HP Database and Middleware Automation

Software Version: 10.30

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

WebSphere 7 Provisioning

Document Release Date: May 2015

Software Release Date: May 2015

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

UNIX® is a registered trademark of The Open Group.

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

Documentation Updates

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

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to: **https://softwaresupport.hp.com**

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: **https://hpp12.passport.hp.com/hppcf/createuser.do**

Or click the **Register** link at the top of the HP Software Support 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
Title Page Legal Notices	10.01	Updated version number, software release date, document release date, and copyright date range.
WebSphere 7 Provisioning Quick Start	10.01	Updated from 10.00 to 10.01.

Document Changes, continued

Chapter	Version	Changes
Workflow Details	10.01	Merged 9.10 and 10.00 user guides—included all workflows in new format. Added disclaimer that the component workflow steps cannot be run in a proxy situation.
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.
Title Page Legal Notices	10.20	Updated version number, software release date, document release date, and copyright date range.
WebSphere 7 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*.
Title Page Legal Notices Entire guide	10.21	Updated version number, software release date, document release date, and copyright date range. Updated document template.
Title Page Legal Notices	10.22	Updated version number, software release date, document release date, and copyright date range.
Deprecated WebSphere 7 Provisioning Workflows Workflow Details	10.22	Deprecated the WebSphere 7 master workflows.
Title Page Legal Notices Entire guide	10.30	Updated version number, software release date, document release date, and copyright date range. Updated to new documentation template.

Support

Visit the HP Software Support Online web site at: **https://softwaresupport.hp.com**

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:

https://hpp12.passport.hp.com/hppcf/createuser.do

To find more information about access levels, go to:

https://softwaresupport.hp.com/web/softwaresupport/access-levels

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.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 version 7 (WebSphere 7).
- Engineers who are implementing—or planning to implement—HP Database and Middleware Automation (HP DMA)

To use this solution, you should be familiar with WebSphere 7 and its requirements (see links to the WebSphere 7 Product Documentation on page 109).

Document Map

The following table shows you how to navigate this guide:

Topic	Description
The WebSphere 7 Provisioning Solution	General information about this solution, including what it contains and what it does.
Workflow Details	Information about the WebSphere 7 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 7 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 122.

Chapter 1: The WebSphere 7 Provisioning Solution

The WebSphere 7 provisioning solution provides workflows that you can use to provision many features of a WebSphere 7 environment. These workflows enable you to:

- Install the WebSphere 7 Base core binaries and provision WebSphere 7
- Create a WebSphere 7 stand-alone profile
- Create a WebSphere 7 Deployment Manager
- Create and federate a WebSphere 7 custom node profile
- Create either a stand-alone or custom profile on an existing WebSphere 7 installation
- Provision an IBM HTTP Server 7
- Create a WebSphere Application Server plug-in

The above workflows (components) can be tied together into more powerful master workflows (composites). The composite workflows are Provision IBM HTTP Server and WebSphere 7 Two Node Cell, Add WebSphere 7 Node to Existing Cell, and Provision HTTP Server and WebSphere 7 StandAlone Profile. The WebSphere 7 provisioning composite workflows enable you to:

- Create a WebSphere 7 Network Deployment cell
- Add additional WebSphere 7 nodes to an existing Network Deployment cell
- Create a web server tier
- Create an application tier
- Create an application cluster that is both vertically and horizontally clustered
- Create a replication cluster that is horizontally clustered
- Create unmanaged nodes and web server objects
- Create remote management of IBM HTTP Server 7 web servers

By consistently using the tools provided in this solution, you can quickly, efficiently, and accurately set up your WebSphere 7 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 7 provisioning workflows:

Workflow Name	Purpose
Provision WebSphere 7 StandAlone Profile	Use this workflow to install the WebSphere 7 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 7 and Deployment Manager	Use this workflow to install the WebSphere 7 Base core binaries and, optionally, create a Deployment Manager profile. A Deployment Manager is the administration point for a cell that contains multiple application servers. This type of profile is appropriate for distributed application server environments.
Provision WebSphere 7 and Custom Node	Use this workflow to install the WebSphere 7 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.
Create StandAlone from Existing WebSphere 7 Install	Use this workflow to create a stand-alone profile on an existing WebSphere 7 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.
Create Custom Node from Existing WebSphere 7 Install	Use this workflow to create a custom profile on an existing WebSphere 7 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 7 and Plug-In	Use this workflow to install IBM HTTP Server for WebSphere Application Server V7.0 and, optionally, install its WebSphere Application Server Plug-In.

Deprecated WebSphere 7 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 7 StandAlone Profile	Use this workflow to install the WebSphere 7 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 IBM HTTP Server and WebSphere 7 Two Node Cell	Use this workflow to provision a web server tier with two web servers and an application tier with a two node Network Deployment cell on a Red Hat Enterprise Linux platform. Each node is an IBM WebSphere Application Server version 7 server. The Network Deployment cell contains an application cluster and a replication cluster.
Add WebSphere 7 Node to Existing Cell	Use this workflow in conjunction with the Provision IBM HTTP Server and WebSphere 7 Two Node Cell workflow to expand the Network Deployment cell by one node (up to a maximum of 10 nodes in the cell).

Tip: Documentation for deprecated workflows is available in the *HP DMA WebSphere 7 Provisioning User Guide* for HP DMA version 10.21. This document is available on the HP Software Support web site: https://softwaresupport.hp.com/

Supported Products and Platforms

Most WebSphere 7 provisioning workflows are supported on Red Hat Enterprise Linux, Solaris, AIX, HP-UX, and Windows platforms.

Operating Systems

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

https://softwaresupport.hp.com/

Hardware Requirements

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

HP Software Requirements

The latest HP DMA solution packs require the latest HP DMA platform. To use the latest solution packs, update the HP DMA platform. HP DMA 10.30 solution packs are supported on HP DMA 10.30 (and later).

WebSphere 7 Hardware and Software Requirements

For IBM WebSphere 7requirements, see WebSphere 7 Product Documentation on page 109.

Prerequisites

The following prerequisites must be satisfied before you can run the WebSphere 7 provisioning workflows in this solution pack:

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

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 libXp-1.0.0-8 compat-libstdc++- 296-2.96-138 rpm-build- 4.4.2-37.el5

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.

Chapter 2: Workflow Details

The Application Server Provisioning solution pack contains the following WebSphere 7 provisioning workflows. You can run these workflows ad-hoc for custom WebSphere 7 installations or create reusable deployments to standardize WebSphere 7 installations in your environment.

Workflow Name	Purpose
Provision WebSphere 7 StandAlone Profile	Use this workflow to install the WebSphere 7 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 7 and Deployment Manager	Use this workflow to install the WebSphere 7 Base core binaries and, optionally, create a Deployment Manager profile. A Deployment Manager is the administration point for a cell that contains multiple application servers. This type of profile is appropriate for distributed application server environments.
Provision WebSphere 7 and Custom Node	Use this workflow to install the WebSphere 7 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.
Create StandAlone from Existing WebSphere 7 Install	Use this workflow to create a stand-alone profile on an existing WebSphere 7 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.
Create Custom Node from Existing WebSphere 7 Install	Use this workflow to create a custom profile on an existing WebSphere 7 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 7 and Plug-In	Use this workflow to install IBM HTTP Server for WebSphere Application Server V7.0 and, optionally, install its WebSphere Application Server Plug-In.

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 14).
- 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 7 StandAlone Profile

Use this workflow to install the WebSphere 7 Base core binaries and, optionally, create a stand-alone profile.

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

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

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

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere 7 StandAlone Profile workflow:

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

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 libXp-1.0.0-8 compat-libstdc++- 296-2.96-138 rpm-build- 4.4.2-37.el5

   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 7, refer to the WebSphere 7 Product Documentation on page 109.

How this Workflow Works

This topic contains the following information about the Provision WebSphere 7 StandAlone Profile workflow:

Overview

This workflow does the following things in the order shown:

1. Prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebSphere 7 environment
2. Checks the documented library requirements, files system space requirements, and temporary space requirements
3. Checks whether the WebSphere 7 binaries are available—if not, they will be downloaded from the software repository—and extracts the binary files from the compressed archive
4. Creates a new response file
5. Provisions IBM WebSphere Application Server version 7 on a target machine
6. Creates a stand-alone profile
7. Starts the stand-alone WebSphere Application Server V7.0

Validation Checks Performed

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

The workflow first performs the following parameter checks:

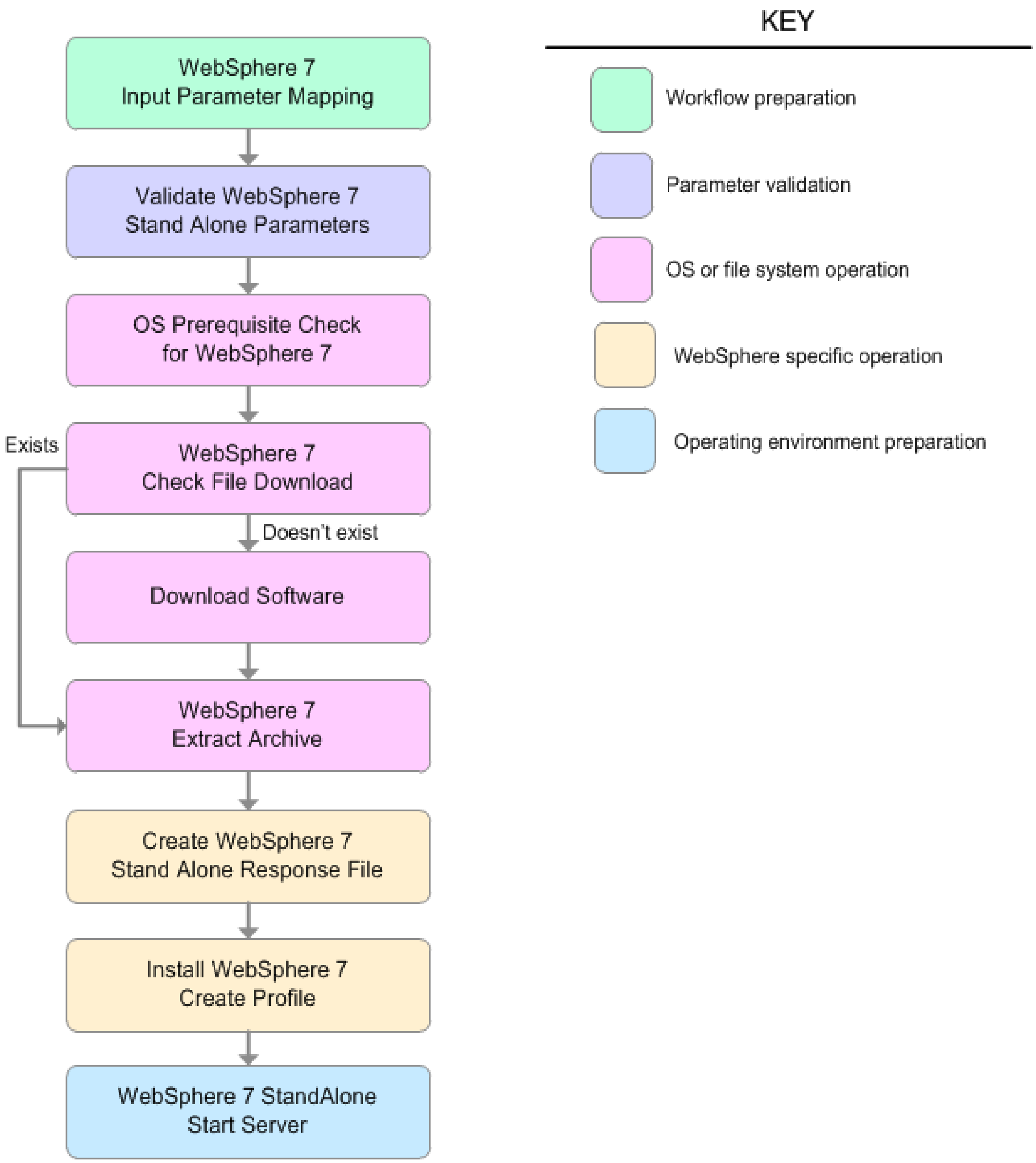
1. Binary Archive is specified. It either exists or can be created successfully.
2. Extract Path and Install Location either exist or can be created successfully.
3. Admin User (if specified) does not begin with a period (.), hyphen (-) or space. It does not contain any of the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
4. Admin Password (if specified) does not begin with a hyphen (-) or contain a space.
5. Cell Name, Node Name, Profile Name, and Server Name are specified. They do not contain the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { } or space. They do not begin with a period.
6. Host Name is specified.
7. Default Ports and Developer Server (if specified) are true or false.
8. Enable Security is true or false. If Enable Security is true, Admin Password and Admin User are specified.
9. License Acceptance is true.
10. Omit Action (if specified) is defaultAppDeployAndConfig, or deployAdminConsole.
11. Ports File (if specified) exists and Validate Ports is true or false.
12. Starting Port (if specified) is an integer.
13. If the operating system is Windows, Windows Admin User and Windows Admin Password are specified.
14. Profile Path and Response File are specified.
15. Profile Type is standAlone.

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 19).
2. Sufficient disk space is available to install WebSphere 7.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

The Provision WebSphere 7 StandAlone Profile workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.


KEY
Workflow preparation
Parameter validation
OS or file system operation
WebSphere specific operation
Operating environment preparation
WebSphere 7 Input Parameter Mapping
Validate WebSphere 7 Stand Alone Parameters
OS Prerequisite Check for WebSphere 7
WebSphere 7 Check File Download
Exists
Doesn't exist
Download Software
WebSphere 7 Extract Archive
Create WebSphere 7 Stand Alone Response File
Install WebSphere 7 Create Profile
WebSphere 7 StandAlone Start Server

Steps Used in the Provision WebSphere 7 StandAlone Profile Workflow

Workflow Step	Description
WebSphere 7 Input Parameter Mapping	This step creates the call wrapper—the command that executes the step as a specific user—and allows certain parameters to be hidden or exposed.
Validate WebSphere 7 Stand Alone Parameters	This step prepares and validates the parameters needed to install WebSphere Application Server V7.0 and create a stand-alone profile.
OS Prerequisite Check for WebSphere 7	This step checks the documented library requirements, files system space requirements, and temporary space requirements for WebSphere Application Server V7.0.
WebSphere 7 Check File Download	This step checks for the existence of a file before downloading it from the software repository: • Checks if a file exists in the expected location. • If the file is not in the expected location, the file is added to a list of files that need to be downloaded.
Download Software	This step downloads a list of files to a specified location on the target server.
WebSphere 7 Extract Archive	This step checks that the archive file exists and then, based on the archive extension, extracts the archive to the specified directory.
Create WebSphere 7 Stand Alone Response File	This step creates a new response file for installing a new instance of WebSphere Application Server V7.0 and creating a stand-alone profile.
Install WebSphere 7 Create Profile	This step installs a new instance of WebSphere Application Server V7.0 using the `install -options <responsefile> silent` option and then creates a profile.
WebSphere 7 StandAlone Start Server	This step starts the stand-alone WebSphere Application Server V7.0.

For parameter descriptions and defaults, see Parameters for Provision WebSphere 7 StandAlone Profile on page 30.

How to Run this Workflow

The following instructions show you how to customize and run the Provision WebSphere 7 StandAlone Profile in your environment.

Tip: For detailed instructions to run HP DMA workflows—using the 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 7 StandAlone Profile on page 30.

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 7 StandAlone Profile 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:

Input Parameters for Validate WebSphere 7 Stand Alone Parameters

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Binary Archive	no default	required	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.

Input Parameters for Validate WebSphere 7 Stand Alone Parameters, continued

Parameter Name	Default Value	Required	Description
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Extract Dir	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Profile Path	no default	required	Fully qualifed path to the stand-alone profile. For example: `/opt/IBM/WebSphere/AppServer/profiles/AppServer1`
Profile Type	standAlone	required	Because this workflow creates a stand-alone profile, the value is standAlone.
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Name	no default	required	Name of the application server that will be created under the profile.
Windows Admin Password	no default	required	The Windows Administrator password. Required for Windows.

Input Parameters for Validate WebSphere 7 Stand Alone Parameters, continued

Parameter Name	Default Value	Required	Description
Windows Admin 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 7 StandAlone Profile on page 30 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 116).

3. In the workflow editor, expose any additional parameters that you need (see How to Expose Additional Workflow Parameters on page 115). 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.

Optional: if you want to further verify the results, 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 7 is installed. This is the path that you specified in the WebSphere Install Location parameter.
2. Validate that stand-alone 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/SERVER_NAME` directory, and tail the `SystemOut.log` file. Look for the following line:

      ```
      Server SERVER_NAME open for e-business
      ```

      Here, `SERVER_NAME` is the name of the application server that you just created. This is the name that you specified in the Server Name parameter.

Sample Scenario

This topic shows you typical parameter values used for the Provision WebSphere 7 StandAlone Profile workflow.

New WebSphere 7 install with stand-alone profile

Input Parameters for Validate WebSphere 7 Stand Alone Parameters

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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Binary Archive	see description	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`
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.
Extract Dir	`/opt/IBM/wasv7`	Fully qualified path where the compressed software will be extracted on the target machine.
Install Location	see description	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	DevStandAlone1Node	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.

Input Parameters for Validate WebSphere 7 Stand Alone Parameters, continued

Parameter Name	Example Value	Description
Profile Name	StandAlone1	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Profile Path	see description	Fully qualifed path to the stand-alone profile. For example: `/opt/IBM/WebSphere/AppServer/profiles/AppServer1`
Profile Type	standAlone	Because this workflow creates a stand-alone profile, the value is standAlone.
Response File	`/tmp/serverrsp`	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Name	Server1	Name of the application server that will be created under the profile.

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 116).

Parameters for Provision WebSphere 7 StandAlone Profile

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment (see How to Expose Additional Workflow Parameters on page 115). For some parameters, if you do not specify a value for a parameter, a default value is assigned.

> **Note:** Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Parameters Defined in this Step: Validate WebSphere 7 Stand Alone Parameters

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period (.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Binary Archive	no default	required	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. For UNIX targets, the default is: `/opt/hp/dma/client/jython.sh` running as root For Windows targets, the default is: `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.

Parameters Defined in this Step: Validate WebSphere 7 Stand Alone Parameters, continued

Parameter Name	Default Value	Required	Description
Default Ports	false	optional	Provides the option to assign default ports to a profile. Valid values are true or false. If true, the WebSphere Application Server default ports will be used, and the Ports File and Starting Port parameters should not have values. If false, the workflow will increment the default port until it finds a free port. The default value is false.
Developer Server	no default	optional	Use this parameter for development environments only to help with start up time. Valid value is true. Do not use in production environments.
Enable Security	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.
Extract Dir	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Omit Action	no default	optional	Enables you to prevent certain optional features from being installed. Valid values are deployAdminConsole or defaultAppDeployAndConfig. You may only specify one of these options.

Parameters Defined in this Step: Validate WebSphere 7 Stand Alone Parameters, continued

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

Parameters Defined in this Step: Validate WebSphere 7 Stand Alone Parameters, continued

Parameter Name	Default Value	Required	Description
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.
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.
Windows Admin Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Admin User	no default	required	This is the Windows Administrator user. Required for Windows.

Provision WebSphere 7 and Deployment Manager

Use this workflow to install the WebSphere 7 Base core binaries and, optionally, create a Deployment Manager profile.

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

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

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

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere 7 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 WebSphere 7 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server version 7 on 64-bit Red Hat Linux:

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 libXp-1.0.0-8 compat-libstdc++- 296-2.96-138 rpm-build- 4.4.2-37.el5

   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 7, refer to the WebSphere 7 Product Documentation on page 109.

How this Workflow Works

This topic contains the following information about the Provision WebSphere 7 and Deployment Manager workflow:

Overview

This workflow does the following things in the order shown:

1. Prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebSphere 7 environment
2. Checks the documented library requirements, files system space requirements, and temporary space requirements
3. Checks whether the WebSphere 7 binaries are available—if not, they will be downloaded from the software repository—and extracts the binary files from the compressed archive
4. Creates a new response file
5. Provisions IBM WebSphere Application Server version 7 on a target machine
6. Creates a Deployment Manager profile
7. Starts the WebSphere 7 Deployment Manager application server

Validation Checks Performed

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

The workflow first performs the following parameter checks:

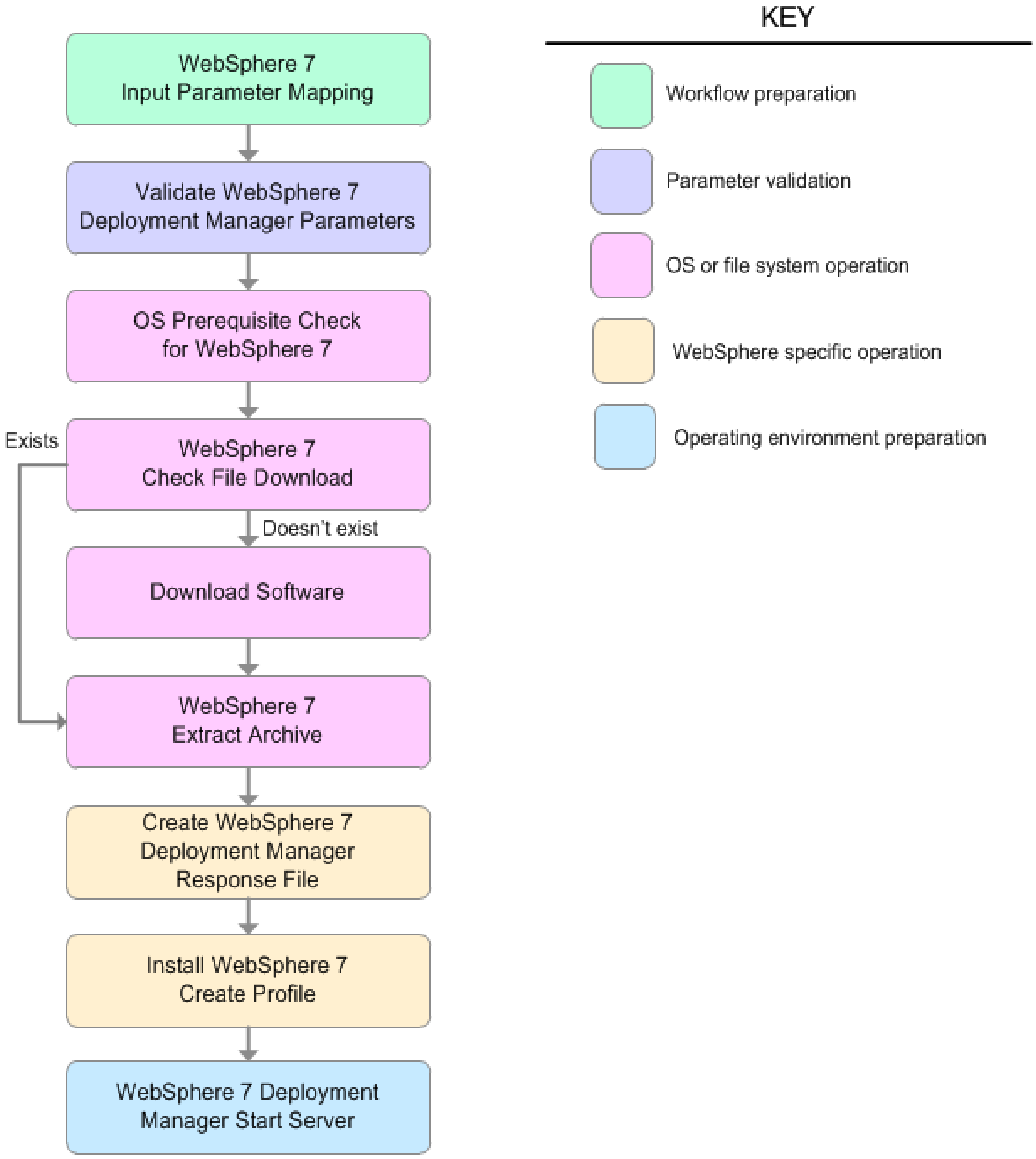
1. Admin User (if specified) does not begin with a period (.), hyphen (-) or space. It does not contain any of the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
2. Admin Password (if specified) does not begin with a hyphen (-) or contain a space.
3. Cell Name, Node Name, and Profile Name are specified. They do not contain the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { } or space. They do not begin with a period.
4. Host Name is specified.
5. Default Ports (if specified) is true or false.
6. Enable Security is true or false. If Enable Security is true, Admin Password and Admin User are specified.
7. Omit Action (if specified) is defaultAppDeployAndConfig, or deployAdminConsole.
8. Ports File (if specified) exists and Validate Ports is true or false.
9. Starting Port (if specified) is an integer.
10. If the operating system is Windows, Windows Admin User and Windows Admin Password are specified.
11. License Acceptance is true.
12. Binary Archive is specified. It either exists or can be created successfully.
13. Extract Path and Install Location either exist or can be created successfully.
14. Profile Path and Response File are specified.
15. Server Type is DEPLOYMENT_MANAGER.
16. Profile Type is management.

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 35).
2. Sufficient disk space is available to install WebSphere 7.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

The Provision WebSphere 7 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.



Steps Used in the Provision WebSphere 7 and Deployment Manager Workflow

Workflow Step	Description
WebSphere 7 Input Parameter Mapping	This step creates the call wrapper—the command that executes the step as a specific user—and allows certain parameters to be hidden or exposed.
Validate WebSphere 7 Deployment Manager Parameters	This step prepares and validates the parameters needed to install WebSphere Application Server V7.0 and create a Deployment Manager profile.
OS Prerequisite Check for WebSphere 7	This step checks the documented library requirements, files system space requirements, and temporary space requirements for WebSphere Application Server V7.0.
WebSphere 7 Check File Download	This step checks for the existence of a file before downloading it from the software repository: • Checks if a file exists in the expected location. • If the file is not in the expected location, the file is added to a list of files that need to be downloaded.
Download Software	This step downloads a list of files to a specified location on the target server.
WebSphere 7 Extract Archive	This step checks that the archive file exists and then, based on the archive extension, extracts the archive to the specified directory.
Create WebSphere 7 Deployment Manager Response File	This step creates a new response file for installing a new instance of WebSphere Application Server V7.0 and creating a Deployment Manager profile.
Install WebSphere 7 Create Profile	This step installs a new instance of WebSphere Application Server V7.0 using the `install -options <responsefile> silent` option and then creates a profile.
WebSphere 7 Deployment Manager Start Server	This step starts the WebSphere 7 Deployment Manager application server.

For parameter descriptions and defaults, see Parameters for Provision WebSphere 7 and Deployment Manager on page 46.

How to Run this Workflow

The following instructions show you how to customize and run the Provision WebSphere 7 and Deployment Manager workflow in your environment.

> **Tip:** For detailed instructions to run HP DMA workflows—using the 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 7 and Deployment Manager on page 46.

> **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 7 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:

Input Parameters for Validate WebSphere 7 Deployment Manager Parameters

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Binary Archive	no default	required	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.

Input Parameters for Validate WebSphere 7 Deployment Manager Parameters, continued

Parameter Name	Default Value	Required	Description
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Extract Dir	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Profile Path	no default	required	Fully qualifed path to the Deployment Manager profile. For example: `/opt/IBM/WebSphere/AppServer/ profiles/ProdDmgr`
Profile Type	management	required	Because this workflow creates a Deployment Manager profile, the value must be management.
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Type	DEPLOYMENT_MANAGER	required	The type of management profile. The value is DEPLOYMENT_MANAGER for a deployment manager server.

Input Parameters for Validate WebSphere 7 Deployment Manager Parameters, continued

Parameter Name	Default Value	Required	Description
Windows Admin Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Admin 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 7 and Deployment Manager on page 46 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 116).

3. In the workflow editor, expose any additional parameters that you need (see How to Expose Additional Workflow Parameters on page 115). 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.

Optional: if you want to further verify the results, 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 7 is installed. This is the path that you specified in the WebSphere Install Location parameter.

2. Validate that the Deployment Manager 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/dmgr` directory, and tail the `SystemOut.log` file. Look for the following line:

      ```
      Server dmgr open for e-business
      ```

Sample Scenario

This topic shows you typical parameter values used for the Provision WebSphere 7 and Deployment Manager workflow.

New WebSphere 7 install with Deployment Manager profile

Input Parameters for Validate WebSphere 7 Deployment Manager Parameters

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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Binary Archive	see description	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`
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.
Extract Dir	`/opt/IBM/wasv7`	Fully qualified path where the compressed software will be extracted on the target machine.
Install Location	see description	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
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	no default	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	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.

Input Parameters for Validate WebSphere 7 Deployment Manager Parameters, continued

Parameter Name	Example Value	Description
Profile Path	no default	Fully qualifed path to the Deployment Manager profile. For example: `/opt/IBM/WebSphere/AppServer/profiles/ProdDmgr`
Profile Type	management	Because this workflow creates a Deployment Manager profile, the value must be management.
Response File	`/tmp/serverrsp`	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Type	DEPLOYMENT_ MANAGER	The type of management profile. The value is DEPLOYMENT_ MANAGER for a deployment manager server.

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 116).

Parameters for Provision WebSphere 7 and Deployment Manager

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment (see How to Expose Additional Workflow Parameters on page 115). For some parameters, if you do not specify a value for a parameter, a default value is assigned.

> **Note:** Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Parameters Defined in this Step: Validate WebSphere 7 Deployment Manager Parameters

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash (-) or contain a space( ).
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash (-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Binary Archive	no default	required	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. For UNIX targets, the default is: `/opt/hp/dma/client/jython.sh` running as root For Windows targets, the default is: `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.

Parameters Defined in this Step: Validate WebSphere 7 Deployment Manager Parameters, continued

Parameter Name	Default Value	Required	Description
Default Ports	false	optional	Provides the option to assign default ports to a profile. Valid values are true or false. If true, the WebSphere Application Server default ports will be used, and the Ports File and Starting Port parameters should not have values. If false, the workflow will increment the default port until it finds a free port. The default value is false.
Enable Security	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.
Extract Dir	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Omit Action	no default	optional	Enables you to prevent certain optional features from being installed. Valid values are deployAdminConsole or defaultAppDeployAndConfig. You may only specify one of these options.

Parameters Defined in this Step: Validate WebSphere 7 Deployment Manager Parameters, continued

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

Parameters Defined in this Step: Validate WebSphere 7 Deployment Manager Parameters, continued

Parameter Name	Default Value	Required	Description
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: CN=dmalab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.
Starting Port	no default	optional	Starting port number that the profile will use to generate and assign port values. Port values are assigned sequentially from the Starting Port. Do not specify this parameter if you specify Default Ports or Ports File.
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.
Windows Admin Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Admin User	no default	required	This is the Windows Administrator user. Required for Windows.

Provision WebSphere 7 and Custom Node

Use this workflow to install the WebSphere 7 Base core binaries and, optionally, create a custom profile.

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

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

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

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere 7 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 WebSphere 7 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server version 7 on 64-bit Red Hat Linux:

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 libXp-1.0.0-8 compat-libstdc++- 296-2.96-138 rpm-build- 4.4.2-37.el5

   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 7, refer to the WebSphere 7 Product Documentation on page 109.

How this Workflow Works

This topic contains the following information about the Provision WebSphere 7 and Custom Node workflow:

Overview

This workflow does the following things in the order shown:

1. Prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebSphere 7 environment
2. Checks the documented library requirements, files system space requirements, and temporary space requirements
3. Checks whether the WebSphere 7 binaries are available—if not, they will be downloaded from the software repository—and extracts the binary files from the compressed archive
4. Creates a new response file
5. Provisions IBM WebSphere Application Server version 7 on a target machine
6. Creates a custom node profile
7. Optionally federates the custom managed node profile into a Deployment Manager

Validation Checks Performed

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

The workflow first performs the following parameter checks:

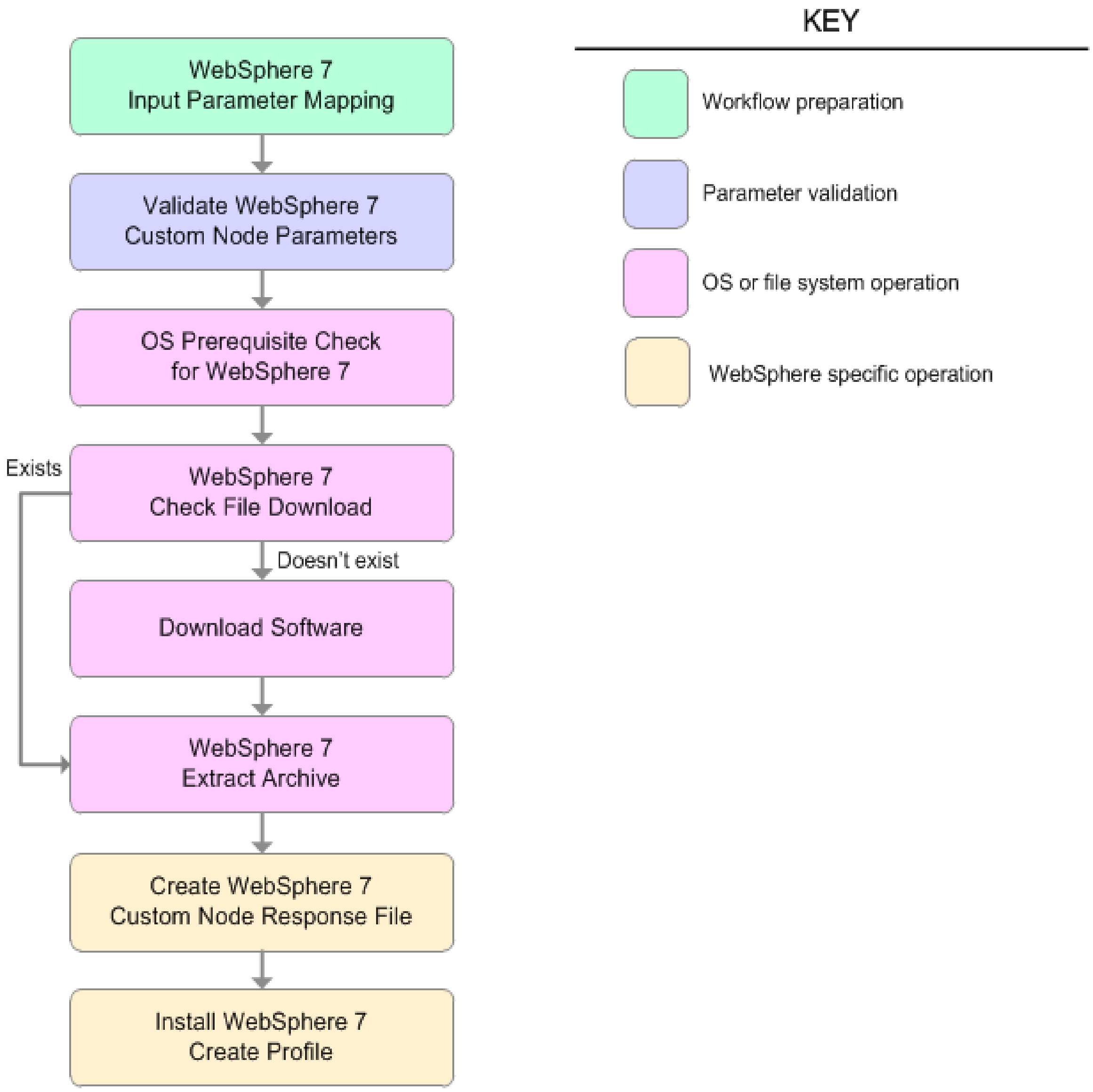
1. Enable Security is true or false. If Enable Security is true, Admin Password and Admin User are specified.
2. Admin User (if specified) does not begin with a period (.), hyphen (-) or space. It does not contain any of the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
3. Admin Password (if specified) does not begin with a hyphen (-) or contain a space.
4. Cell Name, Node Name, and Profile Name are specified. They do not contain the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { } or space. They do not begin with a period.
5. Host Name is specified.
6. Ports File (if specified) exists.
7. Federate Later (if specified) is true or false.
8. Dmgr HostName is specified.
9. Dmgr Port (if specified) is an integer.
10. License Acceptance is true.
11. Binary Archive is specified. It either exists or can be created successfully.
12. Extract Path and Install Location either exist or can be created successfully.
13. Profile Path and Response File are specified.
14. Profile Type is custom.

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 51).
2. Sufficient disk space is available to install WebSphere 7.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

The Provision WebSphere 7 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.


WebSphere 7 Input Parameter Mapping
Validate WebSphere 7 Custom Node Parameters
OS Prerequisite Check for WebSphere 7
Exists
WebSphere 7 Check File Download
Doesn't exist
Download Software
WebSphere 7 Extract Archive
Create WebSphere 7 Custom Node Response File
Install WebSphere 7 Create Profile
KEY
Workflow preparation
Parameter validation
OS or file system operation
WebSphere specific operation

Steps Used in the Provision WebSphere 7 and Custom Node Workflow

Workflow Step	Description
WebSphere 7 Input Parameter Mapping	This step creates the call wrapper—the command that executes the step as a specific user—and allows certain parameters to be hidden or exposed.
Validate WebSphere 7 Custom Node Parameters	This step prepares and validates the parameters needed to install WebSphere Application Server V7.0 and create a custom node profile.
OS Prerequisite Check for WebSphere 7	This step checks the documented library requirements, files system space requirements, and temporary space requirements for WebSphere Application Server V7.0.
WebSphere 7 Check File Download	This step checks for the existence of a file before downloading it from the software repository: • Checks if a file exists in the expected location. • If the file is not in the expected location, the file is added to a list of files that need to be downloaded.
Download Software	This step downloads a list of files to a specified location on the target server.
WebSphere 7 Extract Archive	This step checks that the archive file exists and then, based on the archive extension, extracts the archive to the specified directory.
Create WebSphere 7 Custom Node Response File	This step creates a new response file for installing a new instance of WebSphere Application Server V7.0 and creating a custom node profile.
Install WebSphere 7 Create Profile	This step installs a new instance of WebSphere Application Server V7.0 using the `install -options <responsefile> silent` option and then creates a profile.

For parameter descriptions and defaults, see Parameters for Provision WebSphere 7 and Custom Node on page 62.

How to Run this Workflow

The following instructions show you how to customize and run the Provision WebSphere 7 and Custom Node workflow in your environment.

Tip: For detailed instructions to run HP DMA workflows—using the 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 7 and Custom Node on page 62.

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 7 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:

Input Parameters for Validate WebSphere 7 Custom Node Parameters

Parameter Name	Default Value	Required	Description
Binary Archive	no default	required	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`
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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.

Input Parameters for Validate WebSphere 7 Custom Node Parameters, continued

Parameter Name	Default Value	Required	Description
Dmgr HostName	no default	optional	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). 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.
Extract Dir	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Federate Later	no default	required	If false, the new custom node will be federated by the workflow during profile creation. If true, you must federate it later manually by using the addNode command.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.

Input Parameters for Validate WebSphere 7 Custom Node Parameters, continued

Parameter Name	Default Value	Required	Description
Profile Path	no default	required	Fully qualifed path to the custom node profile. For example: `/opt/IBM/WebSphere/AppServer/profiles/ProdNode01`
Profile Type	custom	required	Because this workflow creates a Custom Node profile, the value must be custom.
Response File	no default	required	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 for Install WebSphere 7 Create Profile

Parameter Name	Default Value	Required	Description
Password	no default	required	The Windows Administrator password. Required for Windows.
Username	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 7 and Custom Node on page 62 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 116).

3. In the workflow editor, expose any additional parameters that you need (see How to Expose Additional Workflow Parameters on page 115). 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.

Optional: if you want to further verify the results, 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 7 is installed. This is the path that you specified in the WebSphere Install Location parameter.

2. Validate that the Deployment Manager 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/nodeagent` directory, and tail the `SystemOut.log` file. Look for the following line:

      ```
      Server nodeagent open for e-business
      ```

Sample Scenario

This topic shows you typical parameter values used for the Provision WebSphere 7 and Custom Node workflow.

New WebSphere 7 install with custom node profile

Input Parameters for Validate WebSphere 7 Custom Node Parameters

Parameter Name	Example Value	Description
Binary Archive	see description	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`
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	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.
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.

Input Parameters for Validate WebSphere 7 Custom Node Parameters, continued

Parameter Name	Example Value	Description
Extract Dir	`/opt/IBM/wasv7`	Fully qualified path where the compressed software will be extracted on the target machine.
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 Location	see description	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Profile Path	see description	Fully qualifed path to the custom node profile. For example: `/opt/IBM/WebSphere/AppServer/profiles/ProdNode01`
Profile Type	custom	Because this workflow creates a Custom Node profile, the value must be custom.
Response File	`/tmp/serverrsp`	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.

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 116).

Parameters for Provision WebSphere 7 and Custom Node

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment (see How to Expose Additional Workflow Parameters on page 115). For some parameters, if you do not specify a value for a parameter, a default value is assigned.

> **Note:** Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Parameters Defined in this Step: Validate WebSphere 7 Custom Node Parameters

Parameter Name	Default Value	Required	Description
Binary Archive	no default	required	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. For UNIX targets, the default is: `/opt/hp/dma/client/jython.sh` running as root For Windows targets, the default is: `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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.

Parameters Defined in this Step: Validate WebSphere 7 Custom Node Parameters, continued

Parameter Name	Default Value	Required	Description
Dmgr HostName	no default	optional	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). 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.
Extract Dir	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Federate Later	no default	required	If false, the new custom node will be federated by the workflow during profile creation. If true, you must federate it later manually by using the addNode command.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.

Parameters Defined in this Step: Validate WebSphere 7 Custom Node Parameters, continued

Parameter Name	Default Value	Required	Description
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmalab-example.com,OU=WAS7LabCell, OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_adminhost=9060). This option should be used with the Validate Ports option.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Profile Path	no default	required	Fully qualifed path to the custom node profile. For example: `/opt/IBM/WebSphere/AppServer/ profiles/ProdNode01`
Profile Type	no default	required	Because this workflow creates a Custom Node profile, the value must be custom.
Response File	no default	required	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.

Parameters Defined in this Step: Validate WebSphere 7 Custom Node Parameters, continued

Parameter Name	Default Value	Required	Description
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.

Additional Parameters Defined in this Step: Install WebSphere 7 Create Profile

Parameter Name	Default Value	Required	Description
Password	no default	required	The Windows Administrator password. Required for Windows.
Username	no default	required	This is the Windows Administrator user. Required for Windows.

Create StandAlone from Existing WebSphere 7 Install

Use this workflow to create a stand-alone profile on an existing WebSphere 7 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.

This workflow uses the built-in profile management functions (manageprofiles) in IBM WebSphere Application Server version 7 to create a stand-alone profile on top of an existing installation.

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

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 libXp-1.0.0-8 compat-libstdc++- 296-2.96-138 rpm-build- 4.4.2-37.el5

   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 7, refer to the WebSphere 7 Product Documentation on page 109.

How this Workflow Works

This topic contains the following information about the Create StandAlone from Existing WebSphere 7 Install workflow:

Overview

This workflow does the following things in the order shown:

1. Prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebSphere 7 environment
2. Creates a new response file
3. Creates a stand-alone profile
4. Starts the stand-alone WebSphere Application Server V7.0

Validation Checks Performed

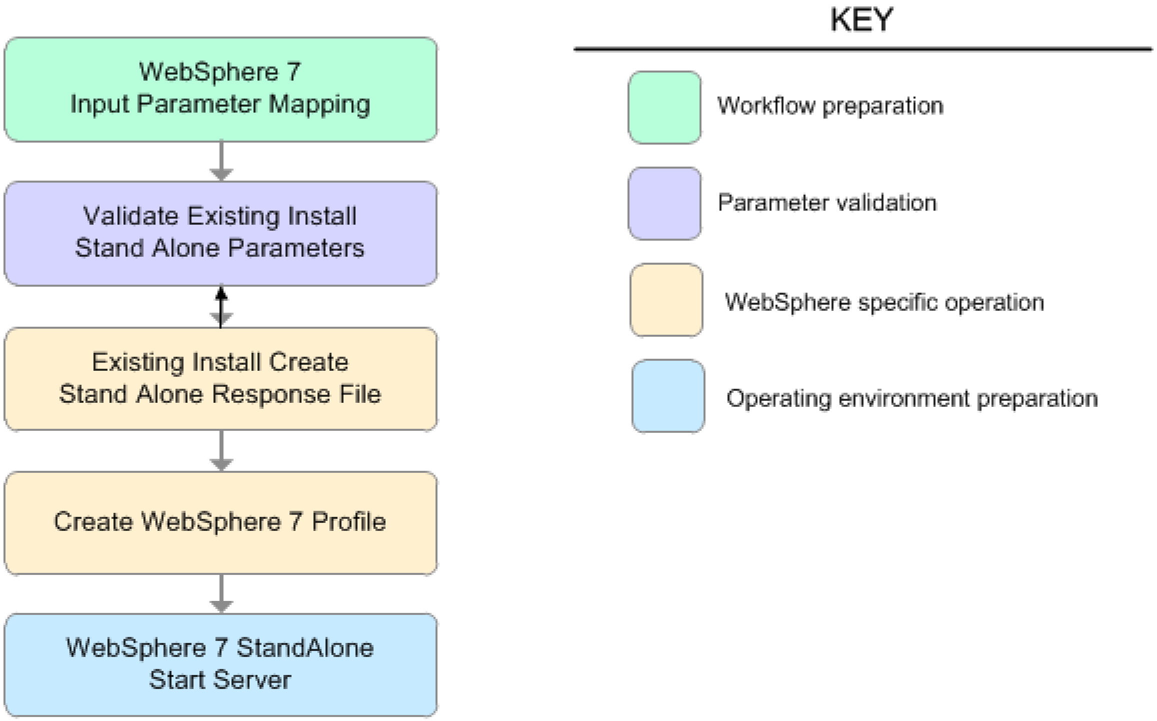
Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks for Red Hat Linux.

The workflow performs the following parameter checks:

1. Admin User (if specified) does not begin with a period (.), hyphen (-) or space. It does not contain any of the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
2. Admin Password (if specified) does not begin with a hyphen (-) or contain a space.
3. Cell Name, Node Name, Profile Name, and Server Name are specified. They do not contain the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { } or space. They do not begin with a period.
4. Host Name is specified.
5. Default Ports and Developer Server (if specified) are true or false.
6. Enable Security is true or false. If Enable Security is true, Admin Password and Admin User are specified.
7. Omit Action (if specified) is defaultAppDeployAndConfig, or deployAdminConsole.
8. Ports File (if specified) exists and Validate Ports is true or false.
9. Starting Port (if specified) is an integer.
10. Profile Path and Response File are specified.
11. Install Location points to a valid existing WebSphere 7 installation.

Steps Executed

The Create StandAlone from Existing WebSphere 7 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.



Steps Used in the Create StandAlone from Existing WebSphere 7 Install Workflow

Workflow Step	Description
WebSphere 7 Input Parameter Mapping	This step creates the call wrapper—the command that executes the step as a specific user—and allows certain parameters to be hidden or exposed.
Validate Existing Install Stand Alone Parameters	This step prepares and validates the parameters needed to create a stand-alone profile for an existing WebSphere Application Server V7.0 installation.
Existing Install Create Stand Alone Response File	This step creates a new response file to create a stand-alone profile on top of an existing WebSphere Application Server V7.0 installation.
Create WebSphere 7 Profile	This step creates a profile on top of an existing WebSphere Application Server V7.0 installation.
WebSphere 7 StandAlone Start Server	This step starts the stand-alone WebSphere Application Server V7.0.

How to Run this Workflow

The following instructions show you how to customize and run the Create StandAlone from Existing WebSphere 7 Install workflow in your environment.

Tip: For detailed instructions to run HP DMA workflows—using the 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 Create StandAlone from Existing WebSphere 7 Install on page 75

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

To customize and run the Create StandAlone from Existing WebSphere 7 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:

Input Parameters for Validate Existing Install Stand Alone Parameters

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period (.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
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.

Input Parameters for Validate Existing Install Stand Alone Parameters, continued

Parameter Name	Default Value	Required	Description
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Profile Path	no default	required	Fully qualifed path to the stand-alone profile. For example: `/opt/IBM/WebSphere/AppServer/profiles/AppServer1`
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Name	no default	required	Name of the application server that will be created under the profile.

Additional Input Parameters for Install WebSphere 7 Create Profile

Parameter Name	Default Value	Required	Description
Password	no default	required	The Windows Administrator password. Required for Windows.
Username	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 Create StandAlone from Existing WebSphere 7 Install on page 75 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 116).

3. In the workflow editor, expose any additional parameters that you need (see How to Expose Additional Workflow Parameters on page 115). 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.

Optional: if you want to further verify the results, 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 7 is installed. This is the path that you specified in the WebSphere Install Location parameter.
2. Validate that stand-alone 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/SERVER_NAME` directory, and tail the `SystemOut.log` file. Look for the following line:

      ```
      Server SERVER_NAME open for e-business
      ```

      Here, `SERVER_NAME` is the name of the application server that you just created. This is the name that you specified in the Server Name parameter.

Sample Scenario

This topic shows you typical parameter values used for the Create StandAlone from Existing WebSphere 7 Install workflow.

Stand-alone profile on Existing Install—Parameter Value Examples

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

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 Location	see description	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Profile Path	see description	Fully qualifed path to the stand-alone profile. For example: `/opt/IBM/WebSphere/AppServer/profiles/AppServer1`
Response File	`/tmp/serverrsp`	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Name	Server1	Name of the application server that will be created under the profile.

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 116).

Parameters for Create StandAlone from Existing WebSphere 7 Install

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment (see How to Expose Additional Workflow Parameters on page 115). For some parameters, if you do not specify a value for a parameter, a default value is assigned.

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

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

Parameters Defined in this Step: Validate Existing Install Stand Alone Parameters, continued

Parameter Name	Default Value	Required	Description
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Omit Action	no default	optional	Enables you to prevent certain optional features from being installed. Valid values are deployAdminConsole or defaultAppDeployAndConfig. You may only specify one of these options.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmalab-example.com,OU=WAS7LabCell, OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_adminhost=9060). This option should be used with the Validate Ports option.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.

Parameters Defined in this Step: Validate Existing Install Stand Alone Parameters, continued

Parameter Name	Default Value	Required	Description
Profile Path	no default	required	Fully qualifed path to the stand-alone profile. For example: `/opt/IBM/WebSphere/AppServer/profiles/AppServer1`
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Name	no default	required	Name of the application server that will be created under the profile.
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: CN=dmalab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.
Starting Port	no default	optional	Starting port number that the profile will use to generate and assign port values. Port values are assigned sequentially from the Starting Port. Do not specify this parameter if you specify Default Ports or Ports File.
Validate Ports	no default	optional	Indicates that the ports should be validated to ensure that they are not already in use. Valid values are true or false. You should use this option if you specify a Ports File.

Additional Parameters Defined in this Step: Create WebSphere 7 Profile

Parameter Name	Default Value	Required	Description
Password	no default	required	The Windows Administrator password. Required for Windows.
Username	no default	required	This is the Windows Administrator user. Required for Windows.

Note: Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Create Custom Node from Existing WebSphere 7 Install

Use this workflow to create a custom profile on an existing WebSphere 7 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 Create Custom Node from Existing WebSphere 7 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 WebSphere 7 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server version 7 on 64-bit Red Hat Linux:

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 libXp-1.0.0-8 compat-libstdc++- 296-2.96-138 rpm-build- 4.4.2-37.el5

   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 7, refer to the WebSphere 7 Product Documentation on page 109.

How this Workflow Works

This topic contains the following information about the Create Custom Node from Existing WebSphere 7 Install workflow:

Overview

This workflow does the following things in the order shown:

1. Prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebSphere 7 environment
2. Creates a new response file
3. Creates a custom node profile
4. Optionally federates the custom managed node profile into a Deployment Manager

Validation Checks Performed

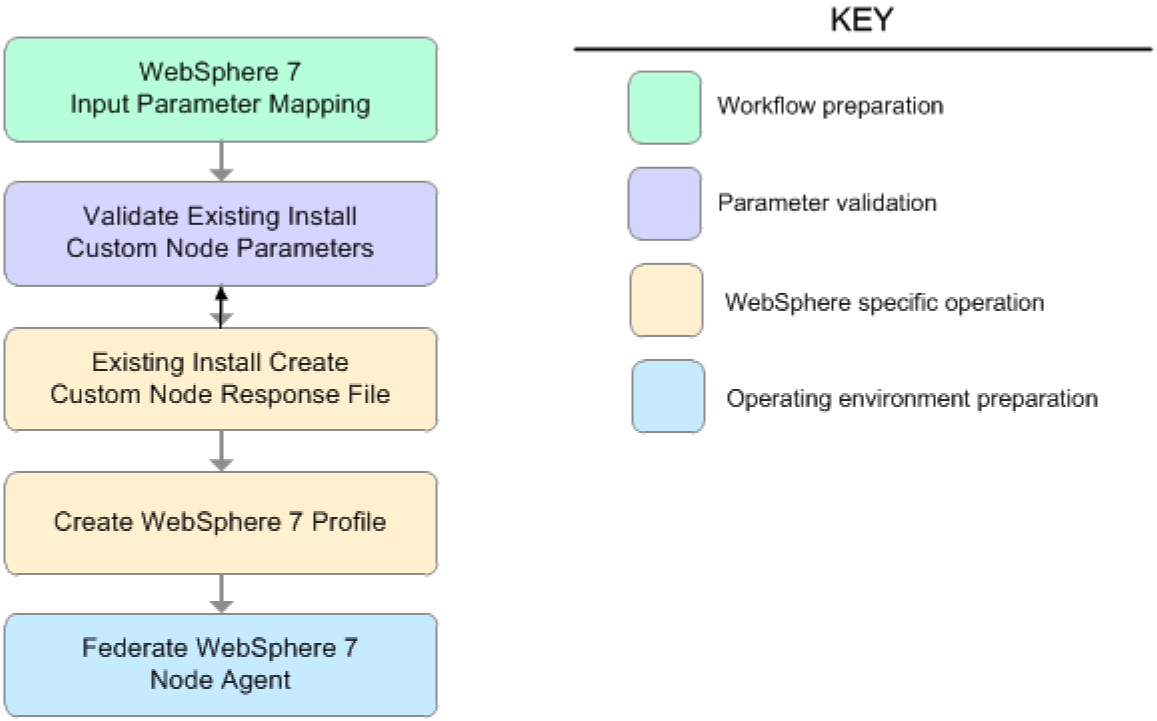
Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks for Red Hat Linux.

The workflow performs the following parameter checks:

1. Enable Security is true or false. If Enable Security is true, Dmgr Admin Password and Dmgr Admin User are specified.
2. Dmgr Admin User (if specified) does not begin with a period (.), hyphen (-) or space. It does not contain any of the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
3. Dmgr Admin Password (if specified) does not begin with a hyphen (-) or contain a space.
4. Cell Name, Node Name, and Profile Name are specified. They do not contain the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { } or space. They do not begin with a period.
5. Host Name is specified.
6. Ports File (if specified) exists.
7. Federate Later (if specified) is true or false.
8. Dmgr Port (if specified) is an integer.
9. Profile Path and Response File are specified.
10. Install Location points to a valid existing WebSphere 7 installation.

Steps Executed

The Create Custom Node from Existing WebSphere 7 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.



Steps Used in the Create Custom Node from Existing WebSphere 7 Install Workflow

Workflow Step	Description
WebSphere 7 Input Parameter Mapping	This step creates the call wrapper—the command that executes the step as a specific user—and allows certain parameters to be hidden or exposed.
Validate Existing Install Custom Node Parameters	This step prepares and validates the parameters needed to create a custom node profile for an existing WebSphere Application Server V7.0 installation.
Existing Install Create Custom Node Response File	This step creates a new response file to create a custom node profile on top of an existing WebSphere Application Server V7.0 installation.
Create WebSphere 7 Profile	This step creates a profile on top of an existing WebSphere Application Server V7.0 installation.
Federate WebSphere 7 Node Agent	This step federates the custom managed node profile into a Deployment Manager, creating a node agent.

How to Run this Workflow

The following instructions show you how to customize and run the Create Custom Node from Existing WebSphere 7 Install workflow in your environment.

> **Tip:** For detailed instructions to run HP DMA workflows—using the 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 Create Custom Node from Existing WebSphere 7 Install on page 89

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

To customize and run the Create Custom Node from Existing WebSphere 7 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:

Input Parameters for Validate Existing Install Custom Node Parameters

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

Input Parameters for Validate Existing Install Custom Node Parameters, continued

Parameter Name	Default Value	Required	Description
Dmgr HostName	no default	optional	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). 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.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Profile Path	no default	required	Fully qualifed path to the custom node profile. For example: `/opt/IBM/WebSphere/AppServer/profiles/ProdNode01`
Response File	no default	required	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 for Install WebSphere 7 Create Profile

Parameter Name	Default Value	Required	Description
Password	no default	required	The Windows Administrator password. Required for Windows.
Username	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 Create Custom Node from Existing WebSphere 7 Install on page 89 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 116).

3. In the workflow editor, expose any additional parameters that you need (see How to Expose Additional Workflow Parameters on page 115). 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.

Optional: if you want to further verify the results, 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 7 is installed. This is the path that you specified in the WebSphere Install Location parameter.
2. Validate that the Deployment Manager 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/nodeagent` directory, and tail the `SystemOut.log` file. Look for the following line:

      ```
      Server nodeagent open for e-business
      ```

Sample Scenario

This topic shows you typical parameter values used for the Create Custom Node from Existing WebSphere 7 Install workflow.

Add custom node profiles on existing WebSphere 7 install

Input Parameters for Validate Existing Install Custom Node Parameters

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	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.
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.
Install Location	see description	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
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.

Input Parameters for Validate Existing Install Custom Node Parameters, continued

Parameter Name	Example Value	Description
Profile Name	DevNode	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Profile Path	see description	Fully qualifed path to the custom node profile. For example: `/opt/IBM/WebSphere/AppServer/profiles/ProdNode01`
Response File	`/tmp/serverrsp`	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.

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 116).

Parameters for Create Custom Node from Existing WebSphere 7 Install

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment (see How to Expose Additional Workflow Parameters on page 115). For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Note: Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Parameters Defined in this Step: Validate Existing Install Custom Node Parameters

<table>
<tr><th>Parameter Name</th><th>Default Value</th><th>Required</th><th>Description</th></tr>
<tr><td>Call Wrapper</td><td>see description</td><td>required</td><td>Command that will execute this step (or subsequent steps) as a specific user.
For UNIX targets, the default is: <code>/opt/hp/dma/client/jython.sh</code> running as root
For Windows targets, the default is: <code>jython</code> running as Administrator
<b>Caution:</b> This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.</td></tr>
<tr><td>Cell Name</td><td>no default</td><td>required</td><td>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.</td></tr>
<tr><td>Dmgr Admin Password</td><td>no default</td><td>optional</td><td>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( ).</td></tr>
<tr><td>Dmgr Admin User</td><td>no default</td><td>optional</td><td>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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.</td></tr>
</table>

Parameters Defined in this Step: Validate Existing Install Custom Node Parameters, continued

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

Parameters Defined in this Step: Validate Existing Install Custom Node Parameters, continued

Parameter Name	Default Value	Required	Description
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_adminhost=9060). This option should be used with the Validate Ports option.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Profile Path	no default	required	Fully qualifed path to the custom node profile. For example: `/opt/IBM/WebSphere/AppServer/profiles/ProdNode01`
Response File	no default	required	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 Parameters Defined in this Step: Install WebSphere 7 Create Profile

Parameter Name	Default Value	Required	Description
Password	no default	required	The Windows Administrator password. Required for Windows.
Username	no default	required	This is the Windows Administrator user. Required for Windows.

Provision IBM HTTP Server 7 and Plug-In

Use this workflow to install IBM HTTP Server for WebSphere Application Server V7.0 and, optionally, install its WebSphere Application Server Plug-In.

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

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 libXp-1.0.0-8 compat-libstdc++- 296-2.96-138 rpm-build- 4.4.2-37.el5

   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 7, refer to the WebSphere 7 Product Documentation on page 109.

How this Workflow Works

This topic contains the following information about the Provision IBM HTTP Server 7 and Plug-In workflow:

Overview

This workflow does the following things in the order shown:

1. Prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebSphere 7 environment
2. Checks the documented library requirements, files system space requirements, and temporary space requirements
3. Checks whether the WebSphere 7 binaries are available—if not, they will be downloaded from the software repository—and extracts the binary files from the compressed archive
4. Creates a new response file for installing IBM HTTP Server and creating its plug-in
5. Installs IBM HTTP Server

Validation Checks Performed

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

The workflow first performs the following parameter checks:

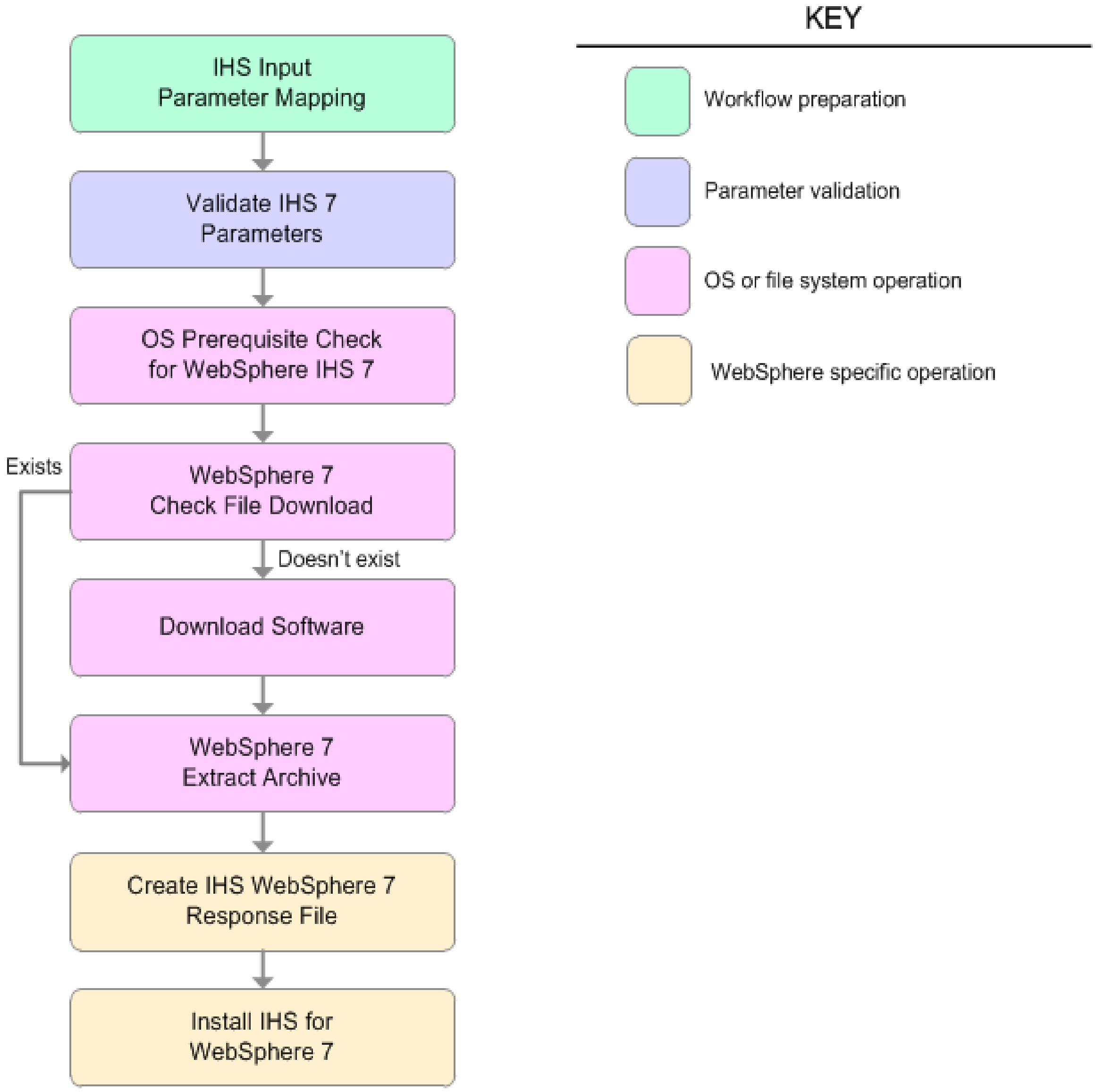
1. If Create Admin Auth is true, Admin Auth User, Admin Auth Password, and Admin Auth Password Confirm are specified.
2. If Create Admin User Group is true, Set Up Admin User and Set Up Admin Group are specified.
3. If Install Plugin is true, WebSphere Hostname is specified.
4. Binary Archive is a full file path.The directory path either exists or can be created successfully.
5. Extract Dir and Install Location are full directory paths. The directory paths either exist or can be created successfully.
6. Admin Auth User does not contain a colon (:).
7. Webserver Definition and WebSphere Hostname do not contain a space ( ).
8. Http Port and Admin Port (if specified) are integers.
9. License Acceptance, Create Admin Auth, Run Admin Setup, Create Admin User Group, and Install Plugin are true or false (case insensitive).

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 the previous page).
2. Sufficient disk space is available to install IBM HTTP Server for WebSphere Application Server V7.0.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

The Provision IBM HTTP Server 7 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.


IHS Input Parameter Mapping
Validate IHS 7 Parameters
OS Prerequisite Check for WebSphere IHS 7
Exists
WebSphere 7 Check File Download
Doesn't exist
Download Software
WebSphere 7 Extract Archive
Create IHS WebSphere 7 Response File
Install IHS for WebSphere 7
KEY
Workflow preparation
Parameter validation
OS or file system operation
WebSphere specific operation

Steps Used in the Provision IBM HTTP Server 7 and Plug-In Workflow

Workflow Step	Description
IHS Input Parameter Mapping	This step allows for either the defaulting of parameters to be used later in a step or to hide or expose certain parameters that will or will not be needed depending on what the end user wants to do.
Validate IHS 7 Parameters	This step prepares and validates the parameters needed to install IBM HTTP Server for WebSphere Application Server V7.0 and, optionally, create its WebSphere Application Server plug-in.
OS Prerequisite Check for WebSphere IHS 7	This step checks the following: 1. Documented library requirements for WebSphere Application Server V7.0. 2. Files system space requirements where IBM HTTP Server for WebSphere Application Server V7.0 will be installed.. 3. Temporary space requirements where the compressed software will be extracted before it is installed.
WebSphere 7 Check File Download	This step checks for the existence of a file before downloading it from the software repository: • Checks if a file exists in the expected location. • If the file is not in the expected location, the file is added to a list of files that need to be downloaded.
Download Software	This step downloads a list of files to a specified location on the target server.
WebSphere 7 Extract Archive	This step checks that the archive file exists and then, based on the archive extension, extracts the archive to the specified directory.
Create IHS WebSphere 7 Response File	This step creates a new response file for installing IBM HTTP Server for WebSphere Application Server V7.0 and then, optionally, creating its WebSphere Application Server plug-in.
Install IHS for WebSphere 7	This step installs IBM HTTP Server for WebSphere Application Server V7.0 using the "install -options <responsefile> silent" option.

How to Run this Workflow

The following instructions show you how to customize and run the Provision IBM HTTP Server 7 and Plug-In workflow in your environment.

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

> **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 7 and Plug-Inworkflow:

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:

Input Parameters for Validate IHS 7 Parameters

Parameter Name	Default Value	Required	Description
Admin Auth Password	no default	optional	The password used to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. When Create Admin Auth is set to true, this parameter must have a value. It cannot begin with a dash(-) or contain a space( ).
Admin Auth Password Confirm	no default	optional	Confirms the Admin Auth Password.
Admin Auth User	no default	optional	The user ID used to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. When Create Admin Auth is set to true, this parameter must have a value. It cannot begin with a dash(-), a period(.), or a space( ) and cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
Admin Port	no default	required	The port on which the HTTP administration web server will run. This is usually 8008.
Binary Archive	no default	required	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`

Input Parameters for Validate IHS 7 Parameters, continued

Parameter Name	Default Value	Required	Description
Create Admin Auth	no default	required	Set this to true to create a user ID and password to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. If this parameter is set to true, the following parameters must have values: Admin Auth Password, Admin Auth Password Confirm, and Admin Auth User.
Create Admin User Group	no default	required	Set to true to create a user ID and group used to set up the IBM HTTP Administration Server on Linux and UNIX operating systems.
Extract Dir	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Http Port	no default	required	The port on which the web server will listen. This is usually set to 80.
Install Location	no default	required	Fully qualified path where IBM HTTP Server will be installed. For example: `/opt/IBM/HTTPServer`
Install Plugin	no default	required	Determines whether or not the WebSphere Application Server Plug-In is installed. Valid options are true or false.
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.
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file is used to drive the installation.
Run Admin Setup	no default	required	Enables the install process to grant the Set Up Admin User write access to the necessary IBM HTTP Server and WebSphere Application Server Plug-In configuration files. Valid options are true or false.
Set Up Admin Group	no default	optional	Group name used to set up the IBM HTTP administration server on Linux and UNIX operating systems. This parameter must have a value if Create Admin User Group is set to true.

Input Parameters for Validate IHS 7 Parameters, continued

Parameter Name	Default Value	Required	Description
Set Up Admin User	no default	optional	User ID used to set up the IBM HTTP administration server on Linux and UNIX operating systems. If Create Admin User Group is set to true, this parameter must have a value.
Webserver Definition	no default	optional	A web server definition allows for web server administration through the WebSphere administrative console. This parameter must be set if the Install Plugin parameter is set to true. An example would be webserver1. No spaces are allowed in the Webserver Definition name.
WebSphere Hostname	no default	optional	Host name of the WebSphere Application Server machine. This parameter is required if Install Plugin is set to true. No spaces are allowed in the host name.

Additional Input Parameters for Install IHS for WebSphere 7

Parameter Name	Default Value	Required	Description
Password	no default	required	The Windows Administrator password. Required for Windows.
Username	no default	required	This is the Windows Administrator user. Required for Windows.

Note: See Parameters for Provision IBM HTTP Server 7 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 116).

3. Save the changes to the workflow (click **Save** in the lower right corner).
4. Create a new deployment (see "Create a Deployment" in *HP DMA Quick Start Tutorial* for instructions).
5. On the Parameters tab, specify values for the required parameters listed in step 2.
6. On the Targets tab, specify one or more targets for this deployment.
7. Save the deployment (click **Save** in the lower right corner).
8. 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.

Optional: if you want to further verify the results, perform the following steps:

1. After the workflow has completed, run the following command to check the version IBM HTTP Server 7 that was installed:

   ```
   IHS_ROOT/bin/versionInfo.sh
   ```

   Here, `IHS_ROOT` is the directory where IBM HTTP Server 7 is installed. This is the path that you specified in the WebSphere Install Location parameter.

2. Validate that the IBM HTTP Server 7 has been properly installed by doing the following:

   View the `IHS_ROOT/logs/install/log.txt` file.

   If the installation was successful, you should see messages similar to these:

   ```
   (Apr 21, 2011 9:21:06 AM), Process,
   com.ibm.ws.install.ni.ismp.actions.SettleNIFRegistryAction, msg1, Current
   install/uninstall process is successful. Process type is: install

   (Apr 21, 2011 9:21:07 AM), Process,
   com.ibm.ws.install.ni.ismp.actions.SetExitCodeAction, msg1, CWUPI0000I:
   EXITCODE=0

   (Apr 21, 2011 9:21:07 AM), Process,
   com.ibm.ws.install.ni.ismp.actions.ISMPLogSuccessMessageAction, msg1,
   INSTCONFSUCCESS
   ```

3. If you installed the WebSphere Application Server Plug-In, validate that it has been properly installed by doing the following:

   View the `IHS_ROOT/Plugins/logs/install/log.txt` file.

   If the installation was successful, you should see messages similar to these:

   ```
   (Apr 21, 2011 9:21:05 AM), Process,
   com.ibm.ws.install.ni.ismp.actions.ISMPLogFileAction, msg1, INSTCONF_COMPLETE :
   Installation is complete.

   (Apr 21, 2011 9:21:05 AM), Process,
   com.ibm.ws.install.ni.ismp.actions.ISMPLogFileAction, msg1,
   ****************************

   (Apr 21, 2011 9:21:05 AM), Process,
   com.ibm.ws.install.ni.ismp.actions.SetExitCodeAction, msg1, CWUPI0000I:
   EXITCODE=0

   (Apr 21, 2011 9:21:05 AM), Process,
   com.ibm.ws.install.ni.ismp.actions.ISMPLogSuccessMessageAction, msg1,
   INSTCONFSUCCESS
   ```

Sample Scenario

This topic shows you typical parameter values used for the Provision IBM HTTP Server 7 and Plug-In workflow.

Scenario 1: New IBM HTTP Server 7 install with plug-in using the simplest method

This example shows the following:

Task	Parameter Values
Do not create a user ID and password to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console	• Set Create Admin Auth to false
Do not create a user ID and group used to set up the IBM HTTP Administration Server on Linux and UNIX operating systems	• Set Create Admin User Group to false
Do not install the WebSphere Application Server Plug-In	• Set Install Plugin to false
Do not grant the Set Up Admin User write access to the necessary IBM HTTP Server and WebSphere Application Server Plug-In configuration files	• Set Run Admin Setup to false

Input Parameters for Validate IHS 7 Parameters

Parameter Name	Example Value	Description
Admin Port	8008	The port on which the HTTP administration web server will run. This is usually 8008.
Binary Archive	see description	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`
Create Admin Auth	false	Set this to true to create a user ID and password to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. If this parameter is set to true, the following parameters must have values: Admin Auth Password, Admin Auth Password Confirm, and Admin Auth User.
Create Admin User Group	false	Set to true to create a user ID and group used to set up the IBM HTTP Administration Server on Linux and UNIX operating systems.
Extract Dir	`/opt/IBM/wasv7`	Fully qualified path where the compressed software will be extracted on the target machine.
Http Port	80	The port on which the web server will listen. This is usually set to 80.

Input Parameters for Validate IHS 7 Parameters, continued

Parameter Name	Example Value	Description
Install Location	see description	Fully qualified path where IBM HTTP Server will be installed. For example: `/opt/IBM/HTTPServer`
Install Plugin	false	Determines whether or not the WebSphere Application Server Plug-In is installed. Valid options are true or false.
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.
Response File	`/tmp/serverrsp`	Fully qualified path where the response file that this workflow creates will be located. This file is used to drive the installation.
Run Admin Setup	false	Enables the install process to grant the Set Up Admin User write access to the necessary IBM HTTP Server and WebSphere Application Server Plug-In configuration files. Valid options are true or false.

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 116).

Scenario 2: New IBM HTTP Server 7 install with plug-in using all the options

This example shows the following:

Task	Parameter Values
To create a user ID and password to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console	• Set Create Admin Auth to true • Specify values for: Admin Auth Password Admin Auth Password Confirm Admin Auth User
To create a user ID and group used to set up the IBM HTTP Administration Server on Linux and UNIX operating systems	• Set Create Admin User Group to true • Specify values for: Set Up Admin Group Set Up Admin User
To install the WebSphere Application Server Plug-In	• Set Install Plugin to true • Specify values for: WebSphere Hostname Webserver Definition
To grant the Set Up Admin User write access to the necessary IBM HTTP Server and WebSphere Application Server Plug-In configuration files	• Set Run Admin Setup to true

Input Parameters for Validate IHS 7 Parameters

Parameter Name	Example Value	Description
Admin Auth Password	AdminPsWd	The password used to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. When Create Admin Auth is set to true, this parameter must have a value. It cannot begin with a dash(-) or contain a space( ).
Admin Auth Password Confirm	AdminPsWd	Confirms the Admin Auth Password.
Admin Auth User	admin	The user ID used to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. When Create Admin Auth is set to true, this parameter must have a value. It cannot begin with a dash(-), a period(.), or a space( ) and cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
Admin Port	8008	The port on which the HTTP administration web server will run. This is usually 8008.

Input Parameters for Validate IHS 7 Parameters, continued

Parameter Name	Example Value	Description
Binary Archive	see description	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`
Create Admin Auth	true	Set this to true to create a user ID and password to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. If this parameter is set to true, the following parameters must have values: Admin Auth Password, Admin Auth Password Confirm, and Admin Auth User.
Create Admin User Group	true	Set to true to create a user ID and group used to set up the IBM HTTP Administration Server on Linux and UNIX operating systems.
Extract Dir	`/opt/IBM/wasv7`	Fully qualified path where the compressed software will be extracted on the target machine.
Http Port	80	The port on which the web server will listen. This is usually set to 80.
Install Location	see description	Fully qualified path where IBM HTTP Server will be installed. For example: `/opt/IBM/HTTPServer`
Install Plugin	true	Determines whether or not the WebSphere Application Server Plug-In is installed. Valid options are true or false.
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.
Response File	`/tmp/serverrsp`	Fully qualified path where the response file that this workflow creates will be located. This file is used to drive the installation.
Run Admin Setup	true	Enables the install process to grant the Set Up Admin User write access to the necessary IBM HTTP Server and WebSphere Application Server Plug-In configuration files. Valid options are true or false.
Set Up Admin Group	AdminGrp	Group name used to set up the IBM HTTP administration server on Linux and UNIX operating systems. This parameter must have a value if Create Admin User Group is set to true.

Input Parameters for Validate IHS 7 Parameters, continued

Parameter Name	Example Value	Description
Set Up Admin User	AdminUsr	User ID used to set up the IBM HTTP administration server on Linux and UNIX operating systems. If Create Admin User Group is set to true, this parameter must have a value.
Webserver Definition	webserver1	A web server definition allows for web server administration through the WebSphere administrative console. This parameter must be set if the Install Plugin parameter is set to true. An example would be webserver1. No spaces are allowed in the Webserver Definition name.
WebSphere Hostname	was1.mycompany.com	Host name of the WebSphere Application Server machine. This parameter is required if Install Plugin is set to true. No spaces are allowed in the host name.

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 116).

Parameters for Provision IBM HTTP Server 7 and Plug-in

The following tables describe the required and optional input parameters for this workflow. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

> **Note:** Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Parameters Defined in this Step: Validate IHS 7 Parameters

Parameter Name	Default Value	Required	Description
Admin Auth Password	no default	optional	The password used to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. When Create Admin Auth is set to true, this parameter must have a value. It cannot begin with a dash(-) or contain a space( ).
Admin Auth Password Confirm	no default	optional	Confirms the Admin Auth Password.
Admin Auth User	no default	optional	The user ID used to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. When Create Admin Auth is set to true, this parameter must have a value. It cannot begin with a dash(-), a period(.), or a space( ) and cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
Admin Port	no default	required	The port on which the HTTP administration web server will run. This is usually 8008.
Binary Archive	no default	required	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`

Parameters Defined in this Step: Validate IHS 7 Parameters, continued

Parameter Name	Default Value	Required	Description
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. For UNIX targets, the default is: `/opt/hp/dma/client/jython.sh` running as root For Windows targets, the default is: `jython` running as Administrator **Caution:** This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.
Create Admin Auth	no default	required	Set this to true to create a user ID and password to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. If this parameter is set to true, the following parameters must have values: Admin Auth Password, Admin Auth Password Confirm, and Admin Auth User.
Create Admin User Group	no default	required	Set to true to create a user ID and group used to set up the IBM HTTP Administration Server on Linux and UNIX operating systems.
Extract Dir	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Http Port	no default	required	The port on which the web server will listen. This is usually set to 80.
Install Location	no default	required	Fully qualified path where IBM HTTP Server will be installed. For example: `/opt/IBM/HTTPServer`
Install Plugin	no default	required	Determines whether or not the WebSphere Application Server Plug-In is installed. Valid options are true or false.
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.
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file is used to drive the installation.

Parameters Defined in this Step: Validate IHS 7 Parameters, continued

Parameter Name	Default Value	Required	Description
Run Admin Setup	no default	required	Enables the install process to grant the Set Up Admin User write access to the necessary IBM HTTP Server and WebSphere Application Server Plug-In configuration files. Valid options are true or false.
Set Up Admin Group	no default	optional	Group name used to set up the IBM HTTP administration server on Linux and UNIX operating systems. This parameter must have a value if Create Admin User Group is set to true.
Set Up Admin User	no default	optional	User ID used to set up the IBM HTTP administration server on Linux and UNIX operating systems. If Create Admin User Group is set to true, this parameter must have a value.
Webserver Definition	no default	optional	A web server definition allows for web server administration through the WebSphere administrative console. This parameter must be set if the Install Plugin parameter is set to true. An example would be webserver1. No spaces are allowed in the Webserver Definition name.
WebSphere Hostname	no default	optional	Host name of the WebSphere Application Server machine. This parameter is required if Install Plugin is set to true. No spaces are allowed in the host name.

Additional Parameters Defined in this Step: Install IHS for WebSphere 7

Parameter Name	Default Value	Required	Description
Password	no default	required	The Windows Administrator password. Required for Windows.
Username	no default	required	This is the Windows Administrator user. Required for Windows.

Chapter 3: Reference Information

This chapter contains the following information:

Topic	Description
WebSphere 7 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 7,
HP DMA Documentation	Links to additional HP DMA documentation

WebSphere 7 Product Documentation

For the current list of hardware and software requirements, as well as supported platforms for WebSphere 7, see:

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

For WebSphere 7 product documentation, see:

http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp

For IBM Red Book resources for WebSphere 7, 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 Support web site:

https://softwaresupport.hp.com/

Chapter 4: Tips and Best Practices

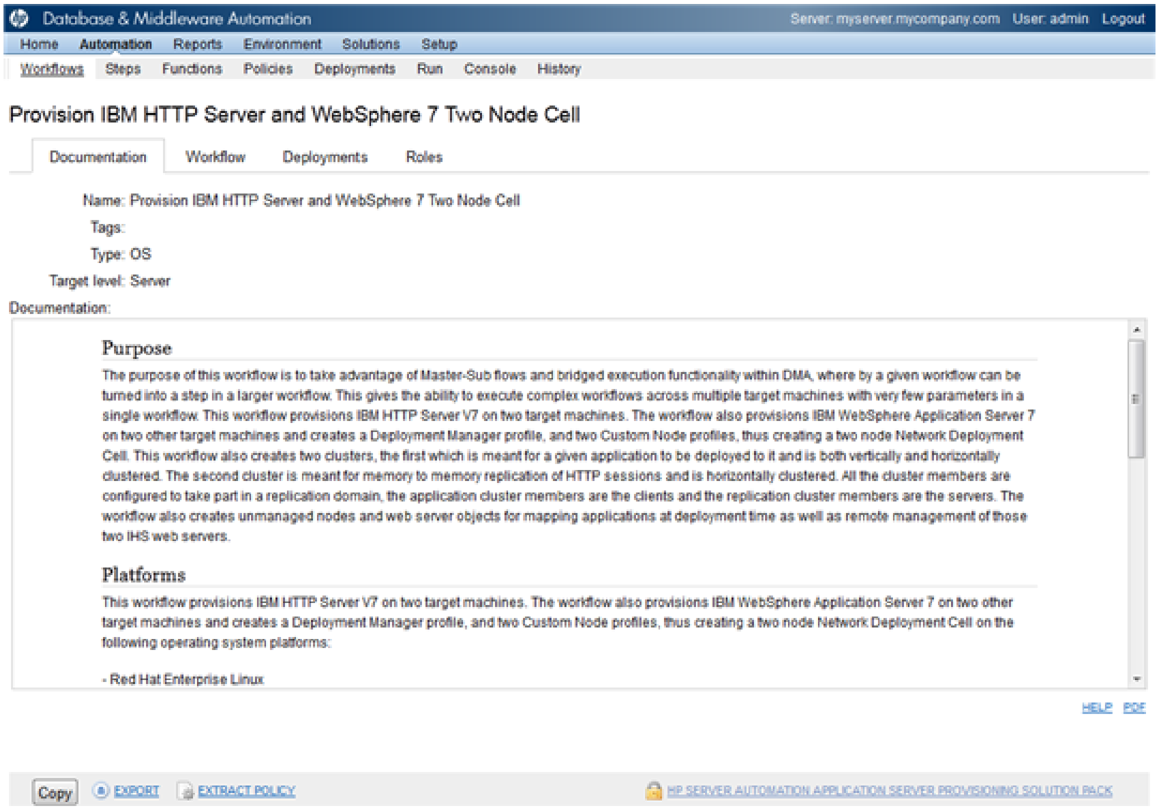
This portion of the document contains a collection of tips and best practices that will enable you to use HP DMA more effectively. It contains the following topics:

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.



Provision IBM HTTP Server and WebSphere 7 Two Node Cell

Name: Provision IBM HTTP Server and WebSphere 7 Two Node Cell

Tags:

Type: OS

Target level: Server

Documentation:

Purpose

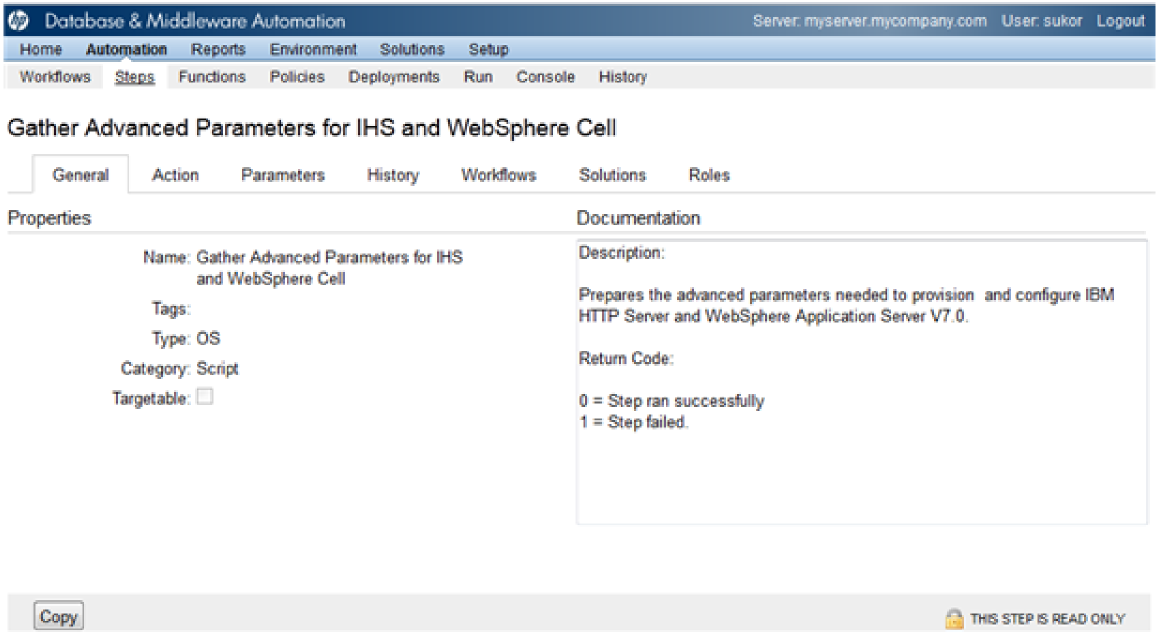
The purpose of this workflow is to take advantage of Master-Sub flows and bridged execution functionality within DMA, where by a given workflow can be turned into a step in a larger workflow. This gives the ability to execute complex workflows across multiple target machines with very few parameters in a single workflow. This workflow provisions IBM HTTP Server V7 on two target machines. The workflow also provisions IBM WebSphere Application Server 7 on two other target machines and creates a Deployment Manager profile, and two Custom Node profiles, thus creating a two node Network Deployment Cell. This workflow also creates two clusters, the first which is meant for a given application to be deployed to it and is both vertically and horizontally clustered. The second cluster is meant for memory to memory replication of HTTP sessions and is horizontally clustered. All the cluster members are configured to take part in a replication domain, the application cluster members are the clients and the replication cluster members are the servers. The workflow also creates unmanaged nodes and web server objects for mapping applications at deployment time as well as remote management of those two IHS web servers.

Platforms

This workflow provisions IBM HTTP Server V7 on two target machines. The workflow also provisions IBM WebSphere Application Server 7 on two other target machines and creates a Deployment Manager profile, and two Custom Node profiles, thus creating a two node Network Deployment Cell on the following operating system platforms:

- Red Hat Enterprise Linux

A workflow consists of a sequence of **steps**. Each step performs a very specific task. Each step includes a documentation panel that briefly describes its function.


Database & Middleware Automation
Server: myserver.mycompany.com User: sukor Logout
Home Automation Reports Environment Solutions Setup
Workflows Steps Functions Policies Deployments Run Console History
General Action Parameters History Workflows Solutions Roles
Copy
THIS STEP IS READ ONLY

Gather Advanced Parameters for IHS and WebSphere Cell

Properties

Name: Gather Advanced Parameters for IHS and WebSphere Cell
Tags:
Type: OS
Category: Script
Targetable: □

Documentation

Description:

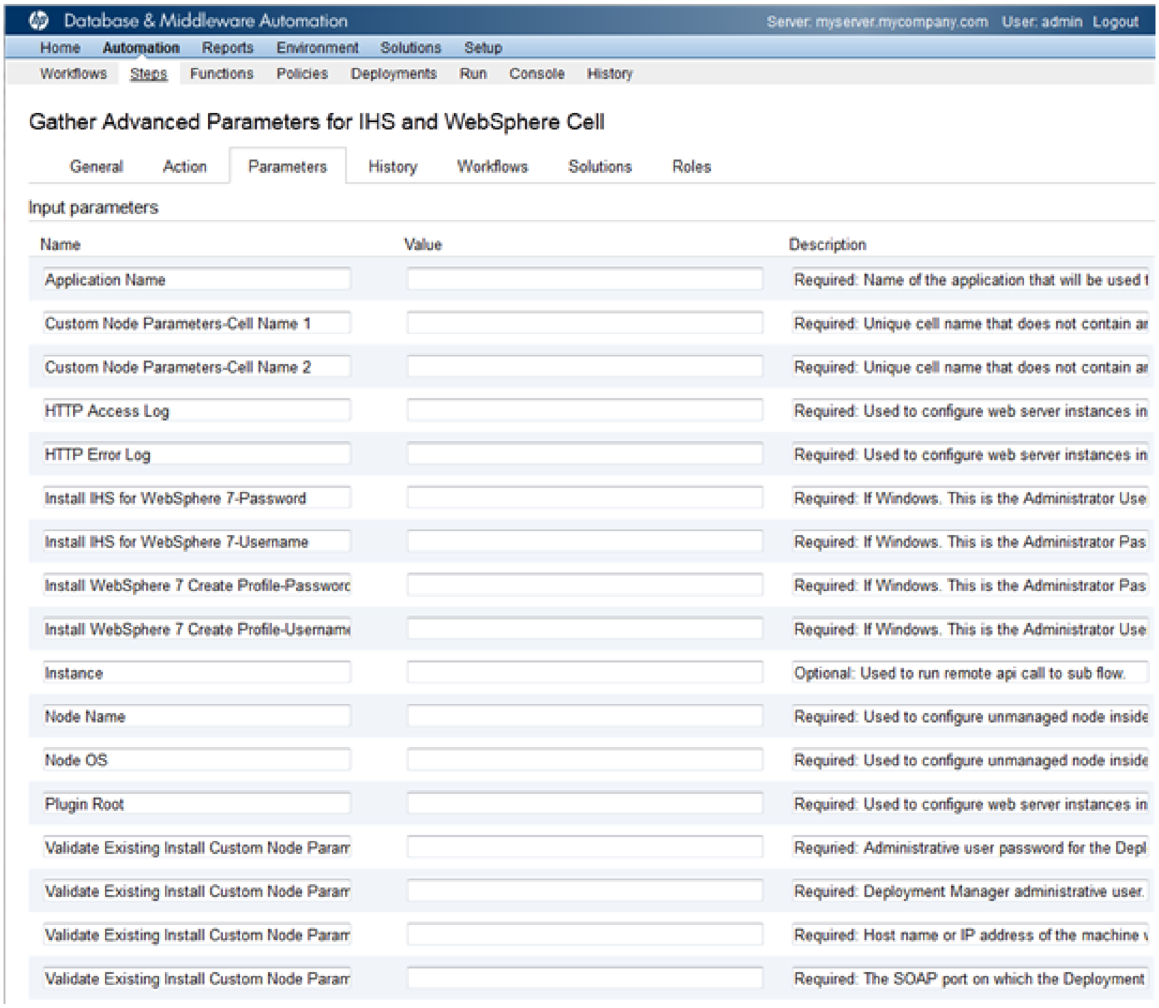
Prepares the advanced parameters needed to provision and configure IBM HTTP Server and WebSphere Application Server V7.0.

Return Code:

0 = Step ran successfully
1 = Step failed.

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

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


Database & Middleware Automation
Server: myserver.mycompany.com User: admin Logout
Home Automation Reports Environment Solutions Setup
Workflows Steps Functions Policies Deployments Run Console History

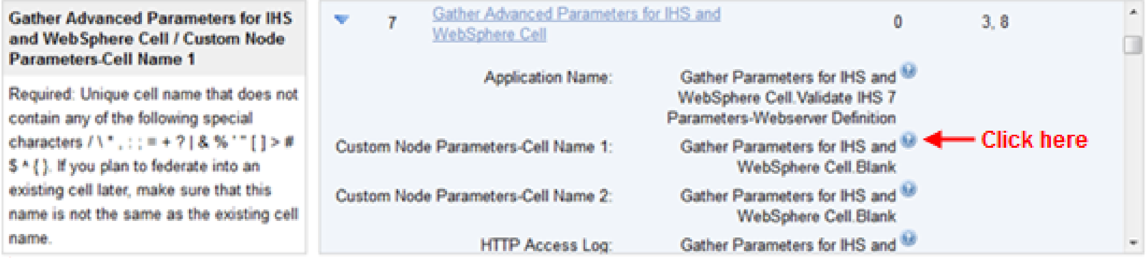
Gather Advanced Parameters for IHS and WebSphere Cell

General Action Parameters History Workflows Solutions Roles

Input parameters

Name	Value	Description
Application Name		Required: Name of the application that will be used t
Custom Node Parameters-Cell Name 1		Required: Unique cell name that does not contain ar
Custom Node Parameters-Cell Name 2		Required: Unique cell name that does not contain ar
HTTP Access Log		Required: Used to configure web server instances in
HTTP Error Log		Required: Used to configure web server instances in
Install IHS for WebSphere 7-Password		Required: If Windows. This is the Administrator Use
Install IHS for WebSphere 7-Username		Required: If Windows. This is the Administrator Pas
Install WebSphere 7 Create Profile-Passworc		Required: If Windows. This is the Administrator Pas
Install WebSphere 7 Create Profile-Usernam		Required: If Windows. This is the Administrator Use
Instance		Optional: Used to run remote api call to sub flow.
Node Name		Required: Used to configure unmanaged node inside
Node OS		Required: Used to configure unmanaged node inside
Plugin Root		Required: Used to configure web server instances in
Validate Existing Install Custom Node Param		Required: Administrative user password for the Depl
Validate Existing Install Custom Node Param		Required: Deployment Manager administrative user.
Validate Existing Install Custom Node Param		Required: Host name or IP address of the machine v
Validate Existing Install Custom Node Param		Required: The SOAP port on which the Deployment

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



Gather Advanced Parameters for IHS and WebSphere Cell / Custom Node Parameters-Cell Name 1

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.

7 Gather Advanced Parameters for IHS and WebSphere Cell 0 3, 8

Application Name: Gather Parameters for IHS and WebSphere Cell.Validate IHS 7 Parameters-Webserver Definition

Custom Node Parameters-Cell Name 1: Gather Parameters for IHS and WebSphere Cell.Blank

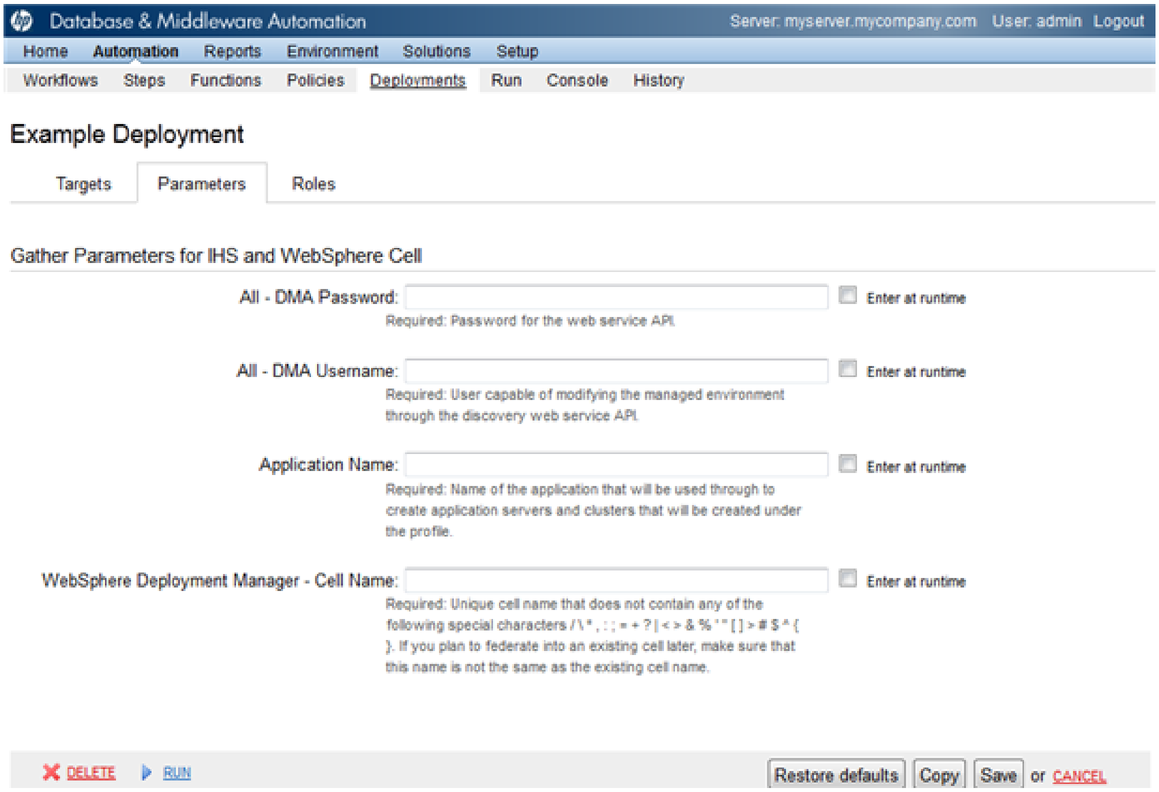
Custom Node Parameters-Cell Name 2: Gather Parameters for IHS and WebSphere Cell.Blank

HTTP Access Log: Gather Parameters for IHS and

Click here

To see the parameter description here

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



Example Deployment

Gather Parameters for IHS and WebSphere Cell

All - DMA Password: ☐ Enter at runtime
Required: Password for the web service API.

All - DMA Username: ☐ Enter at runtime
Required: User capable of modifying the managed environment through the discovery web service API.

Application Name: ☐ Enter at runtime
Required: Name of the application that will be used through to create application servers and clusters that will be created under the profile.

WebSphere Deployment Manager - Cell Name: ☐ Enter at runtime
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.

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.

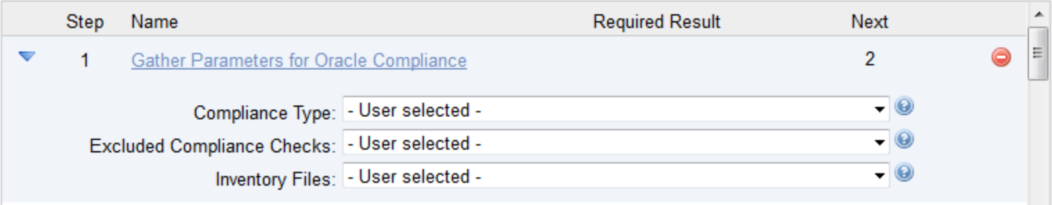
How to Expose Additional Workflow Parameters

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

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

To expose a hidden workflow parameter:

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



	Step	Name	Required Result	Next
▼	1	Gather Parameters for Oracle Compliance		2

Compliance Type: - User selected -

Excluded Compliance Checks: - User selected -

Inventory Files: - User selected -

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

How to Use a Policy to Specify Parameter Values

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

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

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

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

For more information, see the *HP DMA User Guide*. This document is available on the HP Software Support web site: https://softwaresupport.hp.com/

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 the next page).

To create a policy that provides parameter values:

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

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

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

   c. Click **Add**.

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

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

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

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

Extract a Policy

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

To extract a policy:

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

Reference the Policy in the Deployment

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

To reference policy attributes in a deployment:

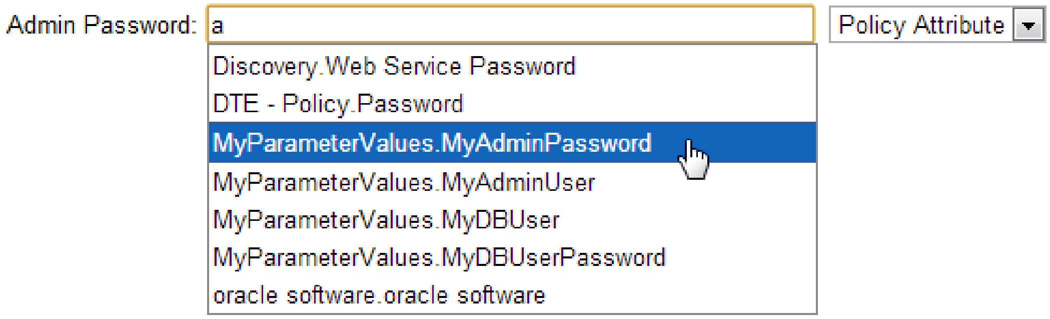
1. Create or access the deployment.

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

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

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

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

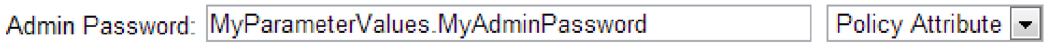


Admin Password: a

Policy Attribute

Discovery.Web Service Password
DTE - Policy.Password
MyParameterValues.MyAdminPassword
MyParameterValues.MyAdminUser
MyParameterValues.MyDBUser
MyParameterValues.MyDBUserPassword
oracle software.oracle software

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



Admin Password: MyParameterValues.MyAdminPassword

Policy Attribute

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

How to Import a File into the Software Repository

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

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

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

To import a file into the HP SA Software Library:

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

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

   If the HP SA Client is not installed locally, follow the instructions under “Installing the SA Client Launcher” in the *User Guide: Server Automation*, available on the HP Software Support web site: https://softwaresupport.hp.com/
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 the 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 the HP Server Automation 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 Support web site: https://softwaresupport.hp.com/

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 Support web site: https://softwaresupport.hp.com/

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 HP Server Automation. 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 HP Server Automation. 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.