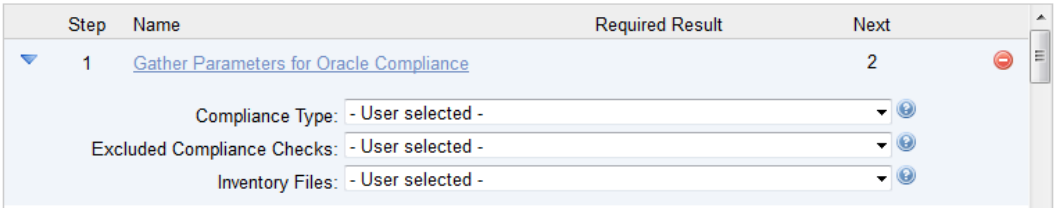
How to Expose Additional Workflow Parameters

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

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

To expose a hidden workflow parameter:

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



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

How to Use a Policy to Specify Parameter Values

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

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

To establish a policy, you can either Create a Policy or Extract a Policy from a workflow.

After you establish the policy, you must Reference the Policy in the Deployment.

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

Create a Policy

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

To create a policy that provides parameter values:

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

   b. In the text box to the left of the Add button, specify the name of the attribute.

      For your convenience, this name should be similar to the parameter name used in the pertinent workflow (or workflows).

   c. Click **Add**.

   d. In the new text box to the right of the attribute's name, enter a value for this attribute.

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

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

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

Extract a Policy

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

To extract a policy:

1. Go to Automation > Workflows.
2. Select the Workflow that you want to work with.
3. Click the Extract Policy link at the bottom of the screen.
4. Specify values for each attribute listed.
5. *Optional:* Remove any attributes that you do not want to use.
6. *Optional:* Add any new attributes that you want to use.
7. *Optional:* On the Roles tab, select the Read box for any users or user groups that you want to be able to use this policy to provide parameter values in a Deployment. Select the Write box for any users or groups that you want to be able to modify this Policy (add or remove attributes).
8. Click **Save**.

Reference the Policy in the Deployment

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

To reference policy attributes in a deployment:

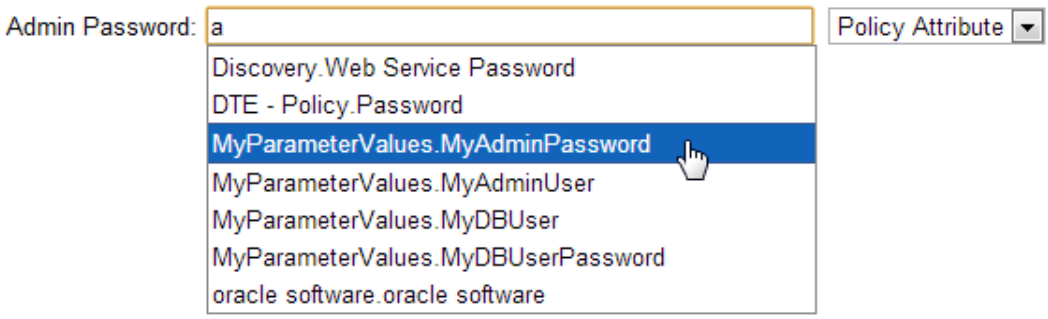
1. Create or access the deployment.

   See “Deployments” in the *HP DMA User Guide* for details.

2. On the Parameters tab, perform the following steps for each parameter whose value you want to provide by referencing a policy attribute:

   a. In the drop-down menu for that parameter, select **Policy Attribute**.

   b. In the text box for that parameter, type any character. A drop-down list of policy attributes appears. For example:



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

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

How to Import a File into the Software Repository

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

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

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

To import a file into the HP SA Software Library:

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

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

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

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

Chapter 5

Troubleshooting

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

- Target Type below
- User Permissions and Related Requirements below
- Discovery in HP DMA on next page

Target Type

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

User Permissions and Related Requirements

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

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

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

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

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

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

Discovery in HP DMA

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

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

Glossary

A

automation items

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

B

bridged execution

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

C

capability

Capabilities are collections of related privileges. There are three capabilities defined in HP DMA. Login Access capability enables a user to log in to the web interface. This capability does not guarantee that this user can view any organizations or automation items—permissions are required to access those items. Workflow Creator capability enables a user to create new workflows and make copies of other workflows. Administrator capability enables a user to perform any action and view all organizations. If you have Administrator capability, you do not need Workflow Creator capability. The Administrator can assign any of these capabilities to one or more roles registered roles.

connector

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

cross-platform

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

custom field

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

D

deployment

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

F

function

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

I

input parameters

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

M

mapping

An input parameter is said to be "mapped" when it's value is linked to an output parameter from a previous step in the workflow or to a metadata field. Mapped parameters are not visible on the Deployment page. You can "unmap" a parameter by specifying - User Selected - in the workflow editor. This parameter will then become visible on the Deployment page.

O

organization

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

P

parameters

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

policy

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

R

raw devices

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

role

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

S

smart group

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

software repository

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

solution pack

A solution pack contains one or more related workflow templates. These templates are read-only and cannot be deployed. To run one of the workflows included in a solution pack, you must first create a deployable copy of that template and then customize that copy for your environment. Solution packs are organized by function - for example: database patching or application server provisioning.

steps

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

T

target instance

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

W

workflow

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

workflow editor

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

workflow templates

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