

HP Database and Middleware Automation

For Red Hat Enterprise Linux, Solaris, AIX, and Windows®

Software Version: 9.15

Database Compliance User Guide

Document Release Date: October 2012

Software Release Date: October 2012



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2010 - 2012 Hewlett-Packard Development Company, L.P.

Trademark Notices

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

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

UNIX® is a registered trademark of The Open Group.

Support

Visit the HP Software Support Online web site at:

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

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

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

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

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

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

To find more information about access levels, go to:

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

Documentation Updates

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

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

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

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

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

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

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

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

Contents

Contents	5
Audience	8
Document Map	9
Important Terms	10
The Database Compliance Solution	11
What this Solution Includes	11
What this Solution Does	11
Database Compliance Report	12
Database Compliance Detail Report	13
Compliance Audit Results Email	14
Supported Products and Platforms	15
Compliance Quick Start	16
Import the Solution Pack	17
Create a Deployable Workflow	20
Create a Deployment	21
Run Your Workflow	24
View the Results	26
View a Compliance Report	28
Workflow Details	29
Run Oracle Compliance Audit	30
Prerequisites for this Workflow	31
How this Workflow Works	32
How to Run this Workflow	36
Sample Scenarios	39
Parameters for Run Oracle Compliance Audit	44
Run MS SQL Compliance Audit	46
Prerequisites for this Workflow	47

How this Workflow Works	48
How to Run this Workflow	53
Sample Scenarios	55
Parameters for Run MS SQL Compliance Audit	60
Run Sybase Compliance Audit	62
Prerequisites for this Workflow	63
How this Workflow Works	64
How to Run this Workflow	68
Sample Scenarios	71
Parameters for Run Sybase Compliance Audit	76
Reference Information	79
Compliance Benchmark Information	80
Compliance Benchmark Mappings for Oracle Database	81
Compliance Benchmark Mappings for Microsoft SQL Server	88
Compliance Benchmark Mappings for Sybase ASE	91
Database Product Documentation	93
Oracle Database Product Documentation	93
Microsoft SQL Server Documentation	93
Sybase Adaptive Server Enterprise Documentation	93
Additional Resources	94
Security Benchmark Documentation	94
HP DMA Documentation	94
Tips and Best Practices	95
How a Solution Pack is Organized	96
How to Expose Additional Workflow Parameters	100
How to Use a Policy to Specify Parameter Values	101
Create a Policy	101
Extract a Policy	102
Reference the Policy in the Deployment	102
How to Import a File into the Software Repository	104
Troubleshooting	105
Target Type	105

User Permissions and Related Requirements 105

Discovery in HP Server Automation 105

Glossary 107

Audience

This solution is designed for the following people:

- Database engineers who are responsible for establishing and maintaining database security processes. In most cases, a mandate has been delivered by the security team to bring the environment into compliance with specific standards and benchmarks. It is typically the database engineer's responsibility to ensure that this happens.
- Database administrators who are responsible for establishing, maintaining, and reporting on security compliance.

To use this solution effectively, you should be familiar with the pertinent security configuration benchmarks for the database products used in your environment. You should also be familiar with the terms used in those benchmarks (see the [Additional Resources](#) on page 94).

Document Map

The following table shows you how to navigate this guide:

Topic	Description
The Database Compliance Solution	General information about this solution, including what it contains and what it does.
Compliance Quick Start	A step-by-step tutorial that shows you how to run a compliance audit and view the results.
Workflow Details	Information about each of the workflows included in this solution, including: prerequisites, how it works, how to run it, sample scenarios, and a list of input parameters.
Reference Information	Detailed mappings of the CIS benchmark to the PCI and SOX benchmarks for each database product, links to database product documentation, and links to more information about HP DMA.
Tips and Best Practices	Simple procedures that you can use to accomplish a variety of common HP DMA tasks.
Troubleshooting	Tips for solving common problems.

Important Terms

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

- In HP DMA, a **workflow** executes a process —such as installing a software product or checking a database instance for compliance with a specific security benchmark.
- A workflow consist of a sequence of **steps**. Each step performs a very specific task. Steps can be shared among workflows.
- 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 this solution pack, you must first create a deployable copy of that template and then customize that copy for your environment.
- 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.

- 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.

Additional terms are defined in the [Glossary](#) on page 107.

Tip: For more information about the basic structure of a solution pack, including HP DMA screen images, see [How a Solution Pack is Organized](#) on page 96.

Chapter 1

The Database Compliance Solution

The HP DMA Database Compliance solution provides tools that you can use to audit your database environment for compliance with a specific security benchmark. These tools enable you to:

- Assess the level of compliance across your database environment
- Identify security vulnerabilities present in a specific database instance
- Expedite the resolution of database configuration issues
- Reduce the complexity and cost of performing compliance audits
- Schedule regular "lights-out" automated compliance audits

By consistently using the tools provided in this solution, you can better protect sensitive information, reduce the risk of unauthorized access, and accurately demonstrate compliance with relevant security benchmarks.

What this Solution Includes

This solution includes the following three workflows. You can run these workflows on demand or create a schedule to run fully automated "lights out" compliance audits at regular intervals.

Workflow Name	Database Product Audited
Run Oracle Compliance Audit	Oracle Database Server versions 10g and 11g
Run MS SQL Compliance Audit	Microsoft SQL Server 2005 and 2008
Run Sybase Compliance Audit	Sybase Adaptive Server Enterprise version 15

What this Solution Does

The workflows in this solution perform a compliance audit against the following security benchmarks:

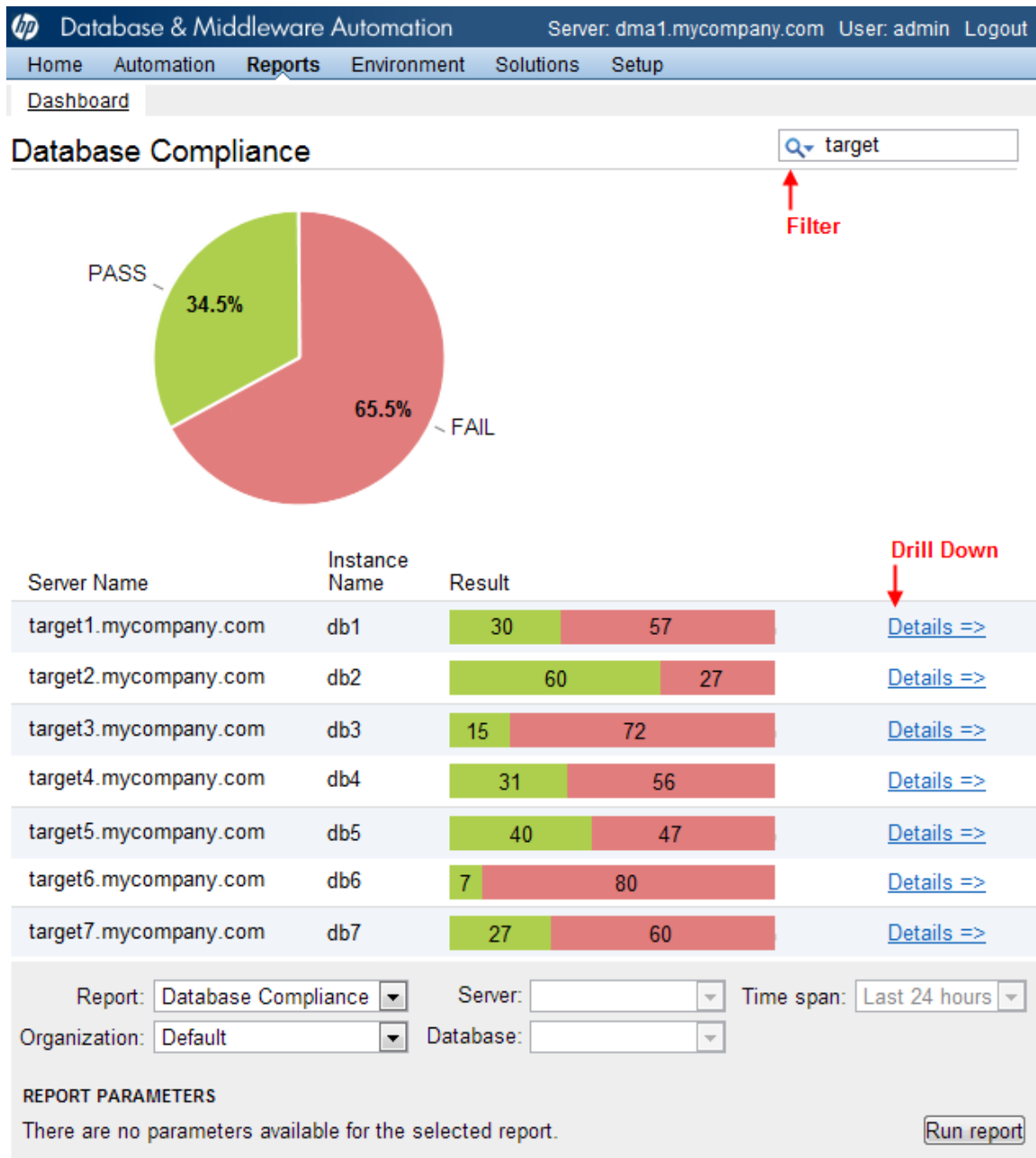
- Center for Internet Security (CIS) security configuration benchmarks
- Payment Card Industry (PCI) data security standard
- Sarbanes-Oxley (SOX) requirements

These benchmarks document the settings and procedures required for the secure installation, configuration, and operation of a specific database environment. By bringing your environment into compliance with these benchmarks, you can better protect it from related threats. For information about the specific security benchmark versions implemented in this solution, see [Compliance Benchmark Information](#) on page 80.

This solution provides three types of reports that you can use to actively track compliance status in your environment and satisfy compliance reporting requirements.

Database Compliance Report

This summary report shows you the number of compliance checks that passed and failed for each database instance in your environment that was audited.

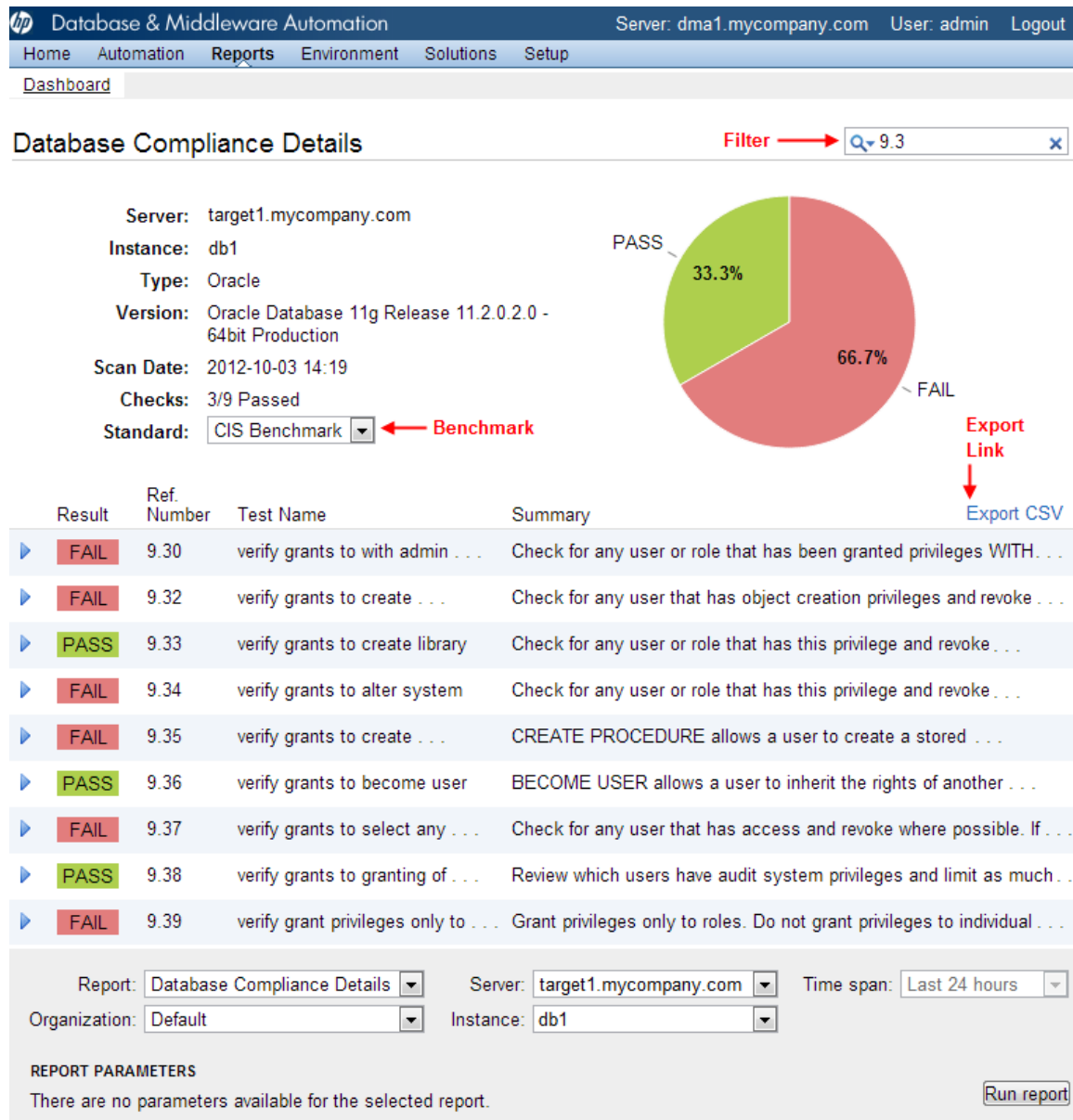


In this example, the report is filtered such that only those servers in the Default organization whose host names include the string "target" appear in the list. The pie chart shows the percentage of CIS benchmark checks that passed and failed for the database instances in the filtered list.

You can drill down to the detailed audit results for a specific database instance by clicking the Details link for that instance.

Database Compliance Detail Report

The Database Compliance Detail report shows you the result of each benchmark check performed for a specific database instance.



In this report, you can specify which compliance benchmark (CIS, PCI, or SOX) is used to format the results. The pie chart shows the percentage of checks in the specified benchmark that passed and failed for this particular database instance.

You can filter this report based on the information associated with each compliance check. In this example, only those checks that contain the string "9.3" appear in the table. Both the pie chart and the Checks indicator change when you apply filter conditions.

You can export the contents of this report to a comma-separated value (CSV) file. This is useful, for example, if you want to include the detailed results in a spreadsheet.

Compliance Audit Results Email

You can instruct the workflows in this solution to send an email message containing the results of the compliance audit for each target database instance. This email message contains the result of every benchmark check performed. It is formatted according to the benchmark that you specify.

You can use the HP DMA scheduling feature to run fully automated "lights-out" compliance audits. The email report can be sent to any valid email address, enabling you to analyze the detailed results from any email-enabled device.

The following example shows the beginning of the compliance audit results email message for a CIS audit.

Note: The email message contains the result of every check performed. Only the first five checks are shown here.

From: CISComplianceAuditor@mycompany.com

Sent: Thursday, September 6, 2012 8:42 AM

To: DBAdminTeam@mycompany.com, DBAdminMgr@mycompany.com

Subject: Weekly Oracle Database Compliance Audit Results for db1 on target1.mycompany.com

Compliance Audit Results

Compliance CIS Number	Compliance Test Name	Test Result	Reason
1.13	Oracle software owner host account	PASS	Locking the user account will deter attackers from leveraging this account in brute force authentication attacks
2.09	Default Accounts (created by Oracle)	FAIL	The default Oracle installation locks and expires the installation accounts. These accounts should be left locked and expired unless absolutely necessary. Check to ensure these accounts have not been unlocked. Lock and expire the system accounts.
2.05	listener.ora	FAIL	The listener must not be called by the default name as it is commonly known. A distinct name must be selected. Edit \$ORACLE_HOME/network/admin/listener.ora and change the default name.
2.13	Service or SID name	PASS	Do not use the default SID or service name of ORCL. It is commonly know and used in many automated attacks.

Supported Products and Platforms

The HP DMA Database Compliance workflows are supported on Red Hat Enterprise Linux, Solaris, AIX, and Windows platforms.

Operating Systems

For specific operating system versions supported by each workflow, see the *HP Database and Middleware Automation version 9.15 Support Matrix* available on the HP Software Product Manuals web site:

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

Hardware Requirements

For HP DMA hardware requirements, see the *HP Server Automation Quick Reference: SA Installation Requirements* or the *HP Server Automation Standard/Advanced Installation Guide*.

For database product hardware and software requirements, see the pertinent [Database Product Documentation](#) on page 93.

Software Requirements

This solution requires HP Server Automation version 9.13 with DMA 9.13 Hotfix 2 (or later).

Chapter 2

Compliance Quick Start

This tutorial shows you how to run a compliance audit for Oracle Database on a single target. It also shows you how to access and view a compliance report.

The tutorial will guide you through the following steps:

1. [Import the Solution Pack](#) on next page
2. [Create a Deployable Workflow](#) on page 20
3. [Create a Deployment](#) on page 21
4. [Run Your Workflow](#) on page 24
5. [View the Results](#) on page 26
6. [View a Compliance Report](#) on page 28

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

See [Parameters for Run Oracle Compliance Audit](#) on page 44 for descriptions of available input parameters, including default values.

The information presented in this tutorial assumes the following:

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

Note: This tutorial uses a very simple scenario to help you get started quickly. For detailed information about how the workflows in this solution pack work and how you can customize them for your environment, see the [Workflow Details](#) on page 29.

Import the Solution Pack

Before you can use the workflows in the HP DMA Database Compliance solution, you must import that solution into HP DMA.

The following instructions assume that you have purchased the Database Compliance solution pack.

To import the solution pack:

1. Get the latest Database Compliance solution pack from HP Software Support. To do this, follow these steps:
 - a. Go to the following web site: <http://www.hp.com/go/hpssoftwaresupport>
 - b. Go to the Self-solve tab, and sign in using your HP Passport credentials (see [Support](#) on page 3 for more information).
 - c. On the Advanced Search page, specify the following search criteria:

Product:	HP Database and Middleware AutomationSolution Packs
Version:	9.15
Operating System:	Linux
Document Type:	Patches
 - d. Click **Search**.
 - e. In the search results, locate and click the link for the Database Compliance solution pack (for example: DB Comp 9.15).
 - f. Click the DOWNLOAD PATCH link, and download the ZIP file. For example:
DBMASP_00046.zip
 - g. From that ZIP file, extract the file that contains the solution pack. For example:
DBCompliance_v9_15_ALL.zip
2. On the system where you downloaded the solution pack, log in to HP DMA. To do this, follow these steps:
 - a. In a web browser, go to the following URL: `http://<DMAServer>/dma/login`
Here, `<DMAServer>` represents the host name (or IP address) of your HP DMA server.
 - b. Specify your HP DMA Login Name and Password, and click **Login**.
Be sure to log in to the DMA server using an account with administrative privileges.
3. On the Solutions > Installed page, click the **Browse** button in the lower right corner. The Choose File dialog opens.

Note: This button and the dialog that subsequently opens may have different names depending on the browser that you are using.
4. Locate and select the solution pack file that you extracted in step 1.g (for example: DBCompliance_v9_15_ALL.zip), and click **Open**.
5. Click **Import solution pack**.

Tip: To view basic information about the solution pack, hover your mouse over its name in the right pane.

Database & Middleware Automation

Server: dma1.mycompany.com User: admin Logout

[Home](#) [Automation](#) [Reports](#) [Environment](#) **[Solutions](#)** [Setup](#)

[Installed](#) [History](#)

Installed Solutions

Successfully imported [HP Server Automation Database Compliance Solution Pack](#)

SOLUTION PACKS

HP Server Automation Application Server Patching Solution Pack
Version 9.15

HP Server Automation Application Server Provisioning Solution Pack
Version 9.15

HP Server Automation Database Compliance Solution Pack
Version 9.15

HP Server Automation Database Release Management Solution Pack
Version 9.15

HP Server Automation Discovery Solution Pack
Version 9.15

DETAILS

- Name: HP Server Automation Database Compliance Solution Pack
- Version: 9.15
- Targets: 2
- Installed: 28 Aug, 2012
- Description: Provides CIS Level I and II auditing for Oracle, SQL Server, and Sybase. Build 29807

© 2006–2012 Hewlett-Packard Development Company, L.P.
Web Server: 9.13.1 Repository: 9.10.0

Tip: To view detailed information about the solution pack, including a list of the workflows and reports that it contains, click its name in the left pane.

The screenshot displays the HP Database & Middleware Automation web interface. The top navigation bar includes the HP logo, the title "Database & Middleware Automation", and user information: "Server: dma1.mycompany.com", "User: admin", and a "Logout" link. Below this is a secondary navigation bar with tabs: "Home", "Automation", "Reports", "Environment", "Solutions", and "Setup". The "Solutions" tab is active, and a sub-tab "Installed" is selected.

The main content area is titled "HP Server Automation Database Compliance Solution Pack" with "Version 9.15" below it. There are four sub-tabs: "General", "Policies", "Workflows", and "Steps". The "Workflows" tab is selected.

On the left side, there is a list of three workflow items, each with a small icon and a text label:

- Run MS SQL Compliance Audit
- Run Oracle Compliance Audit (highlighted with a mouse cursor)
- Run Sybase Compliance Audit

On the right side, a detailed list of steps for the selected workflow is shown, numbered 1 through 12:

- Gather Parameters for Oracle Compliance
- Gather Advanced Parameters for Oracle Compliance
- Prepare Server
- Validate Compliance Parameters
- Get Oracle Home
- Prepare Oracle Instance
- Get Listener Names
- Audit Unix or Linux OS Specific Settings
- Audit Installation and Patch
- Audit Directory and File Permissions
- Audit Oracle Parameter Settings
- Audit Encryption Configuration

At the bottom of the main content area, there is a red "X" icon followed by the word "DELETE".

The footer contains copyright information: "© 2006–2012 Hewlett-Packard Development Company, L.P." and "Web Server: 9.13.1 Repository: 9.10.0".

Create a Deployable Workflow

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

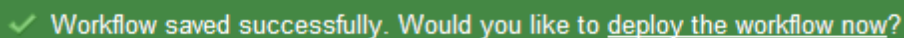


Read-only workflows are not deployable. You can create a deployable workflow by making a copy of a workflow template.¹

To create a deployable copy of the workflow template:

1. In the DMA web interface, go to Solutions > Installed.
2. In the left pane, click the Database Compliance Solution Pack.
3. Go to the Workflows tab.
4. From the list of workflows, select the [Run Oracle Compliance Audit](#) on page 30 workflow template.
5. Click the **Copy** button in the lower left corner.
6. 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 – OS (this will be selected as a result of the copy)
 - Target level – Instance (this will be selected as a result of the copy)
7. On the Roles tab, grant Read access to at least one user or group and Write access to at least one user or group.
8. 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?](#)

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

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

Create a Deployment

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

To create a deployment:

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

- From the list of AVAILABLE targets on the left side of the Targets area, click the **ADD** link for the instance where the workflow will run.

hp Database & Middleware Automation

Home **Automation** Reports Environment Solutions Setup

Workflows Steps Functions Policies Deployments Run Console History

New deployment

Targets Parameters Roles

Name: My Deployment - Oracle Compliance

Workflow: My Copy of Run Oracle Compliance Audit [VIEW WORKFLOW](#)

Schedule: None

Targets

AVAILABLE	SELECTED
ORCL1.MYCOMPANY.COM ADD ALL	ORCL1.MYCOMPANY.COM REMOVE ALL
inst1 ADD ← Instance	inst1 REMOVE
inst2 ADD	
inst3 ADD	
ORCL2.MYCOMPANY.COM ADD ALL	
DB1 ADD	
DB2 ADD	
ORCL3.MYCOMPANY.COM ADD ALL	
LN_DS ADD	
NY_DS ADD	
ORCL4.MYCOMPANY.COM ADD ALL	

Save or **CANCEL**

4. On the Parameters tab, specify values for the following input parameters:

hp Database & Middleware Automation

Home Automation Reports Environment Solutions Setup

Workflows Steps Functions Policies Deployments Run Console History

New deployment

Targets Parameters Roles

Gather Parameters for Oracle Compliance

Compliance Type: Text

Compliance type that will be audited by the workflow. Compliance types supported: CIS, PCI, SOX. Will be defaulted to CIS.

Excluded Compliance Checks: Text

Optional: Checks to exclude from of Compliance Checks

Inventory Files: Text

Optional: Comma separated list of fully qualified Oracle inventory files. If not specified, default to /etc/orainst.loc, /var/opt/oracle/orainst.loc, or %ProgramFiles%\Oracle\Inventory.

Gather Advanced Parameters for Oracle Compliance

Email Addresses to Receive Report: Text

*Optional. Provided an email address or multiple email addresses separated by commas without spaces that you would like to receive an email of the results of the compliance tests run against the target specified.

[Restore defaults](#) [Save](#) or [CANCEL](#)

Note: These are a subset of the required parameters for this workflow. Parameters that are not visible in the deployment will have default values. See the [Parameters for Run Oracle Compliance Audit](#) on page 44 for descriptions of all available input parameters for this workflow, including default values.

5. Click **Save**.

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

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

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

Run Your Workflow

Now you are ready to run your workflow against the target 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: show
 - 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 on the right side, select the deployment that you just created.
2. Select the target selector check box for the instance where you want to run the workflow.

Database & Middleware Automation

Home Automation Reports Environment Solutions Setup

Workflows Steps Functions Policies Deployments **Run** Console History

Run Workflow

Workflow name: My Copy of Run Oracle Compliance Audit

Deployment name: My Deployment - Oracle Compliance

My Copy of Run Oracle Compliance Audit: My Deployment - Oracle Compliance

ORCL1.MYCOMPANY.COM

inst1 (Target selector)

Instance, Server

SELECT ALL

Gather Parameters for Oracle Compliance 1

Parameters

Compliance Type: CIS

Excluded Compliance Checks:

Inventory Files: /etc/orainst.loc

Gather Advanced Parameters for Oracle Compliance 2

Parameters


Email Addresses to Receive Report: DBAdminTeam@mycompany.com

Prepare Server 3

No parameters.

Run workflow

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

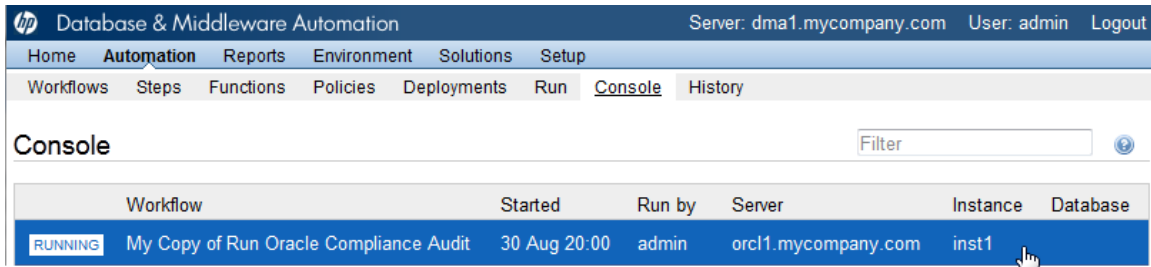
 Workflow started successfully. For status, see the [console](#) or [history](#).

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

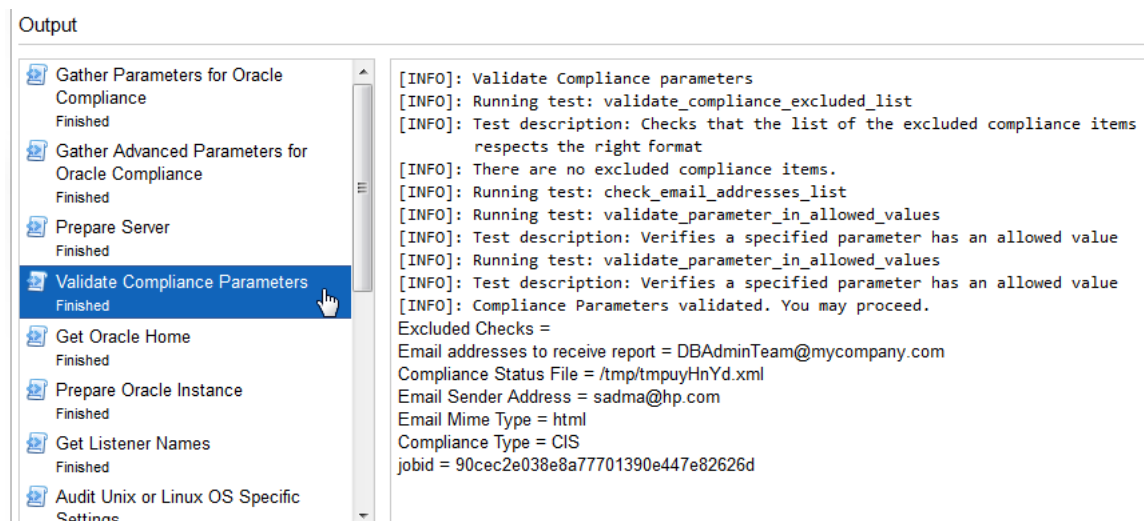
View the Results

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

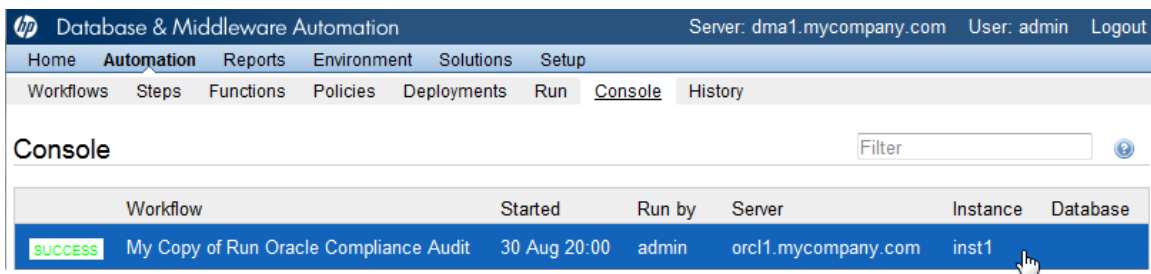
To view the progress of the workflow as the deployment proceeds, click the workflow name in the upper box on the Console page.



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



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



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 DMA server during the time period specified in the Filter box.

To view step-by-step results, select the row in the table that corresponds to your deployment.

Database & Middleware Automation Server: dma1.mycompany.com User: admin Logout

Home Automation Reports Environment Solutions Setup

Workflows Steps Functions Policies Deployments Run Console History

History Filter Last 8 hours

Workflow	Started	Run by	Server	Instance	Database	Status
Run Oracle Compliance Audit Run Oracle Compliance Audit CIS	30 Aug 20:00	admin	orcl1.mycompany.com	inst1		SUCCESS
Sybase Release Management Sybase ASE 15.0.3 Release Mgt	30 Aug 19:30	sa	syb1.mycompany.com	LN_DS	mytestdb	SUCCESS
Sybase Release Management Sybase ASE 15.0.3 Release Mgt	30 Aug 19:17	sa	syb1.mycompany.com	LN_DS	mytestdb	FAILURE
Sybase Release Management Sybase ASE 15.0.3 Release Mgt	30 Aug 19:30	sa	syb1.mycompany.com	LN_DS	mytestdb	SUCCESS
Sybase Release Management Sybase ASE 15.0.3 Release Mgt	30 Aug 19:17	sa	syb1.mycompany.com	LN_DS	mytestdb	FAILURE

Output Errors Header

[Gather Parameters for Oracle Compliance](#)
02:01:03 - 02:01:12 Exit: 0
[INFO]: Gather Parameters for SQL Server Compliance

[Gather Advanced Parameters for Oracle Compliance](#)
02:01:22 - 02:01:32 Exit: 0
[INFO]: Gather Advanced Parameters for SQL Server Compliance

[Prepare Server](#)
02:01:54 - 02:02:12 Exit: 0

[Validate Compliance Parameters](#)
02:02:41 - 02:02:59 Exit: 0
[INFO]: Validate Compliance parameters
[INFO]: Running test: validate_compliance_excluded_list
[INFO]: Test description: Checks that the list of the excluded compliance items respects the right format
[INFO]: There are no excluded compliance items.
[INFO]: Running test: check_email_addresses_list
[INFO]: Running test: validate_parameter_in_allowed_values
[INFO]: Test description: Verifies a specified parameter has an allowed value
[INFO]: Running test: validate_parameter_in_allowed_values

© 2006–2012 Hewlett-Packard Development Company, L.P.
Web Server: 9.13.1 Repository: 9.10.0

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 a Compliance Report

The workflows in this solution pack provide three different types of compliance reports:

Report Type	Description
Compliance Audit Results Email	You can instruct the workflows in this solution to send an email message containing the results of the compliance audit for each target database instance. This email message contains the result of every benchmark check performed. It is formatted according to the benchmark that you specify.
Database Compliance Report	This summary report shows you the number of compliance checks that passed and failed for each database instance in your environment that was audited.
Database Compliance Detail Report	The Database Compliance Detail report shows you the result of each benchmark check performed for a specific database instance.

To access the Compliance Audit Results Email, be sure to specify your email address in the Email Addresses to Receive Report parameter when you create your deployment.

To access the Database Compliance reports:

1. Go to the Reports page.
2. At the bottom of the page, specify the following settings:

For the Database Compliance Report:

Report: Server: Time span:

Organization: Database:

REPORT PARAMETERS

There are no parameters available for the selected report.

Because this report lists the latest compliance audit reports for all targets in the specified organization, you do not specify a Server, Database, or Time span.

For the Database Compliance Detail Report:

Report: Server: Time span:

Organization: Instance:

REPORT PARAMETERS

There are no parameters available for the selected report.

Specify the Server and Instance that you selected when you created your deployment.

For both reports, be sure to specify the organization where your target resides.

3. Click **Run report**.

Chapter 3

Workflow Details

This solution pack contains the following workflows:

- [Run Oracle Compliance Audit](#) on next page
- [Run MS SQL Compliance Audit](#) on page 46
- [Run Sybase Compliance Audit](#) on page 62

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

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

Tip: Detailed instructions are provided in the "How to Use this Workflow" topic for 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 15).
- You are logged in to the HP DMA web interface.
- You have permission to create, edit, and deploy copies of the workflows included in this solution pack.

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

Run Oracle Compliance Audit

The [Run Oracle Compliance Audit](#) workflow enables you to audit an Oracle Database instance for compliance with the one of the following security benchmarks:

- Center for Internet Security (CIS) security configuration benchmarks
- Payment Card Industry (PCI) data security standard
- Sarbanes-Oxley (SOX) requirements

The workflow performs CIS Level 1 and Level 2 auditing and can identify more than 175 compliance related problems.

The workflow performs the checks included in the CIS benchmark and then maps those CIS checks to the benchmark type that you specify in the Compliance Type parameter. The audit summary email will match the Compliance Type that you specify.

To understand how the CIS benchmarks for Oracle Database map to the PCI and SOX requirements, see [Compliance Benchmark Mappings for Oracle Database](#) on page 81.

For links to the CIS, PCI, and SOX standards, see [Additional Resources](#) on page 94.

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 Scenarios	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 [Run Oracle Compliance Audit](#) workflow:

- You are using HP Database and Middleware Automation version 9.13 with the DMA 9.13 Hotfix 2 (or later).
- You have installed the Database Compliance solution pack.

For more information about prerequisites for Oracle Database, refer to the [Oracle Database Product Documentation](#) on page 93.

How this Workflow Works

This workflow performs the following actions:

- Prepares to run the workflow by gathering information about the target Oracle Database instance and validating parameter values.
- Audits the various configuration settings specified in the pertinent benchmark.
- Composes and sends an email containing the results of the audit.

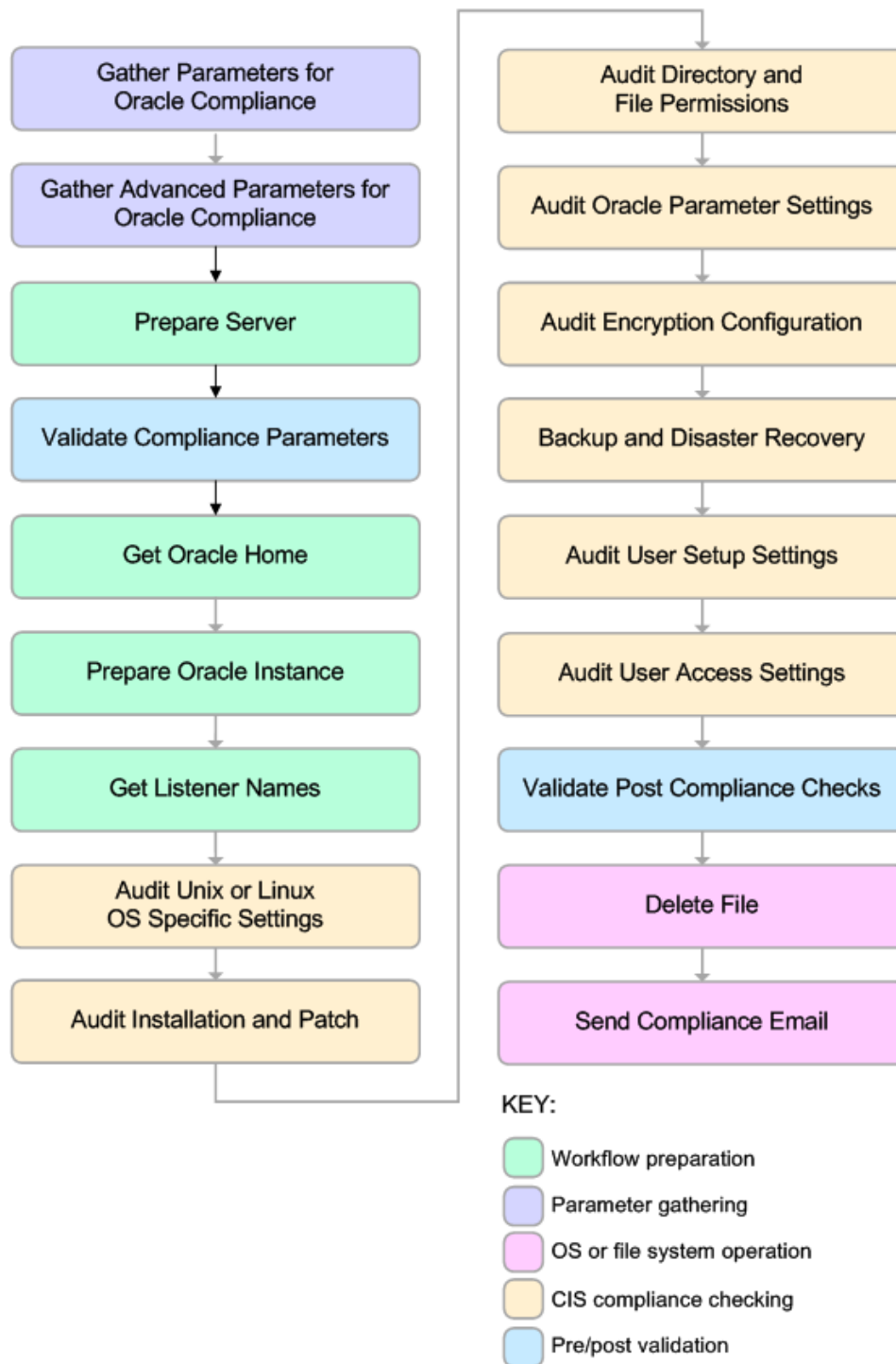
Validation Checks Performed

This workflow validate the following conditions:

1. The Oracle Home derived in the Get Oracle Home step is a fully qualified path that exists on the target server.
2. The workflow can connect to the Oracle SID derived in the Get Oracle Home step.
3. Any Excluded Checks specified by the user refer to actual CIS checks.
4. Any email addresses specified are valid addresses.
5. The specified email MIME type is either "text" or "html."
6. The workflow can create the temporary file that will store the compliance check results.

Steps Executed

The [Run Oracle Compliance Audit](#) 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 Run Oracle Compliance Audit

Workflow Step	Description
Gather Parameters for Oracle Compliance	<p>This step gathers three pieces of information that the workflow needs to perform the compliance audit:</p> <ul style="list-style-type: none"> • The type of compliance audit to perform (CIS, PCI, or SOX) • A list of compliance checks to exclude from the audit (if any) • The location of the Oracle inventory files. <p>All parameters are optional.</p>
Gather Advanced Parameters for Oracle Compliance	<p>This step gathers the information that the workflow needs to create and deliver the compliance audit report via email. It also enables you to specify the name of the most recent Oracle patch that was applied to the pertinent Oracle Home (derived from the Oracle inventory file).</p>
Validate Compliance Parameters	<p>This step validates the input parameters specified in the previous steps. It validates the list of excluded checks to ensure that all specified checks in the list correspond to actual Center for Internet Security (CIS) benchmark items. It also validates the email information to ensure that all specified email addresses are valid and that the MIME format of the email message is either text or html.</p> <p>The step then creates the path to the temporary file that will store the results of the current audit as the workflow is running. This file is deleted after the audit report is sent.</p>
Prepare Server	<p>This step prepares the Server Wrapper and Instance Wrapper, which enable subsequent steps to be executed by the OS administrator user or the owner of the database or middleware software.</p>
Get Oracle Home	<p>This step determines the value of ORACLE_HOME from the Oracle inventory file on UNIX targets or from the Registry on Windows targets.</p>
Prepare Oracle Instance	<p>This step gathers the information that the workflow will need to access the pertinent Oracle instance.</p>
Get Listener Names	<p>This step gets the names of the Oracle listeners that are running.</p> <p>Results can be filtered based on one or more ORACLE_HOMEs, one or more ORACLE_SIDs, or both.</p>
Audit Unix or Linux OS Specific Settings	<p>This step audits the scorable UNIX/Linux related recommendations in Section 1, Operating System Specific Settings, of the Center for Internet Security (CIS) Security Configuration Benchmarks for Oracle 9i/10g and Oracle Database Server 11g.</p>

Steps Used in Run Oracle Compliance Audit (continued)

Workflow Step	Description
Audit Installation and Patch	This step audits the scorable recommendations in Section 2, Installation and Patch, of the Center for Internet Security (CIS) Security Configuration Benchmarks for Oracle 9i/10g and Oracle Database Server 11g.
Audit Directory and File Permissions	This step audits the scorable recommendations in Section 3, Oracle Directory and File Permissions, of the Center for Internet Security (CIS) Security Configuration Benchmarks for Oracle 9i/10g and Oracle Database Server 11g.
Audit Oracle Parameter Settings	This step audits the scorable recommendations in Section 4, Oracle Parameter Settings, of the Center for Internet Security (CIS) Security Configuration Benchmarks for Oracle 9i/10g and Oracle Database Server 11g.
Audit Encryption Configuration	This step audits the scorable recommendations in Section 5, Encryption Specific Settings, of the Center for Internet Security (CIS) Security Configuration Benchmarks for Oracle 9i/10g and Oracle Database Server 11g.
Backup and Disaster Recovery	This step audits the scorable recommendations in Section 7, Backup and Disaster Recovery, of the Center for Internet Security (CIS) Security Configuration Benchmarks for Oracle 9i/10g and Oracle Database Server 11g.
Audit User Setup Settings	This step audits the scorable recommendations in Section 9, Oracle Profile (User) Access Settings, of the Center for Internet Security (CIS) Security Configuration Benchmarks for Oracle 9i/10g and Oracle Database Server 11g.
Validate Post-Compliance Checks	This step reads the temporary file that contains the results of the compliance audit and prints the audit results to the HP DMA Console. If email addresses were specified, it also creates a report in HTML format that will be emailed to those addresses by a later step in the workflow.
Delete File	This step deletes the specified file on the target server.
Send Compliance Email	This step sends the previously generated compliance audit report to the specified email addresses.

Note: For input parameter descriptions and defaults, see [Parameters for Run Oracle Compliance Audit](#) on page 44.

How to Run this Workflow

The following instructions show you how to customize and run the [Run Oracle Compliance Audit](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in [Parameters for Run Oracle Compliance Audit](#) on page 44.

Note: Before following this procedure, review the [Prerequisites for this Workflow](#) on page 31, and ensure that all requirements are satisfied.

To use the Run Oracle Compliance Audit workflow:

1. Create a deployable copy of the workflow (see [Create a Deployable Workflow](#) on page 20).
2. Determine the values that you will specify for the following parameters:

Parameters Defined in this Step: Gather Parameters for Oracle Compliance

Parameter Name	Default Value	Required	Description
Compliance Type	CIS	optional	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Excluded Compliance Checks	no default	optional	Comma-separated list of compliance checks to exclude from the audit. For example: 1.2, 2, 3.*, 5*, 6.1.2 Note: Make sure that the checks specified here correspond with the compliance audit type (CIS, PCI, or SOX) that you are running.

Parameters Defined in this Step: Gather Parameters for Oracle Compliance (continued)

Parameter Name	Default Value	Required	Description
Inventory Files	see description	optional	Comma-separated list of fully qualified Oracle inventory files. If this parameter is not specified, it defaults to one of the following values: Linux or AIX: <code>/etc/oraInst.loc</code> Solaris: <code>/var/opt/oracle/oraInst.loc</code> Windows: <code>%ProgramFiles%\Oracle\Inventory</code>

Parameters Defined in this Step: Gather Advanced Parameters for Oracle Compliance

Parameter Name	Default Value	Required	Description
Email Addresses to Receive Report	no default	optional	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.

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 [How to Expose Additional Workflow Parameters](#) on page 100

See [Parameters for Run Oracle Compliance Audit](#) on page 44 for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment (see [Create a Deployment](#) on page 21 for instructions).
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment (see [Run Your Workflow](#) on page 24 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.

Information about each compliance check is displayed in the step output on the Console (and the History page) for each of the auditing steps. A summary of the compliance audit is also displayed in the step output for the Validate Post-Compliance Checks step.

To view the reports:

A compliance audit summary in HTML format is emailed to all parties on the Email Addresses to Receive Report list (see an example of the [Compliance Audit Results Email](#) on page 14).

After you run this workflow, you can generate two types of compliance reports on the Reports page:

- [Database Compliance Report](#) on page 12
- [Database Compliance Detail Report](#) on page 13

To access these reports, see [View a Compliance Report](#) on page 28.

Sample Scenarios

This topic shows you how to use various parameters to achieve the following compliance audit scenarios in your environment using the [Run Oracle Compliance Audit](#) workflow.

Scenario 1: Perform a Partial CIS Compliance Audit and Email the Results

In the scenario, the following checks are excluded from the audit:

- Section 8: Oracle Profile (User) Setup Settings
- Section 9: Oracle Profile (User) Access Settings

A summary report is sent to the three parties listed in the Email Addresses to Receive Report parameter.

Parameter Name	Example Value	Description
Compliance Type	CIS	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Email Addresses to Receive Report	DBAdminTeam@mycompany.com, DBAdminMgr@mycompany.com, CustomerSupportTeam@mycompany.com	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.
Email Mime Type	HTML	Type of email format that will be used for the compliance audit report: text or html.
Email Sender Address	CISComplianceAuditor@mycompany.com	Email address that will appear in the From field when the compliance audit report is emailed.
Email Subject Line	Weekly Oracle Database Compliance Audit Results	Text that will appear in the Subject field when the compliance audit report is emailed.

Parameter Name	Example Value	Description
SMTP Server Address	smtp001.west.mycompany.com	Fully-qualified host name or IP address of the SMTP server that will send the email containing the compliance audit report.
Excluded Compliance Checks	8.*,9.*	<p>Comma-separated list of compliance checks to exclude from the audit. For example:</p> <p>1.2, 2, 3.*, 5*, 6.1.2</p> <p>Note: Make sure that the checks specified here correspond with the compliance audit type (CIS, PCI, or SOX) that you are running.</p>

Note: Some of these parameters are not exposed by default in the deployment. See [How to Expose Additional Workflow Parameters](#) on page 100.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see [Parameters for Run Oracle Compliance Audit](#) on page 44).

Scenario 2: Perform a Full PCI Compliance Audit and Email the Results

In the scenario, no checks are excluded from the audit. A summary report is sent to the three parties listed in the Email Addresses to Receive Report parameter.

Parameter Name	Example Value	Description
Compliance Type	PCI	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Email Addresses to Receive Report	DBAdminTeam@mycompany.com, DBAdminMgr@mycompany.com, CustomerSupportTeam@mycompany.com	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.
Email Mime Type	HTML	Type of email format that will be used for the compliance audit report: text or html.
Email Sender Address	PCIComplianceAuditor@mycompany.com	Email address that will appear in the From field when the compliance audit report is emailed.
Email Subject Line	Weekly Oracle Database Compliance Audit Results	Text that will appear in the Subject field when the compliance audit report is emailed.
SMTP Server Address	smtp001.west.mycompany.com	Fully-qualified host name or IP address of the SMTP server that will send the email containing the compliance audit report.

Note: Some of these parameters are not exposed by default in the deployment. See [How to Expose Additional Workflow Parameters](#) on page 100.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see [Parameters for Run Oracle Compliance Audit](#) on page 44).

Scenario 3: Perform a Full SOX Compliance Audit and Email the Results

In the scenario, no checks are excluded from the audit. A summary report is sent to the three parties listed in the Email Addresses to Receive Report parameter.

Parameter Name	Example Value	Description
Compliance Type	SOX	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Email Addresses to Receive Report	DBAdminTeam@mycompany.com, DBAdminMgr@mycompany.com, CustomerSupportTeam@mycompany.com	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.
Email Mime Type	HTML	Type of email format that will be used for the compliance audit report: text or html.
Email Sender Address	SOXComplianceAuditor@mycompany.com	Email address that will appear in the From field when the compliance audit report is emailed.
Email Subject Line	Weekly Oracle Database Compliance Audit Results	Text that will appear in the Subject field when the compliance audit report is emailed.
SMTP Server Address	smtp001.west.mycompany.com	Fully-qualified host name or IP address of the SMTP server that will send the email containing the compliance audit report.

Note: Some of these parameters are not exposed by default in the deployment. See [How to Expose Additional Workflow Parameters](#) on page 100.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see [Parameters for Run Oracle Compliance Audit](#) on page 44).

Scenario 4: Perform a Full CIS Compliance Audit and Display the Results on the HP DMA Console

In the scenario, all scorable checks are performed, and the compliance audit report is displayed only on the HP DMA Console. In this case, a summary report is not emailed. This scenario would be appropriate for initial testing.

It is not necessary to specify any input parameters in this scenario unless the Oracle Databaseinventory file is located in a non-standard directory.

Parameter Name	Example Value	Description
Compliance Type	CIS	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements

Note: Some of these parameters are not exposed by default in the deployment. See [How to Expose Additional Workflow Parameters](#) on page 100.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see [Parameters for Run Oracle Compliance Audit](#) on next page).

Parameters for Run Oracle Compliance Audit

The following tables describe the required and optional input parameters for this workflow. Some of these parameters are not initially visible in a deployment (see [How to Expose Additional Workflow Parameters](#) on page 100). For most parameters, if you do not specify a value for a parameter, a default value is assigned.

For information about which steps use which parameters, see [How this Workflow Works](#) on page 32.

Parameters Defined in this Step: Gather Parameters for Oracle Compliance

Parameter Name	Default Value	Required	Description
Compliance Type	CIS	optional	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Excluded Compliance Checks	no default	optional	Comma-separated list of compliance checks to exclude from the audit. For example: 1.2, 2, 3.*, 5*, 6.1.2 Note: Make sure that the checks specified here correspond with the compliance audit type (CIS, PCI, or SOX) that you are running.
Inventory Files	see description	optional	Comma-separated list of fully qualified Oracle inventory files. If this parameter is not specified, it defaults to one of the following values: Linux or AIX: <code>/etc/oraInst.loc</code> Solaris: <code>/var/opt/oracle/oraInst.loc</code> Windows: <code>%ProgramFiles%\Oracle\Inventory</code>

Parameters Defined in this Step: Gather Advanced Parameters for Oracle Compliance

Parameter Name	Default Value	Required	Description
Email Addresses to Receive Report	no default	optional	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.
Email Mime Type	html	optional	Type of email format that will be used for the compliance audit report: text or html.
Email Sender Address	sadma@hp.com	optional	Email address that will appear in the From field when the compliance audit report is emailed.
Email Subject Line	Database Compliance Results	optional	Text that will appear in the Subject field when the compliance audit report is emailed.
Latest Patch	no default	optional	Most recent Oracle patch installed on this Oracle Home.
SMTP Server Address	localhost	optional	Fully-qualified host name or IP address of the SMTP server that will send the email containing the compliance audit report.

Run MS SQL Compliance Audit

The [Run MS SQL Compliance Audit](#) workflow enables you to audit a Microsoft SQL Server instance for compliance with the following security benchmark requirements:

- Center for Internet Security (CIS) security configuration benchmarks
- Payment Card Industry (PCI) data security standard
- Sarbanes-Oxley (SOX) requirements

The workflow performs CIS Level 1 and Level 2 auditing for a SQL Server instance. The audit identifies compliance related problems with a SQL Server instance.

The workflow performs the checks included in the CIS benchmark and then maps those CIS checks to the benchmark type that you specify in the Compliance Type parameter. The audit summary email will match the Compliance Type that you specify.

To understand how the CIS benchmarks for Oracle Database map to the PCI and SOX requirements, see [Compliance Benchmark Mappings for Oracle Database](#) on page 81.

For links to the CIS, PCI, and SOX standards, see [Additional Resources](#) on page 94.

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 Scenarios	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 [Run MS SQL Compliance Audit](#) workflow:

- You are using HP Database and Middleware Automation version 9.13 with the DMA 9.13 Hotfix 2 (or later).
- You have installed the Database Compliance solution pack.

The workflow must be able to:

- Execute `reg.exe` (Windows Server command-line registry tool), `wmic.exe` (Windows Management Instrumentation Command-line tool), and “`net`” Windows utilities on the target server. These utilities are included in the base Windows Server installations.
- Log in to the SQL Server instance using Windows-authenticated login credentials.
- Read system tables and execute system procedures upon connecting to the SQL Server instance.

For more information about prerequisites for Microsoft SQL Server, refer to the [Microsoft SQL Server Documentation](#) on page 93.

How this Workflow Works

This workflow performs the following actions:

- Prepares to run the workflow by gathering information about the target SQL Server instance and validating parameter values.
- Audits the various configuration settings specified in the pertinent CIS, SOX, or PCI benchmark.
- Composes and sends an email containing the results of the audit.

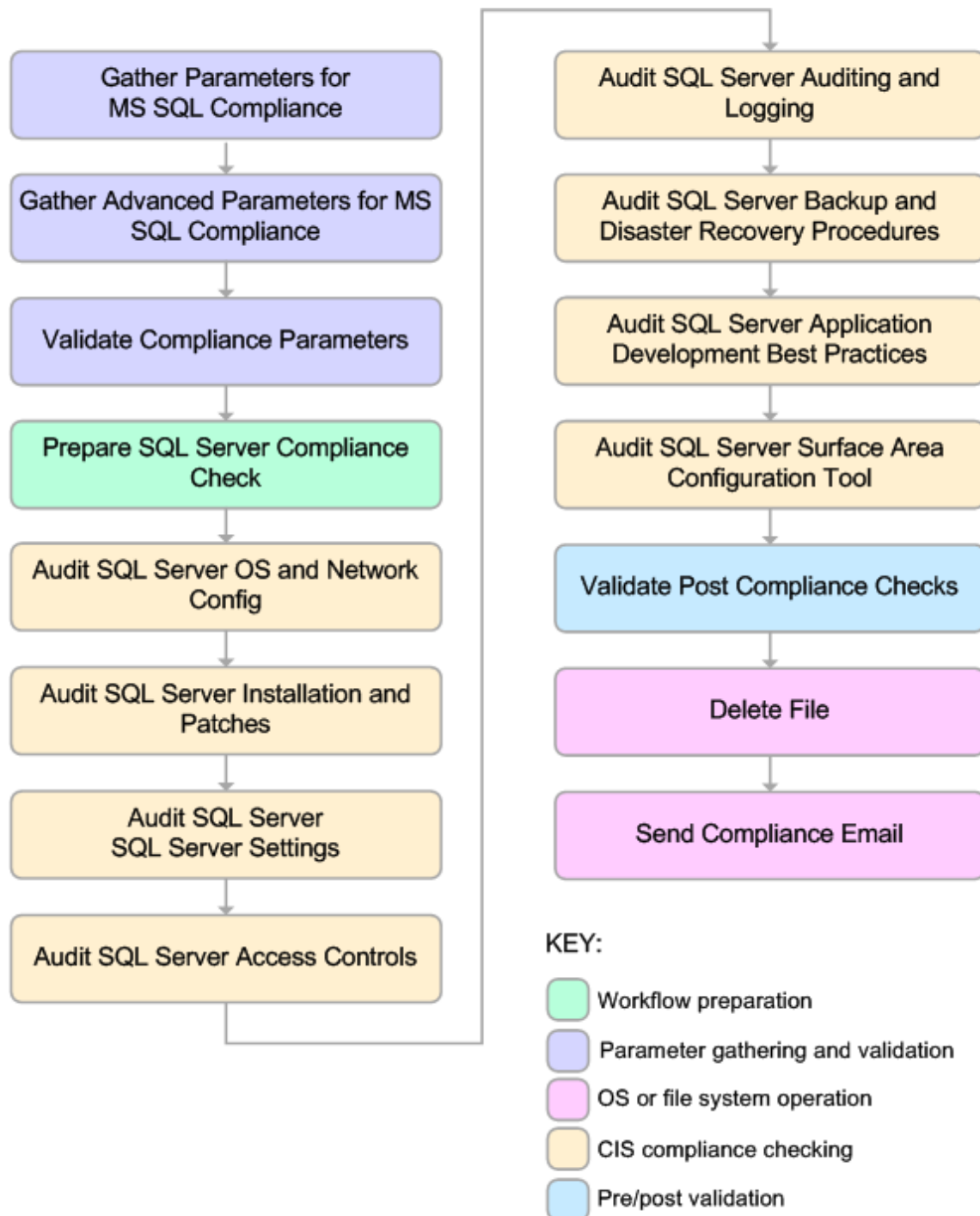
Validation Checks Performed

This workflow validates the following conditions:

1. Either `sqlcmd.exe` or `osql.exe` must be installed on the target machine.
2. Any Excluded Checks specified by the user refer to actual CIS, SOX, or PCI benchmark checks.
3. Any email addresses specified are valid addresses.
4. The specified email MIME type is either "text" or "html."
5. The workflow can create the temporary file that will store the compliance check results.

Steps Executed

The [Run MS SQL Compliance Audit](#) 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 by Run MS SQL Compliance Audit

Workflow Step	Description
Gather Parameters for MS SQL Compliance	This step gathers two pieces of information: (1) the type of compliance audit to perform and (2) the list of compliance checks to exclude from the audit.
Gather Advanced Parameters for MS SQL Compliance	This step gathers the information that the workflow needs to create and deliver the compliance audit report via email. It also enables you to specify the name of the latest available SQL Server build.
Validate Compliance Parameters	<p>This step validates the input parameters specified in the previous steps. It validates the list of excluded checks to ensure that all specified checks in the list correspond to actual Center for Internet Security (CIS) benchmark items. It also validates the email information to ensure that all specified email addresses are valid and that the MIME format of the email message is either text or html.</p> <p>The step then creates the path to the temporary file that will store the results of the current audit as the workflow is running. This file is deleted after the audit report is sent.</p>
Prepare SQL Server Compliance Check	<p>This step determines whether workflow can perform the following actions on the target system:</p> <ul style="list-style-type: none"> • Check database connectivity • Query the registry • Check the registry for SQL Server • Execute Windows Management Instrumentation (WMI) API calls • Execute the <code>net user /?</code> command <p>If the workflow can perform all of these actions, it is capable of running the Center for Internet Security (CIS) Security Configuration Benchmark compliance tests.</p>
Audit SQL Server OS and Network Config	This step audits the scorable recommendations in Section 1, Operating System and Network Specific Configuration, of the Center for Internet Security (CIS) Security Configuration Benchmark for Microsoft SQL Server 2005, version 2.0.0 (December 2011).
Audit SQL Server Installation and Patches	This step audits the scorable recommendations in Section 2, SQL Server Installation and Patches, of the Center for Internet Security (CIS) Security Configuration Benchmark for Microsoft SQL Server 2005, version 2.0.0 (December 2011).

Steps Used by Run MS SQL Compliance Audit (continued)

Workflow Step	Description
Audit SQL Server SQL Server Settings	This step audits the scorable recommendations in Section 3, SQL Server Settings, of the Center for Internet Security (CIS) Security Configuration Benchmark for Microsoft SQL Server 2005, version 2.0.0 (December 2011).
Audit SQL Server Access Controls	This step audits the scorable recommendations in Section 4, Access Controls, of the Center for Internet Security (CIS) Security Configuration Benchmarks for Microsoft SQL Server 2005, version 2.0.0 (December 2011).
Audit SQL Server Auditing and Logging	This step audits the scorable recommendations in Section 5, Auditing and Logging, of the Center for Internet Security (CIS) Security Configuration Benchmark for Microsoft SQL Server 2005, version 2.0.0 (December 2011).
Audit SQL Server Backup and Disaster Recovery Procedures	This step audits the scorable recommendations in Section 6, Backup and Disaster Recovery Procedures, of the Center for Internet Security (CIS) Security Configuration Benchmark for Microsoft SQL Server 2005, version 2.0.0 (December 2011).
Audit SQL Server Application Development Best Practices	This step audits the scorable recommendations in Section 8, Application Development Best Practices, of the Center for Internet Security (CIS) Security Configuration Benchmarks for Microsoft SQL Server 2005, version 2.0.0 (December 2011).
Audit SQL Server Surface Area Configuration Tool	This step audits the scorable recommendations in Section 9, Surface Area Configuration Tool, of the Center for Internet Security (CIS) Security Configuration Benchmarks for Microsoft SQL Server 2005, version 2.0.0 (December 2011).
Validate Post-Compliance Checks	<p>This step reads the temporary file that contains the results of the compliance audit and prints the audit results to the HP DMA Console. It also creates (or updates) the compliance metadata fields for the target.</p> <p>If email addresses were specified, it also creates a report in HTML format that will be emailed to those addresses by a later step in the workflow.</p>
Delete File	This step deletes the specified file on the target server.
Send Compliance Email	This step sends the previously generated compliance audit report to the specified email addresses.

Note: For input parameter descriptions and defaults, see [Parameters for Run MS SQL Compliance Audit](#) on page 60.

How to Run this Workflow

The following instructions show you how to customize and run the [Run MS SQL Compliance Audit](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in [Parameters for Run MS SQL Compliance Audit](#) on page 60.

Note: Before following this procedure, review the [Prerequisites for this Workflow](#) on page 47, and ensure that all requirements are satisfied.

To use the Run MS SQL Server Compliance Audit workflow:

1. Create a deployable copy of the workflow (see [Create a Deployable Workflow](#) on page 20).
2. Determine the values that you will specify for the following parameters:

Parameters Defined in this Step: Gather Parameters for SQL Server Compliance

Parameter Name	Default Value	Required	Description
Compliance Type	CIS	optional	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Excluded Checks	no default	optional	Comma-separated list of compliance checks to exclude from the audit. For example: 1.2, 2, 3.*, 5*, 6.1.2 Note: Make sure that the checks specified here correspond with the compliance audit type (CIS, PCI, or SOX) that you are running.

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 [How to Expose Additional Workflow Parameters](#) on page 100

See [Parameters for Run MS SQL Compliance Audit](#) on page 60 for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment (see [Create a Deployment](#) on page 21 for instructions).
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment (see [Run Your Workflow](#) on page 24 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.

Information about each compliance check is displayed in the step output on the Console (and the History page) for each of the audit steps.

A summary of the compliance audit is also displayed in the step output for the Validate Post Compliance Checks step.

To view the reports:

A compliance audit summary in HTML format is emailed to all parties on the Email Addresses to Receive Report list (see an example of the [Compliance Audit Results Email](#) on page 14).

After you run this workflow, you can generate two types of compliance reports on the Reports page:

- [Database Compliance Report](#) on page 12
- [Database Compliance Detail Report](#) on page 13

To access these reports, see [View a Compliance Report](#) on page 28.

Sample Scenarios

This topic shows you how to use various parameters to achieve the following compliance audit scenarios in your environment using the [Run MS SQL Compliance Audit](#) workflow.

Scenario 1: Perform a Partial CIS Compliance Audit and Email the Results

In the scenario, the following checks are excluded from the audit:

- Section 7: Replication
- Section 9: Surface Area Configuration Tool

A summary report is sent to the three parties listed in the Email Addresses to Receive Report parameter.

Parameter Name	Example Value	Description
Compliance Type	CIS	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Email Addresses to Receive Report	SQLDBAdminTeam@mycompany.com, SQLDBAdminMgr@mycompany.com, CustomerSupportTeam@mycompany.com	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.
Email Mime Type	HTML	Type of email format that will be used for the compliance audit report: text or html.
Email Sender Address	CISComplianceAuditor@mycompany.com	Email address that will appear in the From field when the compliance audit report is emailed.
Email Subject Line	Weekly MS SQL Server Database Compliance Audit Results	Text that will appear in the Subject field when the compliance audit report is emailed.

Parameter Name	Example Value	Description
SMTP Server Address	smtp001.west.mycompany.com	Fully-qualified host name or IP address of the SMTP server that will send the email containing the compliance audit report.
Excluded Compliance Checks	7.*,9.*	<p>Comma-separated list of compliance checks to exclude from the audit. For example:</p> <p>1.2, 2, 3.*, 5*, 6.1.2</p> <p>Note: Make sure that the checks specified here correspond with the compliance audit type (CIS, PCI, or SOX) that you are running.</p>

Note: Some of these parameters are not exposed by default in the deployment. See [How to Expose Additional Workflow Parameters](#) on page 100.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see [Parameters for Run MS SQL Compliance Audit](#) on page 60).

Scenario 2: Perform a Full PCI Compliance Audit and Email the Results

A summary report is sent to the three parties listed in the Email Addresses to Receive Report parameter.

Parameter Name	Example Value	Description
Compliance Type	PCI	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Email Addresses to Receive Report	SQLDBAdminTeam@mycompany.com, SQLDBAdminMgr@mycompany.com, CustomerSupportTeam@mycompany.com	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.
Email Mime Type	HTML	Type of email format that will be used for the compliance audit report: text or html.
Email Sender Address	PCISecurityAuditor@mycompany.com	Email address that will appear in the From field when the compliance audit report is emailed.
Email Subject Line	Weekly SQL Server Database Compliance Audit Results	Text that will appear in the Subject field when the compliance audit report is emailed.
SMTP Server Address	smtp001.west.mycompany.com	Fully-qualified host name or IP address of the SMTP server that will send the email containing the compliance audit report.

Note: Some of these parameters are not exposed by default in the deployment. See [How to Expose Additional Workflow Parameters](#) on page 100.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see [Parameters for Run MS SQL Compliance Audit](#) on page 60).

Scenario 3: Perform a Full SOX Compliance Audit and Email the Results

A summary report is sent to the three parties listed in the Email Addresses to Receive Report parameter.

Parameter Name	Example Value	Description
Compliance Type	SOX	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Email Addresses to Receive Report	SQLDBAdminTeam@mycompany.com, SQLDBAdminMgr@mycompany.com, CustomerSupportTeam@mycompany.com	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.
Email Mime Type	HTML	Type of email format that will be used for the compliance audit report: text or html.
Email Sender Address	SOXComplianceAuditor@mycompany.com	Email address that will appear in the From field when the compliance audit report is emailed.
Email Subject Line	Weekly SQL Server Database Compliance Audit Results	Text that will appear in the Subject field when the compliance audit report is emailed.
SMTP Server Address	smtp001.west.mycompany.com	Fully-qualified host name or IP address of the SMTP server that will send the email containing the compliance audit report.

Note: Some of these parameters are not exposed by default in the deployment. See [How to Expose Additional Workflow Parameters](#) on page 100.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see [Parameters for Run MS SQL Compliance Audit](#) on page 60).

Scenario 4: Perform a Full CIS Compliance Audit and Display the Results on the HP DMA Console

In the scenario, all scorable checks are performed, and the compliance audit report is displayed only on the HP DMA Console. In this case, a summary report is not emailed. This scenario would be appropriate for initial testing.

It is not necessary to specify any input parameters in this scenario unless the SQL Server inventory file is located in a non-standard directory.

Parameter Name	Example Value	Description
Compliance Type	CIS	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements

Note: Some of these parameters are not exposed by default in the deployment. See [How to Expose Additional Workflow Parameters](#) on page 100.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see [Parameters for Run MS SQL Compliance Audit](#) on next page).

Parameters for Run MS SQL Compliance Audit

The following tables describe the required and optional input parameters for this workflow. Some of these parameters are not initially visible in a deployment (see [How to Expose Additional Workflow Parameters](#) on page 100). For most parameters, if you do not specify a value for a parameter, a default value is assigned.

For information about which steps use which parameters, see [How this Workflow Works](#) on page 48.

Parameters Defined in this Step: Gather Parameters for MS SQL Compliance

Parameter Name	Default Value	Required	Description
Compliance Type	CIS	optional	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Excluded Checks	no default	optional	Comma-separated list of compliance checks to exclude from the audit. For example: 1.2, 2, 3.*, 5*, 6.1.2 Note: Make sure that the checks specified here correspond with the compliance audit type (CIS, PCI, or SOX) that you are running.

Parameters Defined in this Step: Gather Advanced Parameters for MS SQL Compliance

Parameter Name	Default Value	Required	Description
Email Addresses to Receive Report	no default	optional	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.
Email Mime Type	html	optional	Type of email format that will be used for the compliance audit report: text or html.
Email Sender Address	sadma@hp.com	optional	Email address that will appear in the From field when the compliance audit report is emailed.

Parameters Defined in this Step: Gather Advanced Parameters for MS SQL Compliance (continued)

Parameter Name	Default Value	Required	Description
Email Subject Line	Database Compliance Results	optional	Text that will appear in the Subject field when the compliance audit report is emailed.
Latest Build to Check for	no default	optional	The latest build of Microsoft SQL Server 2005, according to Microsoft.
SMTP Server Address	localhost	optional	Fully-qualified host name or IP address of the SMTP server that will send the email containing the compliance audit report.

Run Sybase Compliance Audit

The [Run Sybase Compliance Audit](#) workflow enables you to audit a Sybase Adaptive Server Enterprise instance for compliance with the following security benchmark requirements:

- Center for Internet Security (CIS) security configuration benchmarks
- Payment Card Industry (PCI) data security standard
- Sarbanes-Oxley (SOX) requirements

The workflow performs CIS Level 1 and Level 2 auditing for a Sybase ASE instance. The audit identifies up to 31 compliance related problems with a Sybase ASE instance.

The workflow performs the checks included in the CIS benchmark and then maps those CIS checks to the benchmark type that you specify in the Compliance Type parameter. The audit summary email will match the Compliance Type that you specify.

To understand how the CIS benchmarks for Oracle Database map to the PCI and SOX requirements, see [Compliance Benchmark Mappings for Oracle Database](#) on page 81.

For links to the CIS, PCI, and SOX standards, see [Additional Resources](#) on page 94.

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 Scenarios	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 [Run Sybase Compliance Audit](#) workflow:

- You are using HP Database and Middleware Automation version 9.13 with the DMA 9.13 Hotfix 2 (or later).
- You have installed the Database Compliance solution pack.

This workflow runs on the Red Hat Enterprise Linux operating system. For a list of the specific OS versions supported, refer to the HP DMA Version 9.15 Support Matrix (see [Supported Products and Platforms](#)).

This workflow runs against a Sybase ASE instance by default. You can also run it at the Database level, however, by making a copy and modifying the `Target Level`.

This workflow requires unchallenged `sudo` access to a user (typically `root`) who can access all required files and directories.

`isql` must be installed and accessible via the user/password settings stored in metadata. You may find these setting in the Environment screen.

For more information about prerequisites for Sybase Adaptive Server Enterprise, refer to the [Sybase Adaptive Server Enterprise Documentation](#) on page 93.

How this Workflow Works

This workflow performs the following actions:

- Prepares to run the workflow by gathering information about the target Sybase Adaptive Server Enterprise instance and validating parameter values.
- Audits the various configuration settings specified in the pertinent CIS, SOX, or PCI benchmark.
- Composes and sends an email containing the results of the audit.

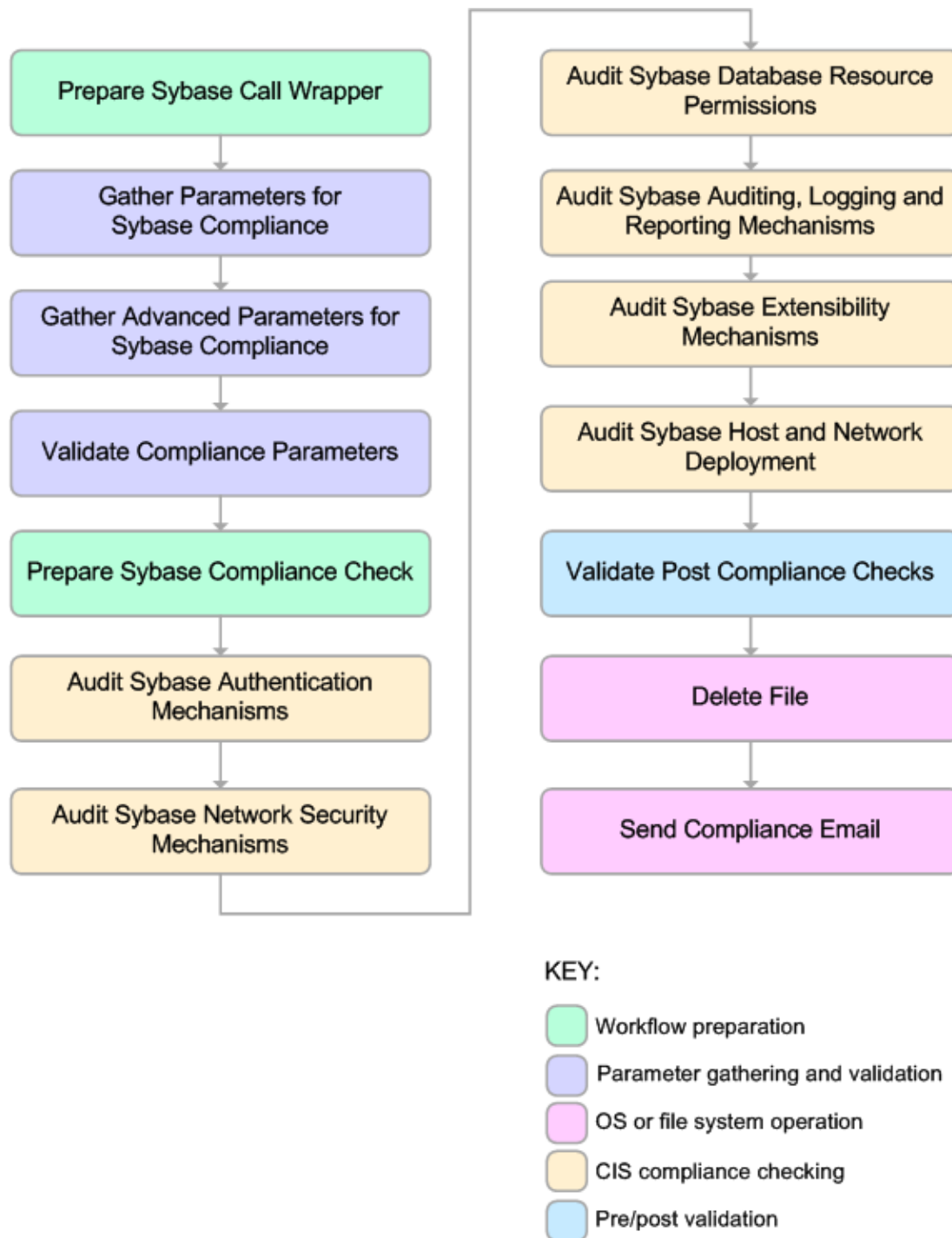
Validation Checks Performed

This workflow validates the following conditions:

1. Any Excluded Checks specified by the user refer to actual CIS, SOX, or PCI benchmark checks.
2. Any email addresses specified are valid addresses.
3. The specified email MIME type is either "text" or "html."
4. The workflow can create the temporary file that will store the compliance check results.

Steps Executed

The [Run Sybase Compliance Audit](#) 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 by Run Sybase Compliance Audit

Workflow Step	Description
Prepare Sybase Call Wrapper	This step constructs the commands that will be used to execute subsequent workflow steps as either the OS administrative user or the owner of the Sybase ASE installation.
Gather Parameters for Sybase Compliance	This step gathers two types of information: the list of compliance checks to exclude from the audit, and basic information about the Sybase ASE installation.
Gather Advanced Parameters for Sybase Compliance	This step gathers the information that the workflow needs to create and deliver the compliance audit report via email. It also enables you to specify the passwords for the various Sybase ASE user roles.
Validate Compliance Parameters	<p>This step validates the input parameters specified in the previous steps. It validates the list of excluded checks to ensure that all specified checks in the list correspond to actual Center for Internet Security (CIS) benchmark items. It also validates the email information to ensure that all specified email addresses are valid and that the MIME format of the email message is either text or html.</p> <p>The step then creates the path to the temporary file that will store the results of the current audit as the workflow is running. This file is deleted after the audit report is sent.</p>
Prepare Sybase Compliance Check	This step checks for database connectivity, verifies that the list of checks to be excluded from this compliance audit is properly formatted, and verifies that the email addresses specified are properly formatted.
Audit Sybase Authentication Mechanisms	<p>This step audits the scorable recommendations in Section 1, Authentication Mechanisms, of the Center for Internet Security (CIS) Security Configuration Benchmark for Sybase Adaptive Server Enterprise (ASE) 15.0, version 1.1.0 (December 2011).</p> <p>Checks not implemented: 1.5 - Remove unused accounts and change default passwords</p>
Audit Sybase Network Security Mechanisms	This step audits the scorable recommendations in Section 2, Network Security Mechanisms, of the Center for Internet Security (CIS) Security Configuration Benchmark for Sybase Adaptive Server Enterprise (ASE) 15.0, version 1.1.0 (December 2011).
Audit Sybase Database Resource Permissions	This step audits the scorable recommendations in Section 3, Database Resource Permissions, of the Center for Internet Security (CIS) Security Configuration Benchmark for Sybase Adaptive Server Enterprise (ASE) 15.0, version 1.1.0 (December 2011).

Steps Used by Run Sybase Compliance Audit (continued)

Workflow Step	Description
Audit Sybase Auditing, Logging and Reporting Mechanisms	This step audits the scorable recommendations in Section 4, Auditing, Logging and Reporting Mechanisms, of the Center for Internet Security (CIS) Security Configuration Benchmark for Sybase Adaptive Server Enterprise (ASE) 15.0, version 1.1.0 (December 2011).
Audit Sybase Extensibility Mechanisms	This step audits the scorable recommendations in Section 5, Extensibility Mechanisms, of the Center for Internet Security (CIS) Security Configuration Benchmark for Sybase Adaptive Server Enterprise (ASE) 15.0, version 1.1.0 (December 2011)
Audit Sybase Host and Network Deployment	This step audits the scorable recommendations in Section 6, Host and Network Deployment, of the Center for Internet Security (CIS) Security Configuration Benchmark for Sybase Adaptive Server Enterprise (ASE) 15.0, version 1.1.0 (December 2011)
Validate Post Sybase Compliance Checks	This step reads the temporary file that contains the results of the compliance audit and prints the audit results to the HP DMA Console. It also creates (or updates) the compliance metadata fields for the target. If email addresses were specified, it also creates a report in HTML format that will be emailed to those addresses by a later step in the workflow.
Delete File	This step deletes the specified file on the target server.
Send Compliance Email	This step sends the previously generated compliance audit report to the specified email addresses.

Note: For input parameter descriptions and defaults, see [Parameters for Run Sybase Compliance Audit](#) on page 76.

How to Run this Workflow

The following instructions show you how to customize and run the [Run Sybase Compliance Audit](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in [Parameters for Run Sybase Compliance Audit](#) on page 76.

Note: Before following this procedure, review the [Prerequisites for this Workflow](#) on page 63, and ensure that all requirements are satisfied.

To use the Run Sybase Compliance Audit workflow:

1. Create a deployable copy of the workflow (see [Create a Deployable Workflow](#) on page 20).
2. Determine the values that you will specify for the following parameters:

Parameters Defined in this Step: Prepare Sybase Call Wrapper

Parameter Name	Default Value	Required	Description
Call Wrapper	see description	optional	Name of the interpreter specified in the command that will execute each step as either the OS administrative user or the owner of the pertinent database or middleware product.
Sybase OS User Name	sybase	required	OS user who owns the Sybase ASE installation directory.

Parameters Defined in this Step: Gather Parameters for Sybase Compliance

Parameter Name	Default Value	Required	Description
Excluded Compliance Checks	no default	optional	Comma-separated list of compliance checks to exclude from the audit. For example: 1.2, 2, 3.*, 5*, 6.1.2 Note: Make sure that the checks specified here correspond with the compliance audit type (CIS, PCI, or SOX) that you are running.

Parameters Defined in this Step: Gather Advanced Parameters for Sybase Compliance

Parameter Name	Default Value	Required	Description
Compliance Type	CIS	optional	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Email Addresses to Receive Report	no default	optional	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.

Parameters Defined in this Step: Audit Sybase Host and Network Deployment

Parameter Name	Default Value	Required	Description
EBF Patch Level	no default	optional	Latest Express Bug Fix (EBF) patch level available from Sybase.
ESD Patch Level	no default	optional	Latest Electronic Software Distribution (ESD) patch level available from Sybase.

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 [How to Expose Additional Workflow Parameters](#) on page 100

See [Parameters for Run Sybase Compliance Audit](#) on page 76 for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment (see [Create a Deployment](#) on page 21 for instructions).
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).

9. Run the workflow using this deployment (see [Run Your Workflow](#) on page 24 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.

Information about each compliance check is displayed in the step output on the Console (and the History page) for each of the audit steps.

A summary of the compliance audit is also displayed in the step output for the Validate Post Sybase Compliance Checks step.

To view the reports:

A compliance audit summary in HTML format is emailed to all parties on the Email Addresses to Receive Report list (see an example of the [Compliance Audit Results Email](#) on page 14).

After you run this workflow, you can generate two types of compliance reports on the Reports page:

- [Database Compliance Report](#) on page 12
- [Database Compliance Detail Report](#) on page 13

To access these reports, see [View a Compliance Report](#) on page 28.

Sample Scenarios

This topic shows you how to use various parameters to achieve the following compliance audit scenarios in your environment using the [Run Sybase Compliance Audit](#) workflow.

Scenario 1: Perform a Partial CIS Compliance Audit and Email the Results

In the scenario, the following checks are excluded from the audit:

- Section 5: Extensibility Mechanisms
- Section 6: Host and Network Deployment

A summary report is sent to the three parties listed in the Email Addresses to Receive Report parameter.

Parameter Name	Example Value	Description
Compliance Type	CIS	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Email Addresses to Receive Report	SybaseDBAdminTeam@mycompany.com, SybaseDBAdminMgr@mycompany.com, CustomerSupportTeam@mycompany.com	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.
Email Mime Type	HTML	Type of email format that will be used for the compliance audit report: text or html.
Email Sender Address	CISComplianceAuditor@mycompany.com	Email address that will appear in the From field when the compliance audit report is emailed.
Email Subject Line	Weekly Sybase Database Compliance Audit Results	Text that will appear in the Subject field when the compliance audit report is emailed.

Parameter Name	Example Value	Description
SMTP Server Address	smtp001.west.mycompany.com	Fully-qualified host name or IP address of the SMTP server that will send the email containing the compliance audit report.
Excluded Compliance Checks	5.*,6.*	<p>Comma-separated list of compliance checks to exclude from the audit. For example:</p> <p>1.2, 2, 3.*, 5*, 6.1.2</p> <div>Note: Make sure that the checks specified here correspond with the compliance audit type (CIS, PCI, or SOX) that you are running.</div>

Note: Some of these parameters are not exposed by default in the deployment. See [How to Expose Additional Workflow Parameters](#) on page 100.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see [Parameters for Run MS SQL Compliance Audit](#) on page 60).

Scenario 2: Perform a Full PCI Compliance Audit and Email the Results

A summary report is sent to the three parties listed in the Email Addresses to Receive Report parameter.

Parameter Name	Example Value	Description
Compliance Type	PCI	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Email Addresses to Receive Report	SybaseDBAdminTeam@mycompany.com, SybaseDBAdminMgr@mycompany.com, CustomerSupportTeam@mycompany.com	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.
Email Mime Type	HTML	Type of email format that will be used for the compliance audit report: text or html.
Email Sender Address	PCIComplianceAuditor@mycompany.com	Email address that will appear in the From field when the compliance audit report is emailed.
Email Subject Line	Weekly Sybase Database Compliance Audit Results	Text that will appear in the Subject field when the compliance audit report is emailed.
SMTP Server Address	smtp001.west.mycompany.com	Fully-qualified host name or IP address of the SMTP server that will send the email containing the compliance audit report.

Note: Some of these parameters are not exposed by default in the deployment. See [How to Expose Additional Workflow Parameters](#) on page 100.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see [Parameters for Run Sybase Compliance Audit](#) on page 76).

Scenario 3: Perform a Full SOX Compliance Audit and Email the Results

A summary report is sent to the three parties listed in the Email Addresses to Receive Report parameter.

Parameter Name	Example Value	Description
Compliance Type	SOX	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Email Addresses to Receive Report	SybaseDBAdminTeam@mycompany.com, SybaseDBAdminMgr@mycompany.com, CustomerSupportTeam@mycompany.com	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.
Email Mime Type	HTML	Type of email format that will be used for the compliance audit report: text or html.
Email Sender Address	SOXComplianceAuditor@mycompany.com	Email address that will appear in the From field when the compliance audit report is emailed.
Email Subject Line	Weekly Sybase Database Compliance Audit Results	Text that will appear in the Subject field when the compliance audit report is emailed.
SMTP Server Address	smtp001.west.mycompany.com	Fully-qualified host name or IP address of the SMTP server that will send the email containing the compliance audit report.

Note: Some of these parameters are not exposed by default in the deployment. See [How to Expose Additional Workflow Parameters](#) on page 100.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see [Parameters for Run Sybase Compliance Audit](#) on page 76).

Scenario 4: Perform a Full CIS Compliance Audit and Display the Results on the HP DMA Console

In the scenario, all scorable checks are performed, and the compliance audit report is displayed only on the HP DMA Console. In this case, a summary report is not emailed. This scenario would be appropriate for initial testing.

It is not necessary to specify any input parameters in this scenario unless the Sybase ASE inventory file is located in a non-standard directory.

Parameter Name	Example Value	Description
Compliance Type	CIS	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements

Note: Some of these parameters are not exposed by default in the deployment. See [How to Expose Additional Workflow Parameters](#) on page 100.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see [Parameters for Run Sybase Compliance Audit](#) on next page).

Parameters for Run Sybase Compliance Audit

The following tables describe the required and optional input parameters for this workflow. Some of these parameters are not initially visible in a deployment (see [How to Expose Additional Workflow Parameters](#) on page 100). For most parameters, if you do not specify a value for a parameter, a default value is assigned.

For information about which steps use which parameters, see [How this Workflow Works](#) on page 64.

Parameters Defined in this Step: Prepare Sybase Call Wrapper

Parameter Name	Default Value	Required	Description
Call Wrapper	see description	optional	Name of the interpreter specified in the command that will execute each step as either the OS administrative user or the owner of the pertinent database or middleware product.
Sybase OS User Name	sybase	required	OS user who owns the Sybase ASE installation directory.

Additional Parameters Defined in this Step: Gather Parameters for Oracle Compliance

Parameter Name	Default Value	Required	Description
Excluded Compliance Checks	no default	optional	Comma-separated list of compliance checks to exclude from the audit. For example: 1.2, 2, 3.*, 5*, 6.1.2 Note: Make sure that the checks specified here correspond with the compliance audit type (CIS, PCI, or SOX) that you are running.
Sybase Home	no default	required	The directory where Sybase ASE is installed. Required only when Instance.Home is not set.
Sybase User Name	no default	required	The Sybase ASE user who is the ASE system administrator and possesses all ASE privileges.
Sybase User Password	no default	required	The password for the ASE system administrator.

Additional Parameters Defined in this Step: Gather Advanced Parameters for Oracle Compliance

Parameter Name	Default Value	Required	Description
Email Addresses to Receive Report	no default	optional	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.
Compliance Type	CIS	optional	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Email Mime Type	html	optional	Type of email format that will be used for the compliance audit report: text or html.
Email Sender Address	sadma@hp.com	optional	Email address that will appear in the From field when the compliance audit report is emailed.
Email Subject Line	Database Compliance Results	optional	Text that will appear in the Subject field when the compliance audit report is emailed.
OPER Role Password	no default	optional	Password for the Sybase ASE oper_role (operator) role.
SA Role Password	no default	optional	Password for the Sybase ASE sa_role (system administrator) role.
SMTP Server Address	localhost	optional	Fully-qualified host name or IP address of the SMTP server that will send the email containing the compliance audit report.
SSO Role Password	no default	optional	Password for the Sybase ASE sso_role (system security officer) role.
Sybase Role Password	no default	optional	Password for the sybase_ts_role (Sybase technical support) role.

Additional Parameters Defined in this Step: Audit Sybase ???

Parameter Name	Default Value	Required	Description
EBF Patch Level	no default	optional	Latest Express Bug Fix (EBF) patch level available from Sybase.
ESD Patch Level	no default	optional	Latest Electronic Software Distribution (ESD) patch level available from Sybase.

Chapter 4

Reference Information

This chapter contains the following information:

Topic	Description
Compliance Benchmark Information	A list of the specific security benchmarks that are used by the workflows in this solution pack, and the mappings between each CIS benchmark requirement and the corresponding PCI and SOX requirements
Database Product Documentation	Links to product documentation for the database products that these workflows support

Compliance Benchmark Information

The workflows in this solution implement compliance audits against the following database security benchmarks:

Benchmark Type	Benchmark Version
Center for Internet Security (CIS)	Security Configuration Benchmarks for: Oracle 9i/10g, version 2.01 (April, 2005) Oracle Database Server 11g, version 1.1.0 (December 2011) Microsoft SQL Server 2005, version 2.0.0 (December 2011) Sybase Adaptive Server Enterprise (ASE) 15.0, version 1.1.0 (December 2011)
Payment Card Industry (PCI)	Data Security Standard version 2.0 (October 2010)
Sarbanes-Oxley (SOX)	Sections 302.2, 302.4b, 302.4c, 302.5

For links to the text of these security benchmarks, see the [Security Benchmark Documentation](#) on page 94.

The following topics show you how the CIS compliance checks map to the PCI and SOX requirements for each database product:

- [Compliance Benchmark Mappings for Oracle Database](#) on next page
- [Compliance Benchmark Mappings for Microsoft SQL Server](#) on page 88
- [Compliance Benchmark Mappings for Sybase ASE](#) on page 91

Note: Of the three benchmarks, the CIS benchmarks define the most granular security configuration requirements. The workflows do not perform checks for every PCI or SOX requirement. They perform only those technical PCI and SOX checks that map directly to the CIS checks.

Compliance Benchmark Mappings for Oracle Database

This topic lists the CIS checks performed by the [Run Oracle Compliance Audit](#) workflow and shows you how those checks map to the pertinent PCI and SOX requirements.

The workflow performs the checks included in the CIS benchmark and then maps those CIS checks to the benchmark type that you specify in the Compliance Type parameter. The audit summary email will match the Compliance Type that you specify.

Compliance Check Mappings for Oracle Database

CIS Section	CIS	SOX	PCI
Section 1: Operating System Specific Settings	1.*		
Section 2: Installation and Patch	2.02	302.4.3	6.1
	2.05	302.4.3	
	2.06	302.4.3	
	2.07	302.4.3	
	2.08	302.4.3	
	2.09	302.4.3	
	2.1	302.4.3	
	2.11	302.4.3	
	2.12	302.4.3	2.1
	2.13	302.4.3	
	2.14	302.4.3	
Section 3: Oracle Directory and File Permissions	3.01	302.4.3	
	3.02	302.4.3	
	3.03	302.4.3	
	3.04	302.4.3	
	3.05	302.4.3	
	3.06	302.4.3	
	3.07	302.4.3	
	3.08	302.4.3	
	3.09	302.4.3	
	3.1	302.4.3	

Compliance Check Mappings for Oracle Database (continued)

CIS Section	CIS	SOX	PCI
	3.11	302.4.3	
	3.12	302.4.3	
	3.13	302.4.3	
	3.14	302.4.3	
	3.15	302.4.3	
	3.16	302.4.3	
	3.17	302.4.3	
	3.18	302.4.3	
	3.19	302.4.3	
	3.2	302.4.3	
	3.21	302.4.3	
	3.22	302.4.3	
	3.23	302.4.3	
	3.24	302.4.3	
	3.25	302.4.3	
	3.26	302.4.3	
Section 4: Oracle Parameter Settings	4.01	302.4.3	
	4.02	302.4.3	
	4.03	302.2	
	4.04	302.2	
	4.05	302.2	
	4.07	302.4.3	
	4.08	302.4.3	
	4.09	302.4.3	
	4.1	302.4.3	
	4.11	302.4.3	
	4.12	302.2	

Compliance Check Mappings for Oracle Database (continued)

CIS Section	CIS	SOX	PCI
	4.13	302.4.3	
	4.14	302.4.3	
	4.15	302.4.3	
	4.16	302.4.3	
	4.17	302.4.3	
	4.18	302.4.2	
	4.19	302.4.3	
	4.2	302.4.3	
	4.23	302.4.3	
	4.24	302.4.3	
	4.25	302.4.3	
	4.26	302.4.3	
	4.27	302.2	
	4.28	302.4.3	
	4.29	302.2	
	4.3	302.4.3	
	4.31	302.4.3	
	4.32	302.2	
	4.33	302.4.3	
	4.34	302.4.3	8.5.13.0
	4.35	302.4.3	
	4.35	302.2	
	4.36	302.4.2	
	4.39	302.2	
	4.4	302.2	
	4.41	302.2	
	4.42	302.2	

Compliance Check Mappings for Oracle Database (continued)

CIS Section	CIS	SOX	PCI
	4.43	302.4.3	
	4.43	302.2	
Section 5: Encryption Specific Settings	5.02	302.2	2.3
	5.03	302.2	
	5.04	302.2	
	5.05	302.2	
	5.06	302.2	
	5.07	302.2	
	5.08	302.2	
	5.09	302.2	
	5.13	302.4.3	
	5.14	302.4.3	
	5.15	302.4.3	
	5.16	302.2	
	5.21	302.2	
	5.24	302.4.3	
	5.25	302.2	
	5.26	302.2	
Section 7: Backup and Disaster Recovery	7.02	302.4.3	
	7.04	302.4.3	
	7.05	302.4.3	
	7.06	302.4.3	
Section 8: Oracle Profile (User) Setup Settings	8.01	302.2	
	8.02	302.2	8.5.9.0
	8.03	302.2	8.5.12.0
	8.04	302.2	
	8.05	302.2	8.5.14.0

Compliance Check Mappings for Oracle Database (continued)

CIS Section	CIS	SOX	PCI
	8.07	302.2	
	8.08	302.2	
	8.09	302.4.3	
	8.1	302.4.3	
	8.11	302.4.3	
	8.12	302.4.3	
	8.13	302.2	
	8.14	302.2	
Section 9: Oracle Profile (User) Access Settings	9.01	302.4.3	
	9.02	302.4.3	
	9.03	302.2	7.1.1
	9.04	302.2	7.1.1
	9.05	302.2	7.1.1
	9.06	302.4.3	7.1.1
	9.07	302.4.3	7.1.1
	9.08	302.2	7.1.1
	9.09	302.4.3	7.1.1
	9.1	302.4.3	7.1.1
	9.11	302.4.3	7.1.1
	9.12	302.4.3	7.1.1
	9.13	302.4.3	7.1.1
	9.14	302.4.3	7.1.1
	9.15	302.2	7.1.1
	9.16	302.4.3	7.1.1
	9.17	302.4.3	7.1.1
	9.18	302.4.3	7.1.1
	9.19	302.4.3	7.1.1

Compliance Check Mappings for Oracle Database (continued)

CIS Section	CIS	SOX	PCI
	9.2	302.4.3	7.1.1
	9.22	302.4.3	7.1.1
	9.23	302.4.3	
	9.24	302.4.3	
	9.26	302.2	7.1.1
	9.27	302.2	7.1.1
	9.28	302.2	7.1.1
	9.29	302.2	
	9.3	302.4.3	
	9.31	302.4.3	
	9.32	302.4.3	
	9.33	302.4.3	
	9.34	302.4.3	7.1.1
	9.35	302.2	
	9.36	302.2	7.1.1
	9.37	302.4.3	7.1.1
	9.38	302.4.3	
	9.39	302.4.3	
	9.4	302.2	
	9.41	302.4.3	
	9.42	302.2	7.1.1
	9.43	302.2	
	9.44	302.2	
	9.45	302.2	
	9.46	302.4.3	
	9.47	302.2	
	9.48	302.2	

Compliance Check Mappings for Oracle Database (continued)

CIS Section	CIS	SOX	PCI
	9.49	302.2	
	9.52	302.4.3	
	9.54	302.4.3	
	9.55	302.4.3	
	9.56	302.2	

Compliance Benchmark Mappings for Microsoft SQL Server

This topic lists the CIS checks performed by the [Run MS SQL Compliance Audit](#) workflow and shows you how those checks map to the pertinent PCI and SOX requirements.

The workflow performs the checks included in the CIS benchmark and then maps those CIS checks to the benchmark type that you specify in the Compliance Type parameter. The audit summary email will match the Compliance Type that you specify.

Compliance Check Mappings for MS SQL Server

CIS Section	CIS	PCI	SOX
Section 1: Operating System and Network Specific Configuration	1.6	2.3	302.2
	1.9.1	2.1	302.2
	1.9.3		302.4.3
	1.9.4		302.4.3
	1.1	2.2.2	302.4.3
	1.13	7.1	302.2
	1.2	7.1	302.2
Section 2: SQL Server Installation and Patches	2.1		302.4.3
	2.2	6.1	302.4.3
	2.3	1.1.5	302.4.3
	2.4		302.4.3
	2.6	8.5.16	302.2
	2.7	2.1	302.2
	2.9	2.2.4	302.4.3
	2.1	10.2	302.4.2
	2.11	2.2.4	302.2
	2.12	2.2.4	302.4.3
Section 3: SQL Server Settings	3.1	1.1.5	302.2
	3.2.1	2.2.2	302.4.3
	3.2.2	2.2.2	302.4.3
	3.2.3	2.2.2	302.4.3
	3.2.4	2.2.4	302.2

Compliance Check Mappings for MS SQL Server (continued)

CIS Section	CIS	PCI	SOX
	3.2.5	8.5.16	302.2
	3.2.6		302.4.3
	3.2.7		302.4.3
	3.3		302.4.3
	3.4		302.4.3
	3.5	2.2.4	302.4.3
	3.6		302.4.2
	3.7	2.2.4	302.4.3
	3.8		302.4.2
	3.9		302.4.3
	3.1	2.2.4	302.4.3
	3.16	2.2.4	302.4.2
	3.17	2.2.2	302.4.3
Section 4: Access Controls	4.1	7.1.1	302.2
	4.2	7.1.1	302.2
	4.4	7.1.1	302.2
	4.5	2.1	302.2
	4.7	7.1.1	302.2
	4.9	7.1.1	302.2
	4.22	2.2.4	302.2
	4.24	7.1.1	302.2
Section 5: Auditing and Logging	5.2	10.2.4	302.5
Section 6: Backup and Disaster Recovery Procedures	6.3		302.4.3
	6.3		302.4.3
	6.5	3.4.1	302.2
	6.6	7.1.1	302.2
Section 7: Replication			

Compliance Check Mappings for MS SQL Server (continued)

CIS Section	CIS	PCI	SOX
Section 8: Application Development Best Practices	8.1	2.2.4	302.2
	8.3	8.5.16	302.2
	8.9	8.5.16	302.2
	8.1	2.1	302.4.3
Section 9: Surface Area Configuration Tool	9.1	2.2.4	302.2
	9.2	2.2.4	302.4.3
	9.3	2.2.4	302.2
	9.4	2.2.4	302.4.3
	9.6	2.2.4	302.4.3
	9.8	2.2.4	302.4.3
	9.9	2.2.4	302.4.3
	9.1	2.2.4	302.2

Compliance Benchmark Mappings for Sybase ASE

This topic lists the CIS checks performed by the [Run Sybase Compliance Audit](#) workflow and shows you how those checks map to the pertinent PCI and SOX requirements.

The workflow performs the checks included in the CIS benchmark and then maps those CIS checks to the benchmark type that you specify in the Compliance Type parameter. The audit summary email will match the Compliance Type that you specify.

Compliance Check Mappings for Sybase Adaptive Server Enterprise

CIS Section	CIS	PCI	SOX
Section 1: Authentication Mechanisms	1.2		302.4.3
	1.3	2.3	302.4.3
	1.4	2.1	302.4.3
	1.6	8.5.10	302.4.3
	1.7	8.5.13	302.4.3
	1.8	8.5.9	302.4.3
	1.9	8.5.16	404.1.1.1
Section 2: Network Security Mechanisms	2.1		302.4.3
	2.3		302.4.3
	2.4		302.4.3
	2.5.1		302.4.3
	2.5.2		302.4.3
Section 3: Database Resource Permissions	3.1.1		302.4.3
	3.2.1		302.4.3
	3.4		302.4.3
	3.5		302.4.3
	3.5.1		302.4.3
	3.6.1		302.4.3
	3.6.2		302.4.3
Section 4: Auditing, Logging and Reporting Mechanisms	4.2		302.4.4
	4.3	10.3	302.4.4
	4.6		302.4.4

Compliance Check Mappings for Sybase Adaptive Server Enterprise (continued)

CIS Section	CIS	PCI	SOX
	4.7		302.4.4
	4.8		302.4.4
Section 5: Extensibility Mechanisms	5.1		302.4.3
	5.2		302.4.3
	5.3.1		302.4.3
	5.3.2		302.4.3
Section 6: Host and Network Deployment	6.6		302.4.3
	6.1		302.4.3
	6.11	6.1	302.4.3

Database Product Documentation

The following topics show contain links to documentation for the database products supported by this solution:

Note: The links to the documents listed here were correct as of the publication of this guide.

Oracle Database Product Documentation

The product documentation for Oracle Database Enterprise Edition version 11gis located here:

<http://www.oracle.com/pls/db112/homepage>

Microsoft SQL Server Documentation

For information about SQL Server, including prerequisites, see the SQL Server documentation available at the following web site:

<http://msdn.microsoft.com/en-us/library>

Sybase Adaptive Server Enterprise Documentation

SAP provides an extensive documentation library for Sybase ASE at this location:

<http://infocenter.sybase.com/help/index.jsp>

For information about Adaptive Server specifications—including database requirements based on page size—see this document:

[Adaptive Server Specifications](#)

Additional Resources

See the following resources for additional contextual information about the workflows in this solution pack.

Security Benchmark Documentation

The workflows in this solution perform compliance audits against the following security benchmarks.

Center for Internet Security (CIS) Security Configuration Benchmarks

Oracle 9i/10g, version 2.01 (April, 2005)

http://benchmarks.cisecurity.org/tools2/oracle/CIS_Oracle_Benchmark_v2.01.pdf

Oracle Database Server 11g, version 1.1.0 (December 2011)

http://benchmarks.cisecurity.org/tools2/oracle/CIS_Oracle_11g_Benchmark_v1.1.0.pdf

Microsoft SQL Server 2005, version 2.0.0 (December 2011)

http://benchmarks.cisecurity.org/tools2/sqlserver/CIS_Microsoft_SQL_Server_2005_Benchmark_v2.0.0.pdf

Sybase Adaptive Server Enterprise (ASE) 15.0, version 1.1.0 (December 2011)

http://benchmarks.cisecurity.org/tools2/sybase/CIS_Sybase_ASE_15.0_Benchmark_v1.1.0.pdf

Payment Card Industry (PCI) Data Security Standard version 2.0 (October 2010)

http://pcisecuritystandards.org/documents/pa-dss_v2.pdf

Sarbanes-Oxley (SOX) Sections 302.2, 302.4b, 302.4c, 302.5

Official product-specific SOX benchmarks do not yet exist. Numerous third-party interpretations of the SOX legislation are available online free of charge. For more information, see the pertinent sections of the [Sarbanes-Oxley Act of 2002](#).

Note: The links to the documents listed here were correct as of the publication of this guide.

HP DMA Documentation

For information about using the HP DMA web interface, see the *User Guide: Database and Middleware Automation* version 9.13 (or later).

This document is part of the HP Server Automation documentation library, which is available on the HP Software Product Manuals web site:

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

Chapter 5

Tips and Best Practices

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

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

[How to Expose Additional Workflow Parameters](#) on page 100

[How to Use a Policy to Specify Parameter Values](#) on page 101

[How to Import a File into the Software Repository](#) on page 104

How a Solution Pack is Organized

Note: This topic uses the Run Oracle Compliance Audit workflow in the Database Compliance solution pack as an example. The information provided here, however, pertains to any solution pack.

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

A solution pack contains one or more related workflow templates.

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

The screenshot displays the HP Database & Middleware Automation web interface. The top navigation bar includes 'Home', 'Automation', 'Reports', 'Environment', 'Solutions', and 'Setup'. The 'Automation' tab is active, showing sub-tabs for 'Workflows', 'Steps', 'Functions', 'Policies', 'Deployments', 'Run', 'Console', and 'History'. The main content area is titled 'Run Oracle Compliance Audit' and has tabs for 'Documentation', 'Workflow', 'Deployments', and 'Roles'. The 'Documentation' tab is selected, showing fields for 'Name' (Run Oracle Compliance Audit), 'Tags', 'Type' (OS), and 'Target level' (Instance). Below these fields is a 'Documentation' section with three sub-sections: 'Purpose', 'Description', and 'Parameters'. The 'Purpose' section states the audit's goal is to check compliance with CIS benchmarks and PCI/SOX requirements. The 'Description' section details the audit process using CIS Level 1 and 2, comparing results to PCI and SOX requirements, and sending reports. The 'Parameters' section is currently empty. At the bottom of the documentation area are links for 'HELP', 'PDF', and 'EDIT'. Below the documentation area is a toolbar with icons for 'DELETE', 'EXPORT', 'EXTRACT POLICY', 'DEPLOY', and 'RUN', followed by 'Copy', 'Save', and 'CANCEL' buttons. The footer contains copyright information: '© 2006–2012 Hewlett-Packard Development Company, L.P. Web Server: 9.13.0 Repository: 9.10.0'.

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

The screenshot displays the HP Database & Middleware Automation web interface. The top navigation bar includes 'Home', 'Automation', 'Reports', 'Environment', 'Solutions', and 'Setup'. The 'Automation' tab is active, showing sub-tabs for 'Workflows', 'Steps', 'Functions', 'Policies', 'Deployments', 'Run', 'Console', and 'History'. The 'Steps' sub-tab is selected, and the 'Get Oracle Home' step is highlighted.

The 'Get Oracle Home' step configuration is shown with the following details:

- Name:** Get Oracle Home
- Tags:** (empty field)
- Type:** Oracle (selected from a dropdown menu)
- Category:** Script
- Targetable:** ☐

The **Documentation** panel on the right provides a description and details for the step:

- Description:** Get the value of ORACLE_HOME from the appropriate source:
 - The /etc/oratab or /var/opt/oracle/oratab file on UNIX
 - The registry on Windows
- Dependencies:** None
- Input Parameters:** None
- Output Parameters:**
 - Oracle Home = The fully qualified name of the ORACLE_HOME
 - Oracle SID = The Oracle server (instance) ID
- Return Code:**
 - 0 = Step was successful
 - 1 = Error occurred in step

At the bottom right of the configuration area, there are buttons for 'Copy', 'Save', and 'CANCEL'. The footer of the interface indicates the copyright information: '© 2006–2012 Hewlett-Packard Development Company, L.P. Web Server: 9.13.0 Repository: 9.10.0'.

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

Get Listener Names

General

Action

Parameters

History

Workflows

Solutions

Roles

Input parameters

Name	Value	Description
<input type="text" value="Listener Homes"/>	<input type="text"/>	Optional: Comma delimited list of fully qualified path
<input type="text" value="Oracle SIDs"/>	<input type="text"/>	Optional: Comma delimited list of ORACLE_SIDs, a

NEW PARAMETER

Output parameters

Name	Description
<input type="text" value="Listener Homes"/>	Comma separated list of homes the listeners are running out of.
<input type="text" value="Listener ORA Files"/>	Comma separated list of listener.ora files used by each Listener.
<input type="text" value="Listener Users"/>	Comma separated list of users the listeners are running as.
<input type="text" value="Listeners"/>	Comma separated list of listeners running from this ORACLE_HOME

NEW PARAMETER

Copy

Save

or CANCEL

© 2006–2012 Hewlett-Packard Development Company, L.P.
Web Server: 9.13.0 Repository: 9.10.0

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

Get Listener Names / Oracle SIDs

Optional: Comma delimited list of ORACLE_SIDs, at least one of which a resulting listener must service. If blank, listeners are not limited to those servicing any specific ORACLE_SID.

↑

To see the parameter description here

▶ 6

Prepare Oracle Instance

7

▶

▼ 7

Get Listener Names

8

▶

▶ 8

Audit Unix or Linux OS Specific Settings

9

▶

▶ 9

Audit Installation and Patch

10

▶

Listener Homes: Prepare Oracle Instance.Oracle Home

Oracle SIDs: Get Oracle Home.Oracle SID

Click here

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

Database & Middleware Automation

Server: myserver.mycompany.com
User: admin
Logout

Home
Automation
Reports
Environment
Solutions
Setup

Workflows
Steps
Functions
Policies
Deployments
Run
Console
History

Run Oracle Compliance CIS

Targets
Parameters
Roles

Gather Parameters for Oracle Compliance

Compliance Type:
CIS
Text

Compliance type that will be audited by the workflow. Compliance types supported: CIS, PCI, SOX. Will be defaulted to CIS.

Excluded Compliance Checks:
Text

Optional: Checks to exclude from of Compliance Checks

Inventory Files:
/etc/orainst.loc
Text

Optional: Comma separated list of fully qualified Oracle inventory files. If not specified, default to /etc/orainst.loc, /var/opt/oracle/orainst.loc, or %ProgramFiles%\Oracle\inventory.

Gather Advanced Parameters for Oracle Compliance

Email Addresses to Receive Report:
CISComplianceAuditor@mycompany.com
Text

*Optional. Provided an email address or multiple email addresses separated by commas without spaces that you would like to receive an email of the results of the compliance tests run against the target specified.

X DELETE
▶ RUN

Restore defaults
Copy
Save
or
CANCEL

© 2006–2012 Hewlett-Packard Development Company, L.P.
Web Server: 9.13.2 Repository: 9.10.0

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 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 *User Guide: Database and Middleware Automation*. This guide is included in the HP Server Automation documentation library.

Create a Policy

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

To create a policy that provides parameter values:

1. In the 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 *User Guide: Database and Middleware Automation* for details. This guide is included in the HP Server Automation documentation library (SA version 9.13 and later).
2. On the Parameters tab, perform the following steps for each parameter whose value you want to provide by referencing a policy attribute:
 - a. In the drop-down menu for that parameter, select **Policy Attribute**.
 - b. In the text box for that parameter, type any character. A drop-down list of policy attributes appears. For example:

Admin Pwd: Policy Attribute ▼

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

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

Admin Pwd: Policy Attribute ▼

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

How to Import a File into the Software Repository

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

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

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

To import a file into the HP SA Software Library:

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

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

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

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

Chapter 6

Troubleshooting

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

- [Target Type](#) below
- [User Permissions and Related Requirements](#) below
- [Discovery in HP Server Automation](#) below

Target Type

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

User Permissions and Related Requirements

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

Roles are assigned by your HP Server Automation (SA) administrator using the SA console. See the HP Server Automation *Administration Guide* and the *User Guide: Database and Middleware Automation* for more information. Both guides are included in the HP Server Automation documentation library

Make sure that the 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 DMA UI. For a detailed breakdown, see the *User Guide: Database and Middleware Automation*.

Discovery in HP Server Automation

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

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

Glossary

B

bridged execution

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

C

cross-platform

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

D

deployment

Deployments associate a workflow with a target environment in which a workflow runs. You can customize a deployment by specifying values for any workflow

parameters that are designated - User Selected - in the workflow. You must save a deployment before you can run the workflow. You can re-use a saved deployment as many times as you like.

destination

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

DESTINATION

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

I

input parameters

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

M

mapping

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

then become visible on the Deployment page.

O

Oracle Data Pump

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

P

parameters

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

R

raw devices

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

Recovery Manager (RMAN)

Oracle Recovery Manager (RMAN) is a backup and recovery tool included in Oracle Database Enterprise Edition (and related products). RMAN enables you to efficiently backup and restore data files, control files, server parameter files, and archived redo log files. It provides block-

level corruption detection during both the backup and restore phases. It is optimized for performance and space consumption.

S

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.

source

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

SOURCE

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

source database

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

steps

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

T

target instance

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

W

workflow

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

workflow editor

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