

HP Database and Middleware Automation

Application Server Provisioning Solution Pack

for the IBM AIX, Red Hat Enterprise Linux, Solaris, and Windows® operating systems

Software version: 9.10

User Guide



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2011 Hewlett-Packard Development Company, L.P.

Trademark Notices

Windows is a U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

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

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

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

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

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

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

Support

Visit the HP Software Support Online web site at:

www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport user ID, go to:

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

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

1	Introduction	7
	Supported Products	7
	Audience	7
	How this Solution Pack is Organized	7
	Workflows	8
	Provision WebSphere 7 StandAlone Profile	8
	Provision WebSphere 7 and Deployment Manager	8
	Provision WebSphere 7 and Customer Node	8
	Create StandAlone From Existing WebSphere 7 Install	8
	Create Custom Node from Existing WebSphere 7 Install	8
	Provision IBM HTTP Server 7 and Plug-in	8
	Steps	9
	Parameters	9
	Prerequisites	10
	Supported Platforms	10
	Additional resources	11
2	Quick Start	12
	Install the Solution Pack	12
	Create a Deployable Workflow	13
	Create a Deployment	13
	Run Your Workflow	14
	View the Results	15
	View the Dashboard	15
3	Customizing this Solution	16
	Expose the Optional Parameters	16
	Enable WebSphere Administrative Security	17
	Configure SSL Certificate Management	18
	Specify Ports	19
	Create a Development Server	20
	Omit the Administrative Console or Default Application	20
4	Troubleshooting	22
	Target Type	22
	User Permissions and Related Requirements	22
	Discovery in HP Server Automation	23
A	Reference Information	24
	Parameters by Workflow	24

Provision WebSphere 7 StandAlone Profile	24
Provision WebSphere 7 and Deployment Manager.....	27
Provision WebSphere 7 and Custom Node	29
Create StandAlone From Existing WebSphere 7 Install	32
Create Custom Node from Existing WebSphere 7 Install	34
Provision IBM HTTP Server 7 and Plug-In	37
WebSphere Application Server Version 7.0 Documentation	39
B Using a Policy to Specify Parameter Values.....	40
Create the Policy.....	40
Extract a Policy.....	41
Reference a Policy in a Deployment.....	41
C Using this Solution with HP Server Automation.....	42

1 Introduction

This document describes the HP Database and Middleware Automation (HP DMA) Application Server Provisioning solution pack, a collection of tools that you can use to automate and simplify the following processes:

- Installation of IBM WebSphere Application Server Version 7.0
- Creation of stand-alone, deployment manager, and custom node profiles for new or existing WebSphere Application Server Version 7.0 installations
- Installation of IBM HTTP Server for WebSphere Application Server Version 7.0

Supported Products

This solution can be used with the following HP products:

- HP Server Automation version 9.02 (or later)
- HP Database and Middleware Automation version 1.00 (or later).

Audience

This solution is designed for IT architects and engineers who are responsible for planning, implementing, and maintaining application-serving environments using WebSphere Application Server Version 7.0.

To use this solution, you should be familiar with WebSphere Application Server Version 7.0 and its requirements (see links to [WebSphere Application Server Version 7.0 Documentation](#) on page 39).

How this Solution Pack is Organized

A solution pack contains a set of related workflow templates. A workflow executes a process—for example, installing WebSphere Application Server Version 7.0 and creating a profile.

Workflows consist of a series of steps. Each step performs a very specific task. 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.

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 and then customize that copy for your environment. For more information, see [Create a Deployable Workflow](#) on page 13.

Each workflow template has a Documentation tab that provides detailed information about that workflow, including a comprehensive list of the parameters used by all steps in the workflow. This information is also provided in the [Reference Information](#) on page 24.

Workflows

This solution pack contains the following workflow templates:

Provision WebSphere 7 StandAlone Profile

Use this workflow to install the WebSphere Application Server Version 7.0 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 Application Server Version 7.0 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 Customer Node

Use this workflow to install the WebSphere Application Server Version 7.0 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 for an existing WebSphere Application Server Version 7.0 installation.

Create Custom Node from Existing WebSphere 7 Install

Use this workflow to create a custom node profile for an existing WebSphere Application Server Version 7.0 installation. The workflow can add (federate) the server to the pertinent cell when the profile is created, or you can add it later yourself.

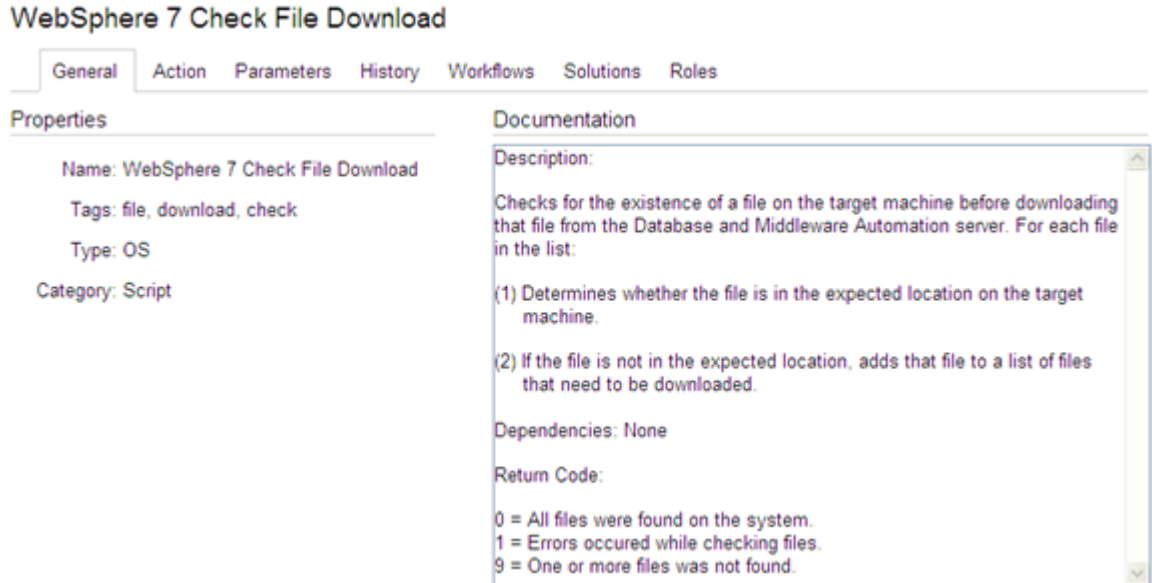
Provision IBM HTTP Server 7 and Plug-in

Use this workflow to install IBM HTTP Server (IHS) Version 7.0 and create a plug-in for IBM WebSphere Application Server Version 7.0.

Steps

Each workflow in this solution consists of a series of steps that perform the actual work. Each step includes a documentation panel that briefly describes its function (see [Figure 1](#)).

Figure 1 Example of Step Documentation



Parameters

Each parameter that is used in a step has a detailed description. You can view the parameter descriptions several different ways in the HP DMA web UI.


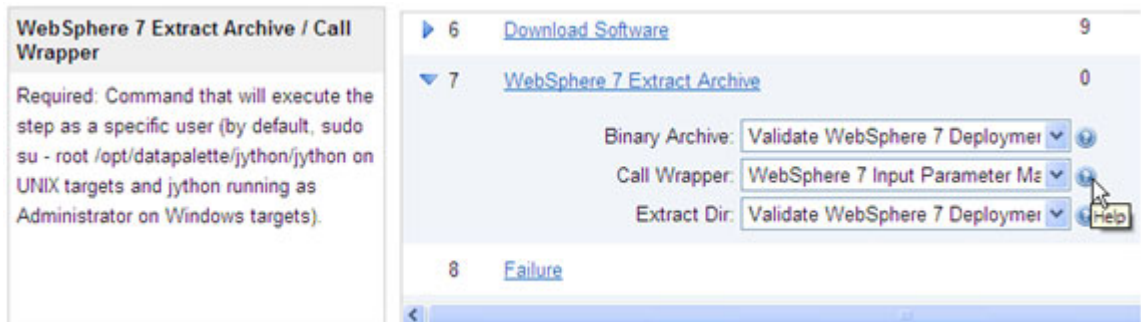
On the Workflow tab, for example, you can click the “Help” button  for a specific parameter. Information about that parameter is displayed in the left pane, as shown in [Figure 2](#).

Figure 2 Example of a Single Parameter Description on the Workflow Tab



You can view the full list of parameters on the Documentation tab, as shown in see [Figure 3](#).

Figure 3 Example of the Parameters List on the Documentation Tab

The following characters cannot be used in Admin User, Cell Name, Node Name, or Profile Name: / \ * . ; = + ? | < > & % ' " [] > # \$ ^ { }

Parameter	Default	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 special characters listed above.
Binary Archive	no default	Required	Fully qualified path to the compressed software package on the target machine.
Call Wrapper	see description	Required	Command that will execute the step as a specific user (by default, sudo su - root /opt/datapalette/jython/jython on UNIX targets and jython running as Administrator on Windows targets).
Cell Name	no default	Required	Unique cell name that does not contain any of the special characters listed above. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Default Ports	false	Optional	Provides the option to assign default ports to a profile. Valid values are true or false. If true, the WebSphere Application Server default ports will be used, and the Ports File and Starting Port parameters should not have values. If false, the workflow will increment the default port until it finds a free port. The default value is false.
Developer Server	no default	Optional	Use this parameter for development environments only to help with start up time. Valid value is true. Do not use in production environments.
Enable Security	true	Required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Extract Dir	no default	Required	Fully qualified path where the compressed software will be extracted on the target machine.

All parameters used by the workflows in this solution pack are also listed in the [Reference Information](#) on page 24.

Prerequisites

HP Server Automation (or HP Database and Middleware Automation version 1.00) must be installed and properly configured before you can use this solution pack.

Supported Platforms

The workflows included in this solution pack have been tested on the following operating system platforms:

- Red Hat Enterprise Linux Server version 5.6
- AIX version 5300-09
- SunOS version 5.10 (Solaris 10)
- Windows Server 2008 R2 x64

For hardware requirements:

- If you are using HP Server Automation, see the *HP Server Automation Quick Reference: SA Installation Requirements* or the *HP Server Automation Installation Guide*.
- If you are using HP Database and Middleware Automation version 1.00, see the *HP Database and Middleware Automation Installation Guide*.

For WebSphere Application Server Version 7.0 hardware and software requirements, see:

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

Additional resources

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

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

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

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

Updated versions of these guides are available online (see [Documentation Updates](#) on page 3).

2 Quick Start

This chapter shows you how to use the HP DMA Application Server Provisioning solution pack to install IBM WebSphere Application Server Version 7.0 and create a stand-alone profile. There are five basic steps:

- [Install the Solution Pack](#)
- [Create a Deployable Workflow](#)
- [Run Your Workflow](#)
- [View the Results](#)
- [View the Dashboard](#)

➤ By providing values for all required input parameters, you can deploy any of the workflows included in this solution pack without any additional configuration or customization.

This chapter presents the simplest method that you can use to provision WebSphere Application Server Version 7.0 on a single target server. HP DMA provides tools and mechanisms that you can then use to customize this solution for your environment. For more information, see [Customizing this Solution](#) on page 16.

➤ The information presented in this chapter assumes the following:

- HP DMA is installed and operational.
- At least one valid target server is available (see [Supported HP DMA Platforms](#) on page 93).

Install the Solution Pack

The following instructions assume that you have purchased this solution pack.

To install the solution pack:

- 1 Using the instructions in your purchase agreement, download the solution pack ISO file, and extract the following file:
`HP Server Automation Application Server Provisioning.zip` file.
- 2 On the system where you downloaded the solution pack, open a web browser, and log in to the HP DMA server using an account with administrator privileges.
For instructions, see “Getting Started” in the *SA User Guide: Database and Middleware Automation*.
- 3 On the Solutions > Installed tab, click the **Browse** button in the lower right corner. The Choose File dialog opens.

- 4 Browse to and select the ZIP file that you extracted in [step 1](#), and click **Open**.
- 5 Click **Import solution pack**.



Subsequent topics in this chapter assume that you have logged in to the HP DMA server.

Create a Deployable Workflow

The workflow templates provided by HP in your solution pack are read-only and cannot be deployed. To use them, you must first create your own copies.

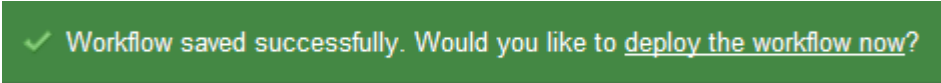
To create a deployable copy of the workflow template:

- 1 In the HP DMA web interface, go to Automation > Workflows.
- 2 From the list of workflows, select the Provision WebSphere 7 StandAlone Profile workflow template.
- 3 Click the **Copy** button in the lower left corner.
- 4 On the Documentation tab, specify the following:

Name	Name that will appear in the list of available workflows
Tags	Keywords that you can use later to search for this workflow (optional)
Type	Must be OS
Target level	Must be Server

- 5 On the Roles tab, grant Read access to at least one user or group and Write access to at least one user or group.
- 6 Click **Save**.

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



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

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

For more information about creating and working with workflows, refer to “Workflows” in the *SA User Guide: Database and Middleware Automation*.

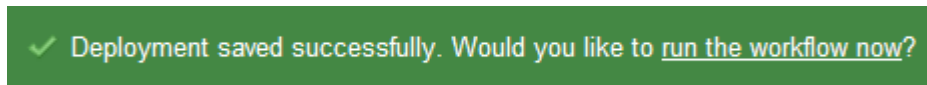
Create a Deployment

Before you can run your new workflow, you must create a deployment. A deployment associates a workflow with one or more specific targets (in this case, a server).

To create a deployment:

- 1 If you do not see the green message bar—for example, if you navigated to another page after you created your copy of the workflow template—follow these steps:

- a Go to the Automation > Deployments area.
 - b In the lower right corner, click **New deployment**.
- 2 Specify the following:
- | | |
|-----------------|---|
| Name | Name that will appear in the list of available deployments. |
| Workflow | From the drop-down list, select the workflow that you just created. |
| Schedule | Frequency with which the workflow will run. If you select None, the workflow will run only once when you explicitly tell it to run. |
- 3 From the list of AVAILABLE servers on the left side of the Targets area, click the **ADD** link for the server where the workflow will run.
- 4 On the Parameters tab, specify values for all required parameters (see [Reference Information](#) on page 24 for a list of these parameters).
- If you do not want to explicitly enter the values here, you can create a policy that stores the values and then reference that policy in your deployment (see [Using a Policy to Specify Parameter Values](#) on page 40).
- 5 Click **Save**.
- Your new deployment now appears in the list of available workflows, and the following message is displayed:



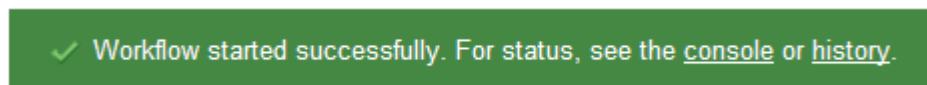
- 6 Click the **run the workflow now** link in the green message area.

Run Your Workflow

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

To run the workflow:

- 1 If you do not see the green message bar—for example, if you navigated to another page after you created your deployment—follow these steps:
 - a Go to the Automation > Run area.
 - b In the list of WORKFLOWS on the left side, select the workflow that you created.
 - c In the list of DEPLOYMENTS in the center, double-click the deployment that you just created.
 - 2 In the list of targets on the left side, select the check box for the target where you want to run the workflow.
 - 3 In the lower right corner of the Run Workflow page, click the **Run workflow** button.
- The following message is displayed.



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

View the Results

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

To view the progress of the workflow as the deployment proceeds, click the workflow name in the upper box on the Console page.

To view the outcome of a specific step, select that step in the left box in the Output area. Informational messages are displayed in the right box, and the values of any output parameters are listed.

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

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



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

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

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

View the Dashboard

You can also use the Dashboard to view a summary of HP DMA automation activity over the last 30 days. Click **Database & Middleware Automation** in the title bar to open the Dashboard.

3 Customizing this Solution

Each workflow included in the Application Server Provisioning solution has a set of required parameters. If you provide correct values for all required parameters, each workflow will achieve its stated objective (see [Workflows](#) on page 8).

To further customize the solution for your environment, you can also provide values for the optional parameters associated with a workflow. You can use the optional parameters to do the following things:

- [Enable WebSphere Administrative Security](#)
- [Configure SSL Certificate Management](#)
- [Specify Ports](#)
- [Create a Development Server](#)
- [Omit the Administrative Console or Default Application](#)

This chapter shows you how to expose the optional parameters and customize this solution for your environment.

All the parameters for each workflow are listed in the [Reference Information](#) on page 24.



The information presented in this chapter assumes the following:


- HP DMA is installed and operational.
- At least one suitable target server is available (see [Supported HP DMA Platforms](#) on page 93).
- You are logged in to the HP DMA web interface using an account with Administrator privileges.
- You have successfully run a copy of the Provision WebSphere 7 StandAlone Profile workflow template against at least one target server in your environment (see [Quick Start](#) on page 12 for instructions).

Expose the Optional Parameters

By default, most of the optional parameters for the workflows in this solution are not visible in the deployment. This is easy to change.

To expose optional parameters:

- 1 In the HP DMA web interface, go to Automation > Workflows.
- 2 From the list of workflows, select your deployable copy of the workflow that you want to customize.
- 3 Go to the Workflow tab.

- 4 Click the blue arrow  to the left of the Validate *<workflowDescription>* Parameters step to expand the list of parameters.
Here *<workflowDescription>* refers to the specific workflow with which you are working. For example: Validate WebSphere 7 Stand Alone Parameters.
- 5 From the drop-down list, select - **User Selected** - for each parameter that you want to customize in the deployment.
- 6 Click **Save**.

Enable WebSphere Administrative Security

The following parameters are used to enable WebSphere administrative security:

Table 1 Administrative Security Parameters

Parameter Name	WebSphere Install Option	Description
Enable Security	PROF_enableAdminSecurity	Enables administrative security for WebSphere to prevent unauthorized access to administrative tasks. By default this option is set to true. This option is valid for cell, deployment manager, and stand-alone profiles. Valid values are true, false.
Admin User	PROF_adminUserName	If Enable Security is “true,” this user name and password will be needed to access the Integrated Solutions Console and other WebSphere administrative tools. When WebSphere creates the profile, this user will be mapped to the Administrator role.
Admin Password	PROF_adminPassword	

See [Table 2: Optional Parameters for Provision WebSphere 7 StandAlone Profile](#) on page 26 for additional details.



To protect the Admin Password, be sure to specify it by using a policy rather than typing it in on the Deployment screen. This will ensure that the password does not appear in clear text. See [Using a Policy to Specify Parameter Values](#) on page 40 for more information.



For more information about WebSphere security features, see “Securing applications and their environment” in the *WebSphere Application Server, Network Deployment, Version 7.0* documentation:

<http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/welc6topsecuring.html>

Configure SSL Certificate Management

WebSphere Application Server includes certificate management features that enable you to encrypt communications between a server and a client by using the Secure Sockets Layer (SSL) protocol.

The workflows included in this solution enable you to create personal and root signing certificates when you create a profile. The following optional parameters are used to create the certificates:

Table 2 Certificate Management Parameters

Parameter Name	WebSphere Install Option	Description
Keystore Password	PROF_keyStorePassword	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
Personal CertDN	PROF_personalCertDN	Distinguished name of the personal certificate. For example: CN=dmalab-example.com,OU=WAS7 LabCell,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	PROF_personalCertValidity Period	Amount of time in years that the personal certificate is valid. Default is one year.
Signing CertDN	PROF_signingCertDN	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	PROF_signingCertValidity Period	Amount of time in years that the root certificate is valid. Default is 15 years.



To protect the Keystore Password, be sure to specify it by using a policy rather than typing it in on the Deployment screen. This will ensure that the password does not appear in clear text. See [Using a Policy to Specify Parameter Values](#) on page 40 for more information.



For more information about WebSphere security features, see “Securing applications and their environment” in the *WebSphere Application Server, Network Deployment, Version 7.0* documentation in the IBM InfoCenter

<http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/welc6topsecuring.html>

Specify Ports

When WebSphere Application Server creates a profile, it assigns a set of ports to that profile. You can use the optional parameters listed in [Table 3](#) to determine how this set of ports is derived.

- If Default Ports is true, WebSphere will assign its default set of ports—without testing to determine whether those ports are in use.
- If Default Ports is false, and you do not specify a Starting Port or a Ports File, WebSphere will automatically generate a set of recommended ports.

The recommended port values may be different than the default port values based on the availability of the default ports.

- If you specify a Starting Port, WebSphere will generate and assign ports sequentially from that starting port.

If you specify a Starting Port, be sure to set Default Ports to false.

- If you specify a Ports File, WebSphere will assign the ports that you specify.

If you specify a Ports File, be sure to set Validate Ports to true and Default Ports to false.

Table 3 Port Parameters

Parameter Name	WebSphere Install Option	Description
Default Ports	PROF_defaultPorts	Provides the option to assign default ports to a profile. Valid values are true or false. <ul style="list-style-type: none"> • 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.
Ports File	PROF_portsFile	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.

Table 3 Port Parameters

Parameter Name	WebSphere Install Option	Description
Starting Port	PROF_startingPort	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	PROF_validatePorts	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.

Create a Development Server

You can instruct the WebSphere Application Server installer to create a “developer” server for testing purposes. This results in a faster installation, because only a subset of the production server components are installed.

Table 4 Development Server Parameter

Parameter Name	WebSphere Install Option	Description
Developer Server	N/A	Use this parameter only in development environments to help with start up time. The only valid value is true. Do not use in production environments.

Omit the Administrative Console or Default Application

When you install WebSphere Application Server using one of the workflows in this solution, you can choose to prevent either of the following optional features from being installed:

- Administrative Console
- Default Application

This would be important, for example, if you have a security requirement that precludes the installation of these components.

Table 5 Omit Action Parameter

Parameter Name	WebSphere Install Option	Description
Omit Action	PROF_omitAction	Enables you to prevent certain optional features from being installed. Valid values are deployAdminConsole or defaultAppDeployAndConfig. You may only specify one of these options.

4 Troubleshooting

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

- [Target Type](#) on page 22
- [User Permissions and Related Requirements](#) on page 22
- [Discovery in HP Server Automation](#) on page 23

For additional information, refer to the “Troubleshooting” chapter in the *HP Server Automation User Guide: Database and Middleware Automation*. (If you are using HP DMA version 1.00, instead see the *HP Database and Middleware Automation Installation Guide*.)

Target Type

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

User Permissions and Related Requirements

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

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

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

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

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

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



Permissions work differently in HP Server Automation. Refer to the *HP Server Automation User Guide: Database and Middleware Automation* for more information.

Discovery in HP Server Automation

HP DMA uses a process called “discovery” to find information about the server, network, and database instances on a target machine.

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

In HP Server Automation, you must explicitly initiate the process of discovery—it is not automatic. Refer to the *HP Server Automation User Guide: Database and Middleware Automation* for instructions.

A Reference Information

This appendix contains the following information:

- A comprehensive list of required and optional [Parameters by Workflow](#) on page 24
- A list of [WebSphere Application Server Version 7.0 Documentation](#) on page 39

Parameters by Workflow

This section lists the required and optional parameters for all workflow templates included in this solution pack:

- [Provision WebSphere 7 StandAlone Profile](#) on page 24
- [Provision WebSphere 7 and Deployment Manager](#) on page 27
- [Provision WebSphere 7 and Custom Node](#) on page 29
- [Create StandAlone From Existing WebSphere 7 Install](#) on page 32
- [Create Custom Node from Existing WebSphere 7 Install](#) on page 34
- [Provision IBM HTTP Server 7 and Plug-In](#) on page 37



The following characters are not permitted in any parameters that specify a user name, cell name, node name, or profile name:

`/ \ * , ; = + ? | < > & % ' " [] > # $ ^ { }`

Provision WebSphere 7 StandAlone Profile

[Table 1](#) lists the required parameters used in this workflow, and [Table 2](#) lists the optional parameters.

Table 1 Required Parameters for Provision WebSphere 7 StandAlone Profile

Parameter Name	Default	Description
Binary Archive	no default	Fully qualified path to the compressed software package on the target machine.
Call Wrapper	see description	Command that will execute the step as a specific user (by default, <code>sudo su - root /opt/datapalette/jython/jython</code> on UNIX targets and <code>jython</code> running as Administrator on Windows targets).

Table 1 Required Parameters for Provision WebSphere 7 StandAlone Profile

Parameter Name	Default	Description
Cell Name	no default	Unique cell name that does not contain any of the special characters listed above. 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	no default	Fully qualified path where the compressed software will be extracted on the target machine.
Host Name	no default	Hostname or IP address of the target machine.
Install Location	no default	Fully qualified path where WebSphere Application Server will be installed. For example: /opt/IBM/WebSphere/AppServer
License Acceptance	false	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 special characters listed above. 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 special characters listed above.
Profile Path	no default	Fully qualified path to the profile. For example: /opt/IBM/WebSphere/AppServer/profiles/AppServer1.
Profile Type	standAlone	Because this workflow creates a stand-alone profile, the value must be standAlone.
Response File	no default	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	Name of the application server that will be created under the profile.

Table 2 Optional Parameters for Provision WebSphere 7 StandAlone Profile

Parameter Name	Default	Description
Admin Password	no default	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	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 special characters listed above.
Default Ports	false	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	Use this parameter for development environments only to help with start up time. Valid value is true. Do not use in production environments.
Keystore Password	no default	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
Omit Action	no default	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	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	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	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.

Provision WebSphere 7 and Deployment Manager

Table 3 lists the required parameters used in this workflow, and Table 4 lists the optional parameters.

Table 3 Required Parameters for Provision WebSphere 7 and Deployment Manager

Parameter Name	Default	Description
Binary Archive	no default	Fully qualified path to the compressed software package on the target machine.
Call Wrapper	see description	Command that will execute the step as a specific user (by default, sudo su – root /opt/datapalette/jython/jython on UNIX targets and jython running as Administrator on Windows targets).
Cell Name	no default	Unique cell name that does not contain any of the special characters listed above. 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	no default	Fully qualified path where the compressed software will be extracted on the target machine.
Host Name	no default	Hostname or IP address of the target machine.
Install Location	no default	Fully qualified path where WebSphere Application Server will be installed. For example: /opt/IBM/WebSphere/AppServer.
License Acceptance	false	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 special characters listed above. 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 special characters listed above.
Profile Path	no default	Fully qualified path to the profile. For example: /opt/IBM/WebSphere/AppServer/profiles/AppServer1.
Profile Type	management	Because this workflow creates a Deployment Manager profile, the value must be management.

Table 3 Required Parameters for Provision WebSphere 7 and Deployment Manager

Parameter Name	Default	Description
Response File	no default	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	Name of the application server that will be created under the profile.
Server Type	DEPLOYMENT_MANAGER	Specifies the type of management profile. Specify DEPLOYMENT_MANAGER for a deployment manager server.

Table 4 Optional Parameters for Provision WebSphere 7 and Deployment Manager

Parameter Name	Default	Description
Admin Password	no default	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	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 special characters listed above.
Default Ports	false	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	Use this parameter for development environments only to help with start up time. Valid value is true. Do not use in production environments.
Keystore Password	no default	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
Omit Action	no default	Enables you to prevent certain optional features from being installed. Valid values are deployAdminConsole or defaultAppDeployAndConfig. You may only specify one of these options.

Table 4 Optional Parameters for Provision WebSphere 7 and Deployment Manager

Parameter Name	Default	Description
Personal CertDN	no default	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	One year	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	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.
Signing CertDN	no default	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 years	Amount of time in years that the root certificate is valid.
Starting Port	no default	Starting port number that the profile will use to generate and assign port values. Port values are assigned sequentially from the Starting Port. Do not specify this parameter if you specify Default Ports or Ports File.
Validate Ports	false	Indicates that the ports should be validated to ensure that they are not already in use. Valid values are true or false. You should use this option if you specify a Ports File.

Provision WebSphere 7 and Custom Node

Table 5 lists the required parameters used in this workflow, and Table 6 lists the optional parameters.

Table 5 Required Parameters for Provision WebSphere 7 and Custom Node

Parameter Name	Default	Description
Binary Archive	no default	Fully qualified path to the compressed software package on the target machine.

Table 5 Required Parameters for Provision WebSphere 7 and Custom Node

Parameter Name	Default	Description
Call Wrapper	see description	Command that will execute the step as a specific user (by default, sudo su – root /opt/datapalette/jython/jython on UNIX targets and jython running as Administrator on Windows targets).
Cell Name	no default	Unique cell name that does not contain any of the special characters listed above. 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	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	Fully qualified path where the compressed software will be extracted on the target machine.
Host Name	no default	Hostname or IP address of the target machine.
Install Location	no default	Fully qualified path where WebSphere Application Server will be installed. For example: /opt/IBM/WebSphere/AppServer.
License Acceptance	no default	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 special characters listed above. 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 special characters listed above.
Profile Path	no default	Fully qualified path to the profile. For example: /opt/IBM/WebSphere/AppServer/profiles/AppServer1.
Profile Type	custom	Because this workflow creates a Custom Node profile, the value must be custom.
Response File	no default	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.

Table 6 Optional Parameters for Provision WebSphere 7 and Custom Node

Parameter Name	Default	Description
Dmgr Admin Password	no default	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	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 special characters listed above.
Dmgr HostName	no default	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.
Dmgr Port	no default	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.
Federate Later	no default	If true, the new custom node will be federated during profile creation. If false, you must federate it later by using the addNode command.
Keystore Password	no default	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
Personal CertDN	no default	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	no default	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	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.

Table 6 Optional Parameters for Provision WebSphere 7 and Custom Node

Parameter Name	Default	Description
Signing CertDN	no default	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	no default	Amount of time in years that the root certificate is valid. Default is 15 years.

Create StandAlone From Existing WebSphere 7 Install

Table 7 lists the required parameters used in this workflow, and Table 8 lists the optional parameters.

Table 7 Required Parameters for Create StandAlone From Existing WebSphere 7 Install

Parameter Name	Default	Description
Call Wrapper	see description	Command that will execute the step as a specific user (by default, sudo su – root /opt/datapalette/jython/jython on UNIX targets and jython running as Administrator on Windows targets).
Cell Name	no default	Unique cell name that does not contain any of the special characters listed above. 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	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Host Name	no default	Hostname or IP address of the target machine.
Install Location	no default	Fully qualified path where WebSphere Application Server is installed. For example: /opt/IBM/WebSphere/AppServer.
Node Name	no default	Unique node name that cannot contain any of the special characters listed above. 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 special characters listed above.
Profile Path	no default	Fully qualified path to the profile. For example: /opt/IBM/WebSphere/AppServer/profiles/AppServer1.

Table 7 Required Parameters for Create StandAlone From Existing WebSphere 7 Install

Parameter Name	Default	Description
Response File	no default	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	Name of the application server that will be created under the profile.

Table 8 Optional Parameters for Create StandAlone From Existing WebSphere 7 Install

Parameter Name	Default	Description
Admin Password	no default	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	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 special characters listed above.
Custom Response File	no default	This parameter provides the option to specify a fully qualified path to an existing response file on the target machine.
Default Ports	no default	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	Use this parameter for development environments only to help with start up time. Valid value is true. Do not use in production environments.
Keystore Password	no default	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
Omit Action	no default	Enables you to prevent certain optional features from being installed. Valid values are deployAdminConsole or defaultAppDeployAndConfig. You may only specify one of these options.

Table 8 Optional Parameters for Create StandAlone From Existing WebSphere 7 Install

Parameter Name	Default	Description
Personal CertDN	no default	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,
Personal CertValidity Period	One year	Amount of time in years that the personal certificate is valid.
Ports File	no default	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.
Signing CertDN	no default	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 years	Amount of time in years that the root certificate is valid.
Starting Port	no default	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	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.

Create Custom Node from Existing WebSphere 7 Install

Table 9 lists the required parameters used in this workflow, and Table 10 lists the optional parameters.

Table 9 Required Parameters for Create Custom Node from Existing WebSphere 7 Install

Parameter Name	Default	Description
Call Wrapper	see description	Command that will execute the step as a specific user (by default, sudo su – root /opt/datapalette/jython/jython on UNIX targets and jython running as Administrator on Windows targets).

Table 9 Required Parameters for Create Custom Node from Existing WebSphere 7 Install

Parameter Name	Default	Description
Cell Name	no default	Unique cell name that does not contain any of the special characters listed above. 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	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	no default	Hostname or IP address of the target machine.
Install Location	no default	Fully qualified path where WebSphere Application Server will be installed. For example: /opt/IBM/WebSphere/AppServer.
Node Name	no default	Unique node name that cannot contain any of the special characters listed above. 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 special characters listed above.
Profile Path	no default	Fully qualified path to the profile. For example: /opt/IBM/WebSphere/AppServer/profiles/AppServer1.
Response File	no default	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the profile creation.

Table 10 Optional Parameters for Create Custom Node from Existing WebSphere 7 Install

Parameter Name	Default	Description
Custom Response File	no default	This parameter provides the option to specify a fully qualified path to an existing response file on the target machine.
Dmgr Admin Password	no default	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	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 special characters listed above.

Table 10 Optional Parameters for Create Custom Node from Existing WebSphere 7 Install

Parameter Name	Default	Description
Dmgr HostName	no default	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.
Dmgr Port	no default	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.
Federate Later	no default	If true, the new custom node will be federated during profile creation. If false, you must federate it later by using the addNode command.
Keystore Password	no default	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
Personal CertDN	no default	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	One year	Amount of time in years that the personal certificate is valid.
Ports File	no default	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.
Signing CertDN	no default	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 years	Amount of time in years that the root certificate is valid.

Provision IBM HTTP Server 7 and Plug-In

Table 11 lists the required parameters used in this workflow, and Table 12 lists the optional parameters.

Table 11 Required Parameters for Provision IBM HTTP Server 7 and Plug-In

Parameter Name	Default	Description
Admin Port	no default	The port on which the HTTP administration web server will run. This is usually 8008.
Binary Archive	no default	Fully qualified path to the compressed software package on the target machine.
Call Wrapper	see description	Command that will execute the step as a specific user (by default, sudo su – root /opt/datapalette/jython/jython on UNIX targets and jython running as Administrator on Windows targets).
Create Admin Auth	no default	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	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	Fully qualified path where the compressed software will be extracted on the target machine.
Http Port	no default	The port on which the web server will listen. Usually, this is set to 80.
Install Location	no default	Fully qualified path where IBM HTTP Server will be installed. For example: /opt/IBM/HTTPServer
Install Plugin	no default	Determines whether or not the WebSphere Application Server Plug-In is installed. Valid options are true or false.
License Acceptance	no default	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true for the installation to continue.
Response File	no default	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	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.

Table 12 Optional Parameters for Provision IBM HTTP Server 7 and Plug-In

Parameter Name	Default	Description
Admin Auth Password	no default	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	Confirms the Admin Auth Password.
Admin Auth User	no default	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 special characters listed above.
Set Up Admin Group	no default	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	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	If set to true, this parameter enables you to administer the IBM HTTP Server by using the WebSphere Application Server administrative console.
WebSphere Hostname	no default	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.

WebSphere Application Server Version 7.0 Documentation

For the current list of hardware and software requirements, as well as supported platforms for IBM WebSphere Application Server Version 7.0, see:

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

For IBM WebSphere Application Server Version 7.0 product documentation, see:

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

For IBM Red Book resources for WebSphere Application Server Version 7.0, see:

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

B Using a Policy to Specify Parameter Values

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


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

Create the 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 page 41).

To create a policy that provides parameter values:

- 1 Go to Automation > Policies.
- 2 Click **New Policy**.
- 3 In **Name** box, specify the name of the policy
- 4 For each parameter value that you want to provide using this policy, perform the following actions on the Attributes tab:
 - a From the drop-down list, select the type of attribute:
 - A Text attribute contains simple text that users can view while deploying and running workflows.
 - A List attribute contains a comma-delimited list of values (or a large amount of text not suitable for a Text attribute).
 - A Password attribute contains simple text, but it is obfuscated so that users cannot see the text.
 - b In the text box to the left of the Add button, specify the name of the attribute.
For your convenience, this name should be similar to the parameter name used in the pertinent workflow (or workflows).
 - c Click **Add**.
 - d In the new text box to the right of the attribute's name, enter a value for this attribute.

To remove an attribute, click the “Remove”  button.
- 5 On the Roles tab, grant Read and Write permission to any additional users and groups who will be using this policy. By default, any groups to which you belong have Read and Write permission.
- 6 Click the **Save** button (lower right corner).

Extract a Policy

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

To extract a policy:

- 1 Go to Automation > Workflows.
- 2 Select the Workflow that you want to work with.
- 3 Click the Extract Policy link at the bottom of the screen.
- 4 Specify values for each attribute listed.
- 5 *Optional:* Remove any attributes that you do not want to use.
 - ▶ Extracted policies only use Text type attributes. Therefore, passwords are not obfuscated when you specify them in an extracted policy. You can, however, delete an automatically extracted attribute and then add a new one of type Password.
- 6 *Optional:* Add any new attributes that you want to use.
- 7 *Optional:* On the Roles tab, select the Read box for any users or user groups that you want to be able to use this policy to provide parameter values in a Deployment. Select the Write box for any users or groups that you want to be able to modify this Policy (add or remove attributes).
- 8 Click **Save**.

Reference a Policy in a 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 *SA User Guide: Database and Middleware Automation* 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 text box to the right of the parameter name, type the first few characters of the policy name.

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

C Using this Solution with HP Server Automation

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

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

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

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

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

- *HP Server Automation User Guide: Application Deployment Manager* (version 9.10 and later)
- *HP Server Automation User Guide: Database and Middleware Automation User Guide* (version 9.10 and later)