

Oracle® Advanced Support Gateway
User's Guide

F58615-01

December 2024

Copyright © 1994, 2024, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface	5
Audience.....	5
Related Documentation	5
Getting Help	6
Documentation Accessibility	6
 1 About the Oracle Advanced Support Gateway User Interface	
Logging onto the Gateway	1-1
About the Gateway User Interface	1-2
About the Navigation Menu.....	1-3
About the My Services Menu	1-3
Selecting a Service	1-4
Selecting a Service Feature.....	1-4
About the Dashboard Menu	1-5
Reviewing and Filtering Information.....	1-5
About the Gateway Menu	1-6
About the Admin Menu	1-6
Viewing Legal and Copyright Information.....	1-7
 2 Using Dashboards	
About Dashboards	2-1
Accessing the Dashboard	2-2
About Widgets	2-2
Adding a Dashboard	2-3
Adding a Widget	2-4
Managing Widgets	2-5
Removing a Widget from a Dashboard.....	2-5
Configuring a Widget.....	2-5
Reviewing Information about a Widget.....	2-6
 3 Managing Users	
About User Management	3-1
Managing Users	3-1
Viewing Users.....	3-1
Adding Users.....	3-2
Activating Users.....	3-3
Updating Users.....	3-4
Deleting Users.....	3-4
Resetting User Passwords	3-5

4 Managing Credentials and Passwords

About Credential Management	4-1
About Oracle Platinum Services Customer Requirements	4-1
Displaying Credentials	4-2
Using Credential Management.....	4-2
About Credentials	4-2
About Required Credentials.....	4-2
About Recommended Credentials	4-3
About Additional Credentials	4-4
About Selected Targets and their Associated Credentials	4-4
Viewing Credentials	4-4
Viewing Credentials for Target Children.....	4-6
Editing Credentials	4-6
Editing Credentials	4-6
Editing Credentials in Bulk	4-7
Creating Credentials	4-8
About Credential Reports	4-9
Viewing Target Credentials	4-9

5 Managing Systems and Hosts

About Managing Systems and Hosts	5-1
Adding a New System	5-1
About Adding a New Engineered System	5-2
Adding an Oracle Exadata Engineered System	5-4
Adding an Oracle Exalogic Engineered System	5-13
Adding an Oracle SuperCluster Engineered System	5-16
Adding an Oracle ZDLRA Engineered System	5-19
Viewing Target Configurations	5-22
Viewing Target Details	5-22
Viewing Statistics	5-23
Viewing Service Requests	5-24
Viewing Recommendations	5-24
Managing System Passwords	5-24
Deactivating Services	5-25

6 Activating Services

About Activating Services	6-1
Selecting a Service for Activation	6-2
Viewing Discovered Databases	6-8
Deactivating Services	6-8

7 Validating Connections

About Gateway Connectivity	7-1
About System Tests	7-2
About Internal System Tests	7-2
About External System Tests.....	7-2

About ILOM Tests	7-2
Viewing System Test Status	7-2
Verifying the External Connection	7-3
Specifying a HTTP Proxy	7-4
Verifying an Internal Connection	7-5
Verifying an ILOM Connection	7-8
Configuring New System Test Targets	7-9
8 Managing Service Requests	
Viewing Service Requests	8-1
Viewing Service Requests Associated with a Managed System	8-2
9 Managing Databases and Database Patches	
About Database Management	9-1
Viewing Managed Databases.....	9-1
Editing Managed Databases.....	9-3
Editing Managed Databases Using the Edit Icon	9-4
Editing Managed Databases Using the Actions List	9-4
Editing the Monitoring Configuration	9-5
Activating a Service on a Database	9-5
About Patching Requests	9-6
Creating a Patching Request	9-7
Editing the CM for a Patching Request	9-21
Assigning an SR for a Patching Request	9-22
Canceling Patching Requests.....	9-24
Contacting the Patch Coordinator.....	9-25
Editing a Patching Request	9-25
Managing Database Patch Compliance	9-25
Setting the Database Patchset Compliance Level	9-26
10 Scheduling Database Blackouts	
About Database Blackouts	10-1
Creating Database Blackouts	10-1
Managing Database Blackouts	10-3
Viewing Scheduled Blackouts	10-3
Viewing Completed Blackouts	10-3
Editing Blackouts	10-4
Canceling Blackouts	10-5
11 Managing Database Entitlements	
About Database Entitlements	11-1
About the High Water Mark	11-1
Viewing Database Entitlements	11-2

12	Setting the HTTP Proxy Server	
	About the HTTP Proxy Server.....	12-1
	Specifying the HTTP Proxy Server Setting.....	12-1
	Specifying a HTTP Proxy During Connectivity Tests.....	12-2
13	Managing Server and ILOM Certificates	
	About Server and ILOM Certificates.....	13-1
	Viewing Server Certificates.....	13-2
	Viewing Certificate Status	13-2
	Managing Server Certificates.....	13-2
	Downloading Server Certificates	13-3
	Installing Server Certificates.....	13-4
	Generating a Certificate Signing Request.....	13-4
	Replacing the Current Server Certificate	13-5
14	Enabling Remote Access to the Oracle Advanced Support Gateway	
	About Remote Access	14-1
	About the Remote Access Icon	14-2
	Enabling Remote Access	14-2
	Disabling Remote Access	14-3
	Viewing Remote Access History	14-3

Preface

This guide explains how to use Oracle Advanced Support Gateway.

Refer to the following sections:

- ? [Audience](#)
- ? [Related Documentation](#)
- ? [Getting Help](#)
- ? [Documentation Accessibility](#)

Audience

This guide is intended for Oracle Advanced Support Gateway customer users.

Oracle Advanced Support Gateway is a multiservice platform that is deployed in customer networks to simplify network connectivity and access for Oracle in the delivery of Oracle services including Platinum Services, ACS Services, Advanced Monitoring and Resolution, and Premier Support.

The Gateway platform is a software appliance, based on the Oracle Linux operating system and hosts a full stack of Oracle software, including Automated Service Request (ASR), Oracle Enterprise Manager, Oracle Configuration Manager (OCM), patch management (such as YUM services), and a suite of Java applications. Together, these applications aggregate and route telemetry messages from the customer environment to the Oracle Support Services infrastructure.

The Gateway provides remote access for Oracle engineers to access the customer network (with customer permission) and to carry out approved actions on the customer's monitored systems. In short, the Gateway allows simplification of the network requirements and a single point of access for the provision and delivery of Oracle connected services.

The Gateway is typically located in the customer data center DMZ behind a firewall, with network access to the infrastructure it is monitoring. It is not directly exposed to the Internet, but it should be continuously accessible from Oracle Cloud Operations infrastructure, using a TLS/VPN tunnel.

Related Documentation

For more information, see the following documents in the Oracle Advanced Support Gateway documentation set:

- ? [Oracle Advanced Support Gateway Installation Guide](#): Describes how to build the Gateway both in the Cloud (using Oracle Cloud Infrastructure, or OCI) and in an on-premises configuration. The document also provides requirements for installing the

Gateway, installation procedures, and post-installation tasks. Also provides information on activating the Gateway on which various services are installed and supported.

- 7 [Oracle Advanced Support Gateway Security Guide](#): Describes security information and instructions for the Gateway. Includes the requirements for deploying the Gateway into the customer environment to support the delivery of Oracle Connected Services. The Gateway is an important part of the Oracle delivery architecture for Oracle Connected Services and its placement must be carefully considered in order for Oracle to deliver Oracle Connected Services. This document outlines network configuration options when integrating the Gateway device within the customer environment.

Getting Help

If you require assistance using the Gateway, please contact the Oracle Support Services contact with whom you have been engaged for review.

Alternatively, you can use your CSI (Customer Support Identifier) to access My Oracle Support at:

<https://support.oracle.com/>.

Thank you for choosing Oracle Advanced Support Gateway.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit

<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit

<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

About the Oracle Advanced Support Gateway User Interface

This chapter offers an introduction to the Oracle Advanced Support Gateway user interface and its principal features.

It includes the following topics:

- ? [Logging onto the Gateway](#)
- ? [About the Gateway User Interface](#)

Logging onto the Gateway

After successfully installing the Oracle Advanced Support Gateway, you can access the Oracle Advanced Support Gateway portal using a Web browser.

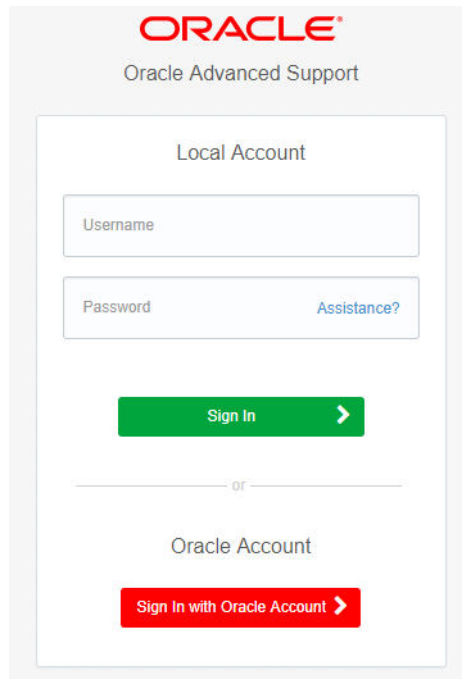
Note: In order to access the Gateway, your Web browser must be connected to the Internet to enable Oracle Single Sign-on (SSO) authentication.

To log on to the Gateway:

1. Navigate to the Oracle Advanced Support Gateway portal at *https://<GATEWAY_IP_ADDRESS>*.

GATEWAY_IP_ADDRESS is the IP address assigned to the physical interface of the Oracle Advanced Support Gateway. Where two interfaces are used, you need to reference the internal interface. This is the IP address which will communicate internally.

2. The Gateway login screen appears.



The screenshot shows the Oracle Advanced Support Gateway User Interface login page. At the top, the Oracle logo is displayed in red, followed by the text "Oracle Advanced Support". Below this, there is a section titled "Local Account" containing a "Username" input field and a "Password" input field with a blue "Assistance?" link to its right. A green "Sign In" button with a right-pointing arrow is positioned below the password field. A horizontal line with the word "or" in the center separates the local account section from the "Oracle Account" section. The "Oracle Account" section features a red "Sign In with Oracle Account" button with a right-pointing arrow.

To log on to the Gateway, use one of the following methods:

- ? Enter the username and password for your local account and click **Sign In**, or
- ? Click **Sign In with Oracle Account** to be logged in using your Oracle login account.

Note: In order to access the Gateway, your Web browser must be able to log in to <http://www.oracle.com> to enable access to the Gateway user interface (UI) using your Oracle Single Sign-on (SSO) authentication.

The All Services page appears.

About the Gateway User Interface




This section briefly describes the Gateway user interface and provides an overview of the main UI components.

The Gateway user interface is made up of a number of principal elements that enable you to optimally manage your services and to perform tasks, for example:

- ? Create users and assign passwords
- ? Activate services
- ? Provision agents
- ? Manage systems and hosts
- ? Review the status of service requests

Refer to [Figure 1–1](#) that shows the user interface.

Figure 1–1 Oracle Advanced Support Gateway User Interface

 Platinum (ID: 100120)	Platinum	Systems 2 Total	Database Status 0 Down	Patch Compliance 2 Non-Compliant	Current Requests 0 Scheduled
 Platinum (ID: 100060)	Platinum	Systems 2 Total	Database Status 0 Down	Patch Compliance 2 Non-Compliant	Current Requests 8 Scheduled
 Oracle Advanced Monitoring and Resolution (ID: 100341)	ACS Cloud Services	Use the Gateway menu on this page for: <ul style="list-style-type: none"> • ACPD auditing • Password Management • Connectivity Tests 			

Refer to the following sections that describe the individual elements of the Gateway user interface:

- ? [About the Navigation Menu](#)
- ? [About the My Services Menu](#)
- ? [About the Dashboard Menu](#)
- ? [About the Gateway Menu](#)
- ? [About the Admin Menu](#)
- ? [Viewing Legal and Copyright Information](#)

About the Navigation Menu

The navigation menu is on the page header under the Oracle logo and application name.

Figure 1–2 Viewing the Navigation Menu

The navigation menu comprises:

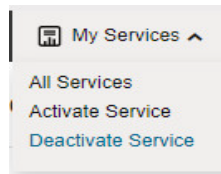
- ? Menu items linked to either:
 - A pull down of sub-menu items, for example, **Admin**, or
 - An individual screen, for example, **Dashboard**
- ? Link to online help and user settings:
 - A support icon that links to online help for Gateway users
 - A user settings icon displaying options to:
 - Edit your user profile. See "[Updating Users](#)."
 - Update your user password.
 - Log out of the current session.

About the My Services Menu

The My Services menu enables you to:

- ? Select **All Services** to display all available customer services on the Gateway, as seen on the My Services main page in [Figure 1–1](#)
- ? Select **Activate Service** to activate a service
- ? Select **Deactivate Service** to deactivate a service

Figure 1–3 Viewing the My Services Menu



Related Information

[Selecting a Service](#)

[Selecting a Service Feature](#)

[Activating Services](#)

Selecting a Service

To select a supported service:

1. Log on to the portal as outlined in ["Logging onto the Gateway."](#)
2. From the My Services menu, select **All Services**.

The My Services page appears. It displays a list of services tailored to the customer contract.

Note: A number of images in this and other chapters may not be applicable to particular customers who do not have features or functionality associated with particular services.

3. From the My Services page, select the required service by clicking it.

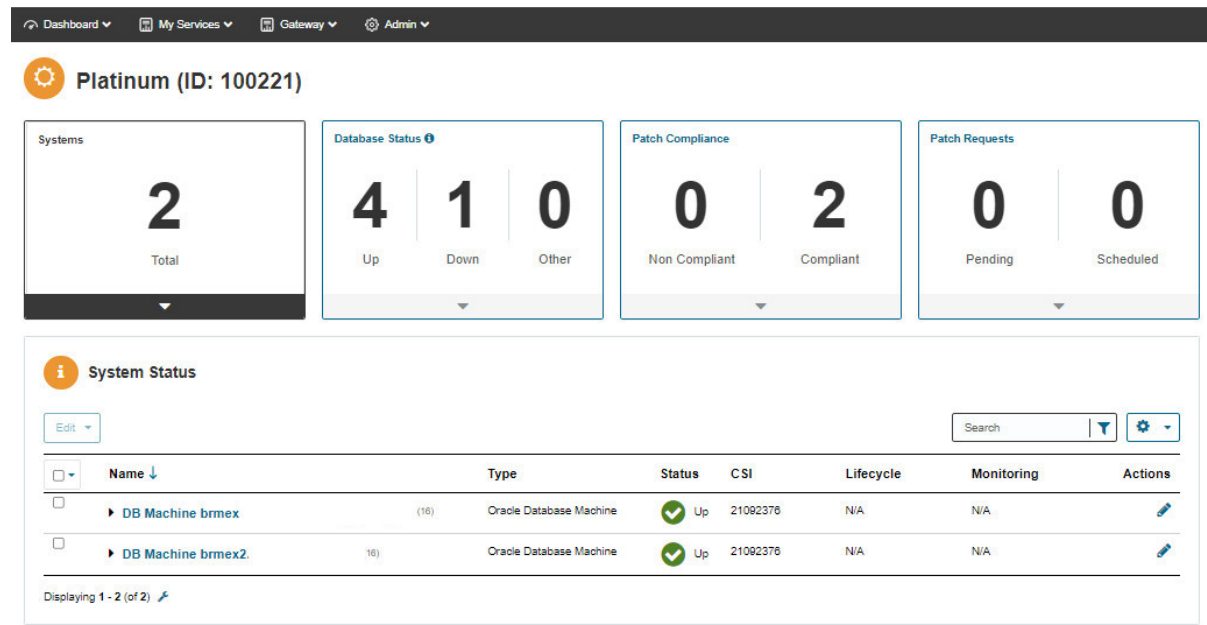
Selecting a Service Feature

To select a supported service feature:

1. Choose the required service as outlined in ["Selecting a Service."](#)
2. From the service page, click a tile to select the service feature, for example, click **Systems** as shown in [Figure 1–4](#) to display the system status table.

The selected service feature is displayed.

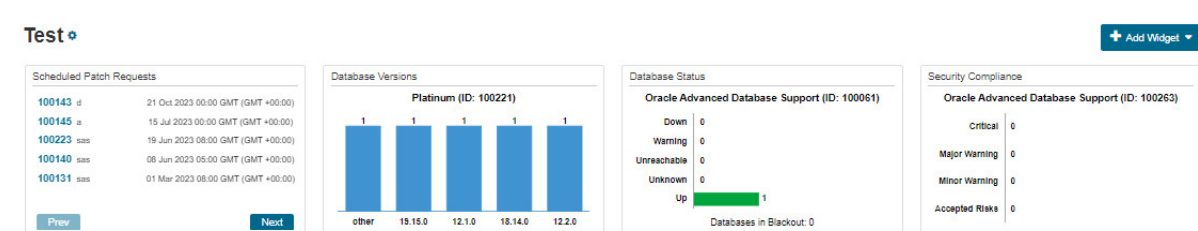
Figure 1–4 Selecting a Service Feature



About the Dashboard Menu

An Oracle Advanced Support Gateway dashboard is a customizable service dashboard framework that provides an overview of your services and enables you to focus on selected items of interest. Although the initial *home* dashboard is blank, the format enables you to add a series of data windows called *widgets*. The dashboard provides a layout to display multiple widgets on one page. You can create multiple dashboard pages, with each page made up of multiple widgets. You can use the dashboard to add, remove, or rename pages or widgets.

Figure 1–5 Viewing the Dashboard



Related Information

[Using Dashboards](#)

Reviewing and Filtering Information

You can filter, refine, and customize the presentation of results in Gateway tables by performing the following actions:

- **Filter Results** - Click any column name to sort data in that column.

For example, click **Name** to sort alphabetically by name.

- **Search** - Perform a search for data in the table.

For example, in the table of Gateway users, In the **Search** field on the menu bar, enter the contact's e-mail address, phone number, type, notification only, user status, applications, or first or last name. You can also use the wildcard symbol. Then click the **Search** icon. The Users page is refreshed, displaying the contact(s) matching the full or partial entry.

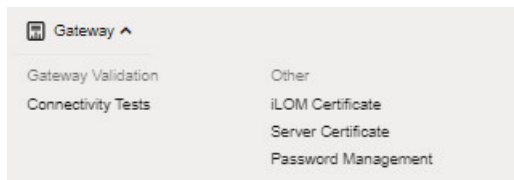
- ? **Re-order** - To reorder a list, use the arrows to alter the display.
- ? **Customize the page** - In the top right of the page or table, use the menu items under the wheel icon to perform the following actions:
 - ? Click **Column Visibility** to deselect column names.
 - ? Click **Print** to print the contents of the page.
 - ? Click **Excel** to save the contents of the page in Microsoft Excel format.
 - ? Click **CSV** to save the contents of the page in comma-separated variable format.

About the Gateway Menu

The Gateway menu provides a number of options for configuration and management of the Gateway.

Note: Menu items may vary from those displayed.

Figure 1–6 Viewing the Gateway Menu



Among the tasks that the Gateway menu enables you to perform are:

- ? [Validating Connections](#)
- ? [Managing Server and ILOM Certificates](#)
- ? [Managing Credentials and Passwords](#)

About the Admin Menu

The Admin menu provides a number of options for administration of the Gateway.

Note: Menu items may vary from those displayed.

Figure 1–7 Viewing the Admin Menu



Among the tasks that the Admin menu enables you to perform are:

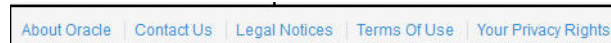
- ? Proxy Setting: [Setting the HTTP Proxy Server](#)

- ? Scheduled Blackouts: [Scheduling Database Blackouts](#)
- ? User List: [Managing Users](#)
- ? Service Requests: [Managing Service Requests](#)
- ? Manage Databases: [Managing Databases and Database Patches](#)
- ? Manage Systems: [Managing Systems and Hosts](#)

Viewing Legal and Copyright Information

The customer information section on the bottom of the screen provides links to Oracle legal notices and policies, as well as displaying a copyright notice.

Figure 1–8 Viewing Customer Information



You can use the customer information section to:

- ? View details about Oracle
- ? Contact Oracle
- ? Review legal notices and policies on privacy rights and terms of use

Using Dashboards

This chapter provides information about using Oracle Advanced Support Gateway to configure and use dashboards.

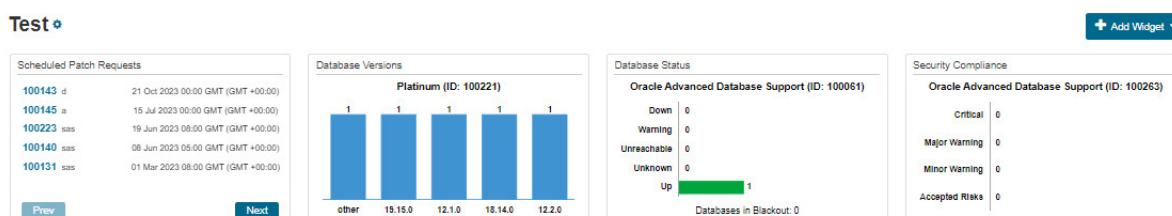
This chapter consists of the following sections:

- ? [About Dashboards](#)
- ? [Accessing the Dashboard](#)
- ? [About Widgets](#)
- ? [Adding a Dashboard](#)
- ? [Adding a Widget](#)
- ? [Managing Widgets](#)

About Dashboards

An Oracle Advanced Support Gateway dashboard is a customizable service dashboard framework that provides an overview of your services and enables you to focus on selected items of interest. The dashboard is made up of a series of data windows called *widgets* as shown in [Figure 2–1](#).

Figure 2–1 Viewing the Dashboard



[Figure 2–1](#), "Viewing the Dashboard" shows a customer service dashboard that displays the status and statistics relating to their systems, hosts, or databases, as well as information about security compliance. Each widget provides one-click access to additional, detailed information about the data presented in the widget.

The dashboard provides a layout to display multiple widgets on one page. You can create multiple (up to five) dashboard pages, with each page made up of multiple widgets. You can use the dashboard to add, remove, or rename pages or widgets.

Related Information[Accessing the Dashboard](#)[About Widgets](#)

Accessing the Dashboard

To use Oracle Advanced Support Gateway to access the dashboard:

1. Log on to the Oracle Advanced Support Gateway portal.
2. From the top level menu, select **Dashboard**.

You can add widgets (and further dashboards) as required.

Related Information[About Dashboards](#)[Adding a Dashboard](#)

About Widgets

A widget is a data window that provides information about a service, such as database version or status, patch compliance, and so on.

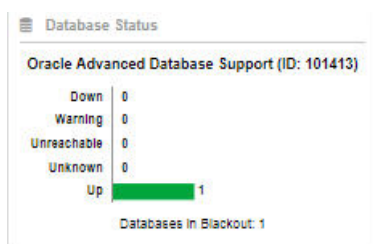
The widgets listed as available are based on the user's role and the services available on the gateway. For example, the Patch Compliance widget is available only if Platinum Services are installed on the gateway.

You can add and remove widgets from a dashboard, reposition widgets on the screen, and drill down into a widget to view the underlying information.

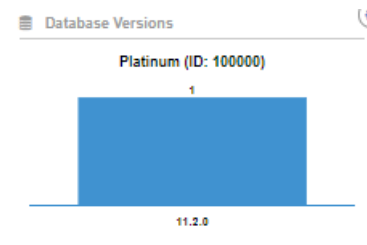
The Gateway widgets include:

- ? **Database Status:** Displays the status counts of the databases activated for a specific service.

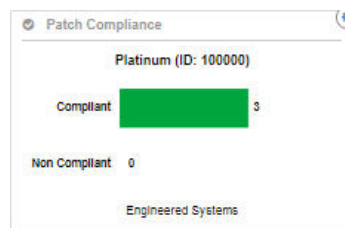
Figure 2–2 Database Status Widget



- ? **Database Versions:** Displays the counts of the databases activated for a specific service by their installed database version.

Figure 2–3 Database Versions Widget

- **Patch Compliance:** Displays the compliance summary for all Oracle Engineered Systems activated under Platinum Services. See [Chapter 9, "Managing Databases and Database Patches."](#)

Figure 2–4 Patch Compliance Widget

- **Patch Requests** Displays scheduled patch requests details. See [Chapter 9, "Managing Databases and Database Patches."](#)

Figure 2–5 Patch Requests Widget

The screenshot shows a widget titled "Scheduled Patch Requests" with a table of data. The table has three columns: ID, Action, and Scheduled Time. Below the table are "Prev" and "Next" buttons.

ID	Action	Scheduled Time
104234	test	29 Aug 2018 00:00 BST (GMT +01:00)
104235	test	14 Aug 2018 00:00 BST (GMT +01:00)
104236	test	14 Aug 2018 00:00 BST (GMT +01:00)
104233	test	13 Aug 2018 00:00 BST (GMT +01:00)
104237	test	08 Aug 2018 00:00 BST (GMT +01:00)

Related Information

[Adding a Widget](#)

Adding a Dashboard

To use Oracle Advanced Support Gateway to add a dashboard:

1. Log on to the Oracle Advanced Support Gateway portal.
2. From the top level menu, select **Dashboard**.
3. Click the + icon to add a dashboard page.
4. Provide a meaningful name for the dashboard page, and click **Create**.

The dashboard page appears.

You can create up to a total of five dashboards per Gateway instance.

Related Information[Accessing the Dashboard](#)

Adding a Widget

To use Oracle Advanced Support Gateway to add a widget:

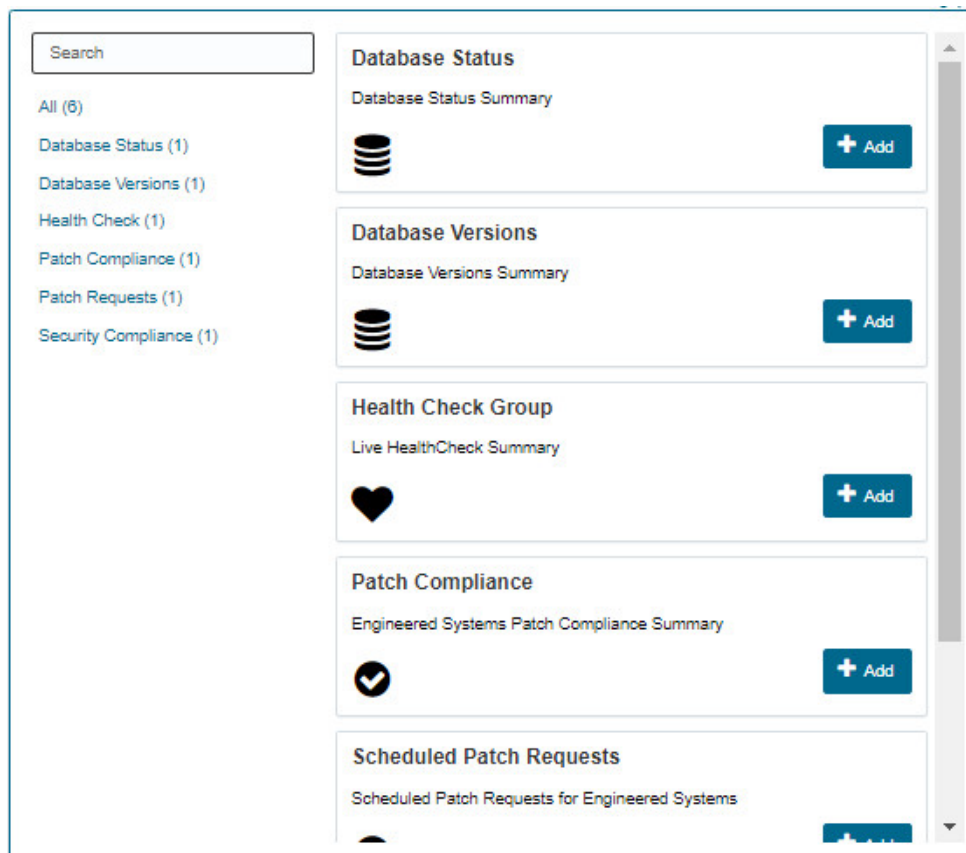
1. Click **Add Widget** as shown in [Figure 2–6](#).

Figure 2–6 Adding a Widget



2. From the available widgets, click **Add** to select the required widget. See [Figure 2–7](#).

Figure 2–7 Selecting a Widget



The widget appears on the dashboard page.

3. (Optional) Add further widgets to the dashboard.

You can add any number of different widgets or multiple instances of the same widget to a dashboard page.

Related Information[Accessing the Dashboard](#)

Managing Widgets

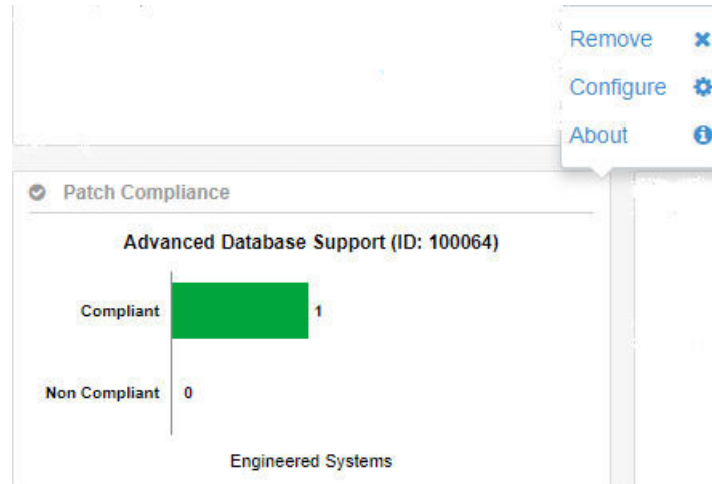
Each widget provides one-click access to additional, detailed information about the data presented in the widget.

You can perform a number of actions on a widget.

To perform an action on a widget:

1. Click the icon associated with a widget as shown in [Figure 2–8](#) to display the actions available on the widget.

Figure 2–8 Viewing the Actions Available on a Widget



2. Select the required action.

Related Information

[Removing a Widget from a Dashboard](#)

[Configuring a Widget](#)

[Reviewing Information about a Widget](#)

Removing a Widget from a Dashboard

To remove a widget from a dashboard:

1. Click the icon shown in [Figure 2–8](#) to display the actions available on the widget.
2. Click **Remove**.

The widget is removed from the dashboard.

Configuring a Widget

To configure a widget:

1. Click the icon shown in [Figure 2–8](#) to display the actions available on the widget.
2. Click **Configure**.
3. Perform the configuration required on the widget.

Note: Only certain widgets can be configured in this way.

Reviewing Information about a Widget

To review information about a widget:

1. Click the icon shown in [Figure 2–8](#) to display the actions available on the widget.
2. Click **About**.

An information panel appears showing a description of the widget and its use.

3. Click **Close**.

Related Information

[Adding a Widget](#)

Managing Users

This chapter describes how to manage accounts for customer users and customer administrators in Oracle Advanced Support Gateway.

It includes the following topics:

- ? [About User Management](#)
- ? [Managing Users](#)

About User Management

You can use the **User List** option from the **Admin** menu to display the **Users** page. You can use this page to manage Gateway users.

The **Users** page provides the ability to view, search for, create and edit user information for your organization. All Gateway users from your organization, and from Oracle, are displayed. The **Users** page enables you to create new customer and provider contacts.

The **Users** page also enables you to customize the way in which fields are displayed, or filter the users displayed by specifying filter criteria. You can also search for users using the Search field. The Search field auto-completes the search criteria entered, returning the first user in the displayed list that matches the criteria.

Managing Users

The Gateway enables customer administrators (CUAs) to add, update, or delete customer users for their organizations. This section contains the following topics:

- ? [Viewing Users](#)
- ? [Adding Users](#)
- ? [Activating Users](#)
- ? [Updating Users](#)
- ? [Deleting Users](#)
- ? [Resetting User Passwords](#)

Viewing Users

The Users page enables you to view and maintain all of your organization's Gateway users and contacts on one page, where:

Prerequisites

- ? A **user** has an account in the Gateway, enabling the user to access the Gateway.
- ? A **contact** is an individual who is involved with Oracle connected services and packages and whose details have been registered in the Gateway. Contacts may or may not have access to the Gateway.

To view Gateway users:

1. Log in to the Gateway.
The Gateway Home page appears.
2. From the **Admin** menu, click **User List**.

The Users page appears, displaying the following information for all entries:

Field	Description
Name	The user name for this Gateway account.
Status	Indicates whether the user status is: <ul style="list-style-type: none">? Enabled, where a Gateway user account has been added and activated. Users with this user status can log in to the Gateway.? Inactive, where a Gateway user account has been deactivated due to inactivity. Users with this user status cannot log in to the Gateway.
Email	The user's e-mail address, as registered in the Gateway.
User Type	Indicates whether the user type is: <ul style="list-style-type: none">? Customer, where a Gateway user is a customer.? Oracle, where a Gateway user is a provider. Oracle users are notified as certain events relating to the user occur. Note: Oracle users are not visible to customer users.
Role	The user's role; for example, <i>Generic Customer</i> or <i>Generic Customer Admin</i> .
Actions>Invite	Invite an individual to become a Gateway user. Note: This action is not available to <i>Generic Customer</i> users.
Actions>Edit	Edit the details of a Gateway user.
Actions>Remove	Remove the user from the Gateway. Note: This action is not available to <i>Generic Customer</i> users.

Adding Users

This section describes how you can add a new user to the Gateway.

Prerequisites

- ? The individual is not already a contact for this customer organization in the Gateway.
- ? You are a customer administrator for your organization, that is, you have been assigned the *Generic Customer Admin* role.

To add a new user of the Gateway:

1. Log in to the Gateway.
The Gateway Home page appears.
2. From the **Admin** menu, click **User List**.
The Users page appears.
3. Click **Create User**.

The Create New User Profile form appears.

4. Enter the following information for the user:

Field	Description
User ID	The user identifier associated with this user. Note: Only letters, numbers, and underscores are allowed. System users are reserved.
First Name	The first name of the user.
Last Name	The last name of the user.
E-mail address	The user's e-mail address. Note: Ensure that the email address is valid and that the user can access it to receive an activation email.
Phone	(Optional) The user's telephone number, including country and area codes.
Status	The status of the user, whether <i>Active</i> or <i>Inactive</i> . An <i>Inactive</i> user is one that has been created, but is not yet activated and hence cannot log on to the Gateway. To activate a user, see " Activating Users ".
Date format	The format to be used when displaying dates for this user.
Time format	The format to be used when displaying times for this user.
User Type	Type of user: <ul style="list-style-type: none"> Customer - creates a customer user. Note: Oracle users may be created on Oracle Advanced Support Platform, but are not visible to customer users.
User Role	Select the type of role (or roles) associated with the user. <ul style="list-style-type: none"> Generic Customer User: This is a business role. A user with the Customer role can log in to the Gateway. Users with this role can also review connectivity checks (that is, the <i>Netcheck</i> functionality.) See Chapter 7, "Validating Connections." Generic Customer Admin This is an administrative role. A user with the Customer Administrator role can manage customer users and perform all customer-facing functions such as password management. This is the default role. Note: Selecting the Generic Customer Admin role ensures that the new user can create other users.

5. Click **Create** to create the user, or click **Cancel** to quit.

When you submit the new user data, you will receive confirmation on the Gateway user interface that an activation email has been sent to the email address you entered.

The Maintain Users page appears, showing information about the new user in the user table.

The new user receives an email in the following format:

Hi <user name>

Please activate your Gateway Portal account by clicking this link: <URL>.

Activating Users

This section describes how you can activate a Gateway user.

Prerequisites

- The user is successfully created on the Gateway.

To activate a Gateway user:

1. Click the URL in the activation email to direct you to the Gateway activation page.
2. Enter a password for the new account.

Passwords must be between 6 and 32 characters long and should contain three of the following four items:

- ? An upper case letter;
- ? A lower case letter;
- ? A symbol (for example ?, %, \$, +);
- ? A number.

When a valid password is set, the user account is activated.

3. Log in to the Gateway using the user credentials.

Updating Users

This section describes how you can update a Gateway user.

This function may be required, for example, after creating a new user, where the user cannot log in to the Gateway, and is shown as an *Inactive user* on the Maintain Users page (as denoted by a grayed out symbol.) An inactive user is one that is created, but is not yet activated and hence can't log on to the Gateway.

Prerequisites

- ? The individual is a contact or user for this customer organization in the Gateway.
- ? You are a customer administrator for this customer organization in the Gateway.

Customers require the *customer admin* role.

To update a Gateway user:

1. Log in to the Gateway.
The Gateway Home page appears.
2. From the **Admin** menu, click **User List**.
The Users page appears.
3. From the list, click the name of the user that you want to update, or select the **Edit** icon associated with the user in the **Actions** column.
The Users form appears for the individual user.
4. Edit the information in the table in "[Adding Users](#)":
5. Click **Save** to update the user (or click **Cancel** to quit without saving.)

The Users page appears, showing information about the user in the user table.

In the case of an *inactive user*, after revising the user's data (for example, email address), click **Send Invite** to resend the activation email.

Deleting Users

This section describes how you can delete a Gateway user.

Prerequisites

- ? The individual is a contact or user for this customer organization in the Gateway.
- ? You are a customer administrator for this customer organization in the Gateway.

To delete a Gateway user:

1. Log in to the Gateway.
The Gateway Home page appears.
2. From the **Admin** menu, click **User List**.
The Users page appears.
3. Select the **Delete** icon associated with the user in the **Actions** column.
When prompted, click **Yes** to confirm that you want to delete this user.
The Users page appears, with a message that the user has been deleted.

Resetting User Passwords

This section describes how you can reset the password of a Gateway user.

Prerequisites

- ? The individual is a contact or user for this customer organization in the Gateway.
- ? You are a customer administrator for this customer organization in the Gateway.

To update the password of a Gateway user:

1. Log in to the Gateway.
The Gateway Home page appears.
2. From the **Admin** menu, click **User List**.
The Users page appears.
3. From the list, click the name of the user that you want to update, or select the **Edit** icon associated with the user in the **Actions** column.
The Users form appears for the individual user.
4. Click **Reset Password** to send the user a form for resetting the password.
5. A confirmation message appears. Click **Yes** to confirm or click **No** to cancel.

Managing Credentials and Passwords

This chapter describes how to view and manage customer credentials for hosts or targets associated to at least one service running on the Gateway production system.

It includes the following topics:

- ? [About Credential Management](#)
- ? [About Credentials](#)
- ? [Viewing Credentials](#)
- ? [Editing Credentials](#)
- ? [Creating Credentials](#)
- ? [About Credential Reports](#)

About Credential Management

The delivery of Oracle connected services using the Gateway requires the safe and secure sharing of passwords between the customer and Oracle. Furthermore, Oracle recommends that you rotate passwords periodically for your production system.

The Gateway provides password or credential management functionality that enables customers to add new accounts, delete existing accounts, and modify stored passwords associated with your databases safely and securely using the customer facing portal running on the Gateway. All passwords managed via the Gateway are routed securely to Oracle Password Vault, which is an application that ensures only authenticated and authorized users can access the accounts information stored in the database.

The automated ORAchk, EXAchk, and OEM deployment procedures, among others, rely on these credentials, so it is essential that these credentials are stored securely using Oracle Enterprise Manager (OEM.)

This is a write only interface and previously entered passwords cannot be read by customer users.

All users, roles, and privileges are created in the Oracle Advanced Support Platform. Refer to the *Managing Users* section of *Oracle Advanced Support Platform User's Guide* on <https://docs.oracle.com/en/engineered-systems/advanced-support-portal/user/index.html>.

About Oracle Platinum Services Customer Requirements

For customers availing of Oracle Platinum Services, refer to the [Oracle Platinum Services – Fault Monitoring What to Expect](#) document; specifically **Appendix III – Access Requirements** that describes how Oracle requires a continuous connection to the Certified

Platinum Configuration during delivery of Oracle Platinum Services, as described in the Oracle Platinum Services Technical Support Policy. The Appendix provides a table describing the user account access required by Oracle during the implementation and ongoing delivery of Oracle Platinum Services.

Displaying Credentials

Credential sets are displayed by target type. The Password Management page lists the managed accounts used by your Oracle Advanced Support Gateway implementation team for which passwords are currently stored in Oracle Password Vault.

Using Credential Management

To use the credential management features:

1. Log on to the portal.

See ["Logging onto the Gateway."](#)

The Gateway Home page appears.

2. From the **Gateway** menu, select **Password Management**.

The Password Management page appears.

Credential sets are displayed by target type. You can view and manage target credentials using the target table.

You can filter the credentials by the target type or name. For example, you can search for Exadata-specific accounts.

You can use the Password Management page to:

- ? Collect and change user credentials;
- ? Populate Password Vault (and/or OEM) with passwords;
- ? Edit credentials in bulk, that is, update multiple targets at the same time for a given credential or credentials;
- ? Review the most up-to-date validation state of credentials.

About Credentials

There are different types of credential defined in the Gateway:

- ? **Required** credentials. See ["About Required Credentials."](#)
- ? **Recommended** credentials. See ["About Recommended Credentials."](#)
- ? **Additional** credentials. See ["About Additional Credentials."](#)

About Required Credentials

Required Credentials are mandatory credentials required for monitoring Gateway targets. Unless these credentials are updated and committed to Oracle Password Vault, the target status is displayed as "Failed" as the target cannot be accessed and monitoring of the target cannot proceed. Examples include *orarom* and *dbsnmp*.

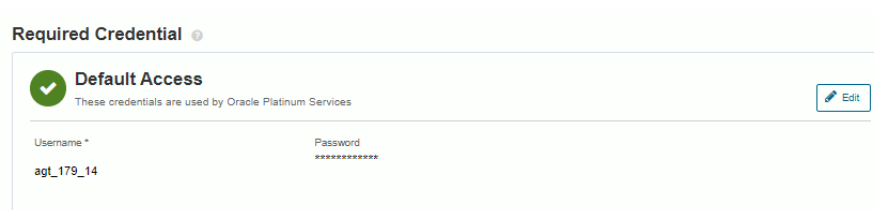
If **Required Credentials** are missing for a particular target, this is flagged using a red warning icon.

You can directly configure credentials using the Credential Management page. These credentials are then updated in Oracle Password Vault as well as in OEM.

These credentials can be viewed and edited singly, or in bulk.

So, for example, in [Figure 4–1](#), for this particular target, required credentials are required for default access by a number of Oracle Support Services.

Figure 4–1 Required Credentials for a Target



Related Information

[Activating Services](#)

[About Recommended Credentials](#)

[About Selected Targets and their Associated Credentials](#)

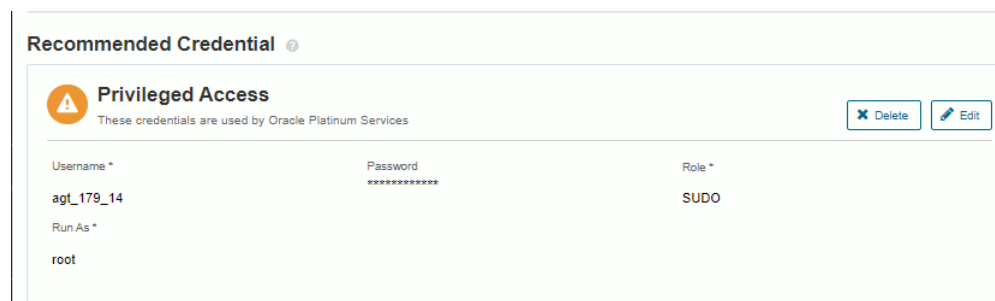
About Recommended Credentials

Recommended Credentials are credentials used to perform particular operations or deliver specific functionality on targets. These operations and functions could include running EXAchk scripts against an Exadata target, triggering EXAchk, and so on. In other words, these credentials are a temporary requirement; the customer sets these credentials when asked and can later edit or delete them as required. Deleting the credentials does not delete the account from the target, but means that Platinum engineers or other Oracle service engineers can no longer access the targets through OEM or Oracle Password Vault. If the customer does not provide these credentials when required, the operation or function - running EXAchk for example - would fail. But not providing Recommended Credentials would not result in an inability to monitor the target.

These credentials can be viewed and edited singly, or in bulk.

So, for example, in [Figure 4–2](#), for this particular target, recommended credentials are used by several services for various functions.

Figure 4–2 Recommended Credentials for a Target



Related Information

[About Required Credentials](#)

[About Additional Credentials](#)

[About Selected Targets and their Associated Credentials](#)

About Additional Credentials

Additional Credentials are those credentials - distinct from **Recommended Credentials** and **Required Credentials** - which customers wish to create and store in Password Vault. These credentials are typically used for testing or demonstration purposes.

Related Information

[About Recommended Credentials](#)

[About Required Credentials](#)

[About Selected Targets and their Associated Credentials](#)

About Selected Targets and their Associated Credentials

The following table displays a number of targets and their associated credentials.

Table 4–1 *Targets and their Associated Credentials*

Target	Required Credentials	Recommended Credentials
Compute/database node	orarom	root
Cell node	celladmin/cellmonitor	root
ILOM	root	Not applicable
Database instance	dbsnmp	Not applicable
PDU	admin	Not applicable
ASM instance	asmsnmp	Not applicable
Cisco switch	admin	Not applicable
InfiniBand switch	ilom_operator	ilom-admin/root
Virtual Machine (VM)	orarom	root
Host	orarom	root
Exadata Grid	(See cell node above)	Not applicable
Oracle PDB	Monitored through database instance	Not applicable
Oracle System Infrastructure Networkswitch	ilom_operator (see InfiniBand switch and Cisco switch)	ilom-admin/root (see InfiniBand switch and Cisco switch)
Oracle SI Rack	Not applicable	Not applicable
Cluster Database	Monitored through database instance	Not applicable

Viewing Credentials

To view credentials by target type:

1. Log on to the portal.

See "[Logging onto the Gateway.](#)"

The Oracle Advanced Support Gateway home page appears.

2. From the **Gateway** menu, select **Password Management**.

The Password Management page appears.

Credential sets are displayed by target type. You can view and manage target credentials using the target table. This table displays "Filter by Exadata Machine" by default.

3. To set the target type, select the required value in the filter list on the top right of the Password Management page. See [Figure 4-3](#).


Figure 4-3 *Selecting the Target Type*



4. All values for the particular target type are displayed.

See [Figure 4-4](#) that shows the credentials for all host instances on a sample Oracle Advanced Support Gateway system.

Figure 4–4 Displaying Credentials for a Target Type

 Password Management

View and Manage Target credentials below. Please refer MOS Article 2285834.1 for more details on how to use the functionality

Credential Reports

Bulk Actions		Search	Filter By Exadata Machine	Filter By Username	
Name	Type	Required Credentials	Recommended Credentials	Total Credentials	Actions
DB Machine brmex (12) Oracle Database Machine					
Host (12)					
<input type="checkbox"/> brmex2adm05vm		!	!	2	
<input type="checkbox"/> brmex2adm05v		!	!	2	
<input type="checkbox"/> brmex2adm05		✓	✓	2	
<input type="checkbox"/> brmex2adm06		!	!	2	
<input type="checkbox"/> brmex2db03		✓	✓	2	

Related Information

[Viewing Credentials for Target Children](#)

Viewing Credentials for Target Children

You can view all credentials for a selected target type, for example, Exadata Machine, as well as its children by expanding the target link.

Editing Credentials

You can edit credentials singly, or in bulk. Refer to the following sections:

- ? ["Editing Credentials"](#)
- ? ["Editing Credentials in Bulk"](#)

Editing Credentials

To edit a credential:

1. Log in to Oracle Advanced Support Gateway.
The Oracle Advanced Support Gateway Home page appears.
2. From the **Gateway** menu, select **Password Management**.
The Password Management page appears.
3. Drill down to the level of the target, or child of the target, as required.
Select the required credential.
Click **Edit**.
The credential page appears. See [Figure 4–5](#).

Figure 4–5 Editing Credentials for a Target

4. For the Required Credential, provide a password for username *orarom* (which has sudo privileges) or *root*. Ensure you provide passwords for all compute nodes.

Edit the following fields as required:

- ? **Username:** Enter the username of the target.
- ? **Password:** Enter the password associated with the target username.
- ? **Confirm Password:** Re-enter the password associated with the target username.
- ? (Optional) **Validate on Save:** Select the **Yes** check box to validate the password prior to saving.

Note: This field is not present for monitoring access, ILOM access, or ASM access.

- ? **(Recommended Credentials Only)**

Role: Select the role associated with the user.

The options include *Normal* (the default) or *SUDO*. For other target types, the roles may vary; for example: for ASM access, the options are *SYSASM* or *SYSDBA*.

- ? **(Recommended Credentials Only)**

Run as: Select the user to run as.

5. For the Recommended Credential, perform the same action: complete the credential either with *orarom* (which has sudo privileges) or the user *root*.
6. Click **Save** (or click **Validate and Save**).

Once the passwords are updated and validated, each nodes displays a green check mark.

Editing Credentials in Bulk

To edit credentials in bulk:

1. Log in to Oracle Advanced Support Gateway.
The Oracle Advanced Support Gateway Home page appears.
2. From the **Gateway** menu, select **Password Management**.
The Password Management page appears.
3. Drill down to the level of the target, or child of the target, as required.
Select the required targets, for example, two ILOM servers. You may first need to filter by user.
When multiple selections are made, the Bulk Actions drop-down list is automatically enabled.

4. From the **Bulk Actions** drop-down list, select **Update**.
5. Select the target for which the bulk edits are required.

The Bulk Edit> [*Credential Name*] page appears. See [Figure 4–6](#).

Figure 4–6 Performing a Bulk Edit on a Credential

6. Complete the steps outlined in ["Editing Credentials."](#)
7. Click **Save**.

Confirm the bulk edit.

Note: The bulk edit overwrites the existing credentials for all selected targets.

Creating Credentials

The **Create New Credential** page enables you to create an additional credential on a target.

To create a credential:

1. Log in to Oracle Advanced Support Gateway.
The Oracle Advanced Support Gateway Home page appears.
2. From the **Gateway** menu, select **Password Management**.
The Password Management page appears.
3. Drill down to the level of the target, or child of the target, as required.
In the Additional Credentials section, click **Create New**.
The Create New Credential page appears. See [Figure 4–7](#).

Figure 4–7 Creating Credentials

Create New Credential
Create a new Credential on Current and Selected targets

Username *

Password *

Select Targets *
- Select a target -

Comments

Cancel

4. Complete the following fields as required:

- ✎ **Username:** Enter the username of the target.
- ✎ **Password:** Enter the password associated with the target username.

Note: The **Expiry Date** field, used to set the date on which the certificate expired, has been removed from this page.

- ✎ **Select Targets:** From the list of available targets, select the Oracle Advanced Support Gateway target associated with the new credential.
(Optional) Use the Ctrl key to make multiple selections.
- ✎ (Optional) **Comments:** Add any information required, for example, to describe the credential owner or function. Any text entered in this field is appended to the “*These credentials are used by...*” subheading under the username.

5. Click **Create** to create the new credential.

About Credential Reports

You can use the credentials report table to view and manage target credentials.

Viewing Target Credentials

To view target credentials:

1. Log in to Oracle Advanced Support Gateway.
The Oracle Advanced Support Gateway Home page appears.
2. From the **Gateway** menu, select **Password Management**.
The Password Management page appears.
3. In the top right of the page, click **Credential Reports**.

The credential list appears.

You can search for a particular credential, view a target associated with a credential, print the credential report, or save the report in Microsoft Excel or CSV format.

Managing Systems and Hosts

This chapter provides information about using Oracle Advanced Support Gateway to manage systems and hosts as well as requesting activations of new systems and the addition of new hosts.

This chapter consists of the following sections:

- ? [About Managing Systems and Hosts](#)
- ? [Adding a New System](#)
- ? [About Adding a New Engineered System](#)
- ? [Viewing Target Configurations](#)
- ? [Managing System Passwords](#)
- ? [Deactivating Services](#)

Related Information

[About Patching Requests](#)

[Managing Databases and Database Patches](#)

About Managing Systems and Hosts

You can use Oracle Advanced Support Gateway to manage existing systems and hosts as well as requesting the activation of new systems and the addition of new hosts.

Refer to the following sections:

- ? [Adding a New System](#)
- ? [About Adding a New Engineered System](#)

Adding a New System

You can activate new systems that are auto-discovered on the Gateway.

To use Oracle Advanced Support Gateway to activate new systems:

1. Log in to Oracle Advanced Support Gateway.
The Oracle Advanced Support Gateway Home page appears.
2. From the **Admin** menu, click **Manage Systems**.
The Systems and Hosts page appears.
3. Click **Add New**.

The Add System page appears.

You use this page to create a request for the monitoring of an Engineered System. This request is then submitted to an Oracle service engineer to complete the monitoring process.

Refer to the following sections:

- ? [About Adding a New Engineered System](#)

About Adding a New Engineered System

You can use Oracle Advanced Support Gateway to create a request to monitor the following Oracle Engineered Systems:

- ? Exadata
- ? Exalogic
- ? SuperCluster
- ? Zero Data Loss Recovery Appliance (ZDLRA)

Note: In order to monitor other Oracle Engineered Systems, such as Exalytics In-Memory Machine, please refer to your Oracle representative for further details.

This section outlines how to collect and validate all required implementation information directly from the customer using the Gateway user interface. There are several stages in creating the monitoring request:

- ? **Welcome:** Introducing the wizard used to create the monitoring request and confirm the pre-requisite tasks
- ? **Add System:** Adding a system, where *system* is understood to mean an Oracle Engineered System, as outlined above
- ? **System Information:** Supplying information about the system
- ? **Network Check:** Checking system connectivity
- ? **Set Credentials:** Performing checks on the system credentials;
- ? **Full Network Check:** Checking end-to-end system connectivity;
- ? **Compliance Check:** Verifying system compliance and network connections
- ? **Complete:** Submitting the provisioning request to Oracle and receiving confirmation of the request

To use the Gateway to create a request for the monitoring of an Engineered System:

1. Log on to the Oracle Advanced Support Gateway portal.
The Oracle Advanced Support Gateway home page appears.
2. From the top-level **Admin** menu, select **Manage Systems**.
The Systems and Hosts page appears.
You use this page to manage existing systems and hosts as well as request activations of new systems and add new hosts.
3. Click **Add New**.
The Welcome to the System and Host install Wizard page appears.
This page provides information about tasks to be performed and information you'll need to access before getting started:

This wizard will help you install monitoring agents on standalone systems or create a request for the monitoring of an Engineered System. As part of the wizard workflow you will be requested to provide the following:

- ? Privileged host credentials;
- ? For standalone systems: IP addresses and their fully qualified domain names (FQDN);
- ? For Engineered Systems: The Engineered System's schematic file, serial number, CSI/MOS ID (and in the case of users of the Platinum Service, the associated Platinum implementation service request (PISR) number);
- ? Additional custom install settings.

The wizard performs the following checks before taking any actions:

- ? Validate the network connectivity between the Gateway and the hosts;
- ? Test credentials; the self-service activation process enables users to enter credentials for individual nodes;
- ? Check each host meets minimum prerequisites for agent installation.

Service activation on multiple targets continues after a single target failure. During service activation, all targets are shown, together with any reason why a target is not eligible for activation.

Before you get started:

- ? Please review the [Oracle Advanced Support Gateway Security Guide](#)

As part of the wizard workflow, users are requested to provide IP address details and passwords for the required Engineered System. Checks are then performed to validate the network connectivity and passwords before a Service Request (SR) is created and submitted for an Oracle engineer to complete the remaining tasks.

4. (Optional) Select the **Don't show message again** check box so that the Welcome Message page is not displayed in future as part of the Add Agent workflow.
5. Click **Get Started**.

The Add System page appears.

Figure 5–1 Adding a System

System Install

1. Add System 2. System Information 3. Network Check 4. Set Credentials 5. Full Network Check

6. Compliance Check Complete

+ Add System
Select system type and either upload CSV file or manually enter information as appropriate.

Select System Type *

* required fields

Exadata Exalogic SuperCluster ZDLRA Other & Single Hosts

Back Exit Install Settings Next

Enter System Name

In general, you can add systems by:

- Importing a schematic file by selecting a comma-separated value (CSV) file from your local computer, *or*
- Manually entering information, for example, host IP address, schematic directory, filename, and SSH credentials, as appropriate

Note: Verify that the CSV file is valid: that it contains the management host name and IP addresses. Edit the CSV file if it contains client host name or IP details.

To add a supported Oracle Engineered System, select one of the following options:

- **Exadata.** See ["Adding an Oracle Exadata Engineered System."](#)
- **Exalogic.** See ["Adding an Oracle Exalogic Engineered System."](#)
- **SuperCluster.** See ["Adding an Oracle SuperCluster Engineered System."](#)
- **ZDLRA.** See ["Adding an Oracle ZDLRA Engineered System."](#)

Adding an Oracle Exadata Engineered System

To add an Exadata system:

1. Follow the initial steps in ["About Adding a New Engineered System."](#)
2. From the Select System Type field, select **Exadata**.
3. From the System Information field, select one of the following options:
 - **File Upload.** This option enables you upload a local file.
Go to step 5.
 - **Remote Upload.** This option enables you to use the file URL from a remote system.
Go to step 4.
4. (For a remote file upload) Complete the following fields:
 - **Host IP Address:** Enter the IP address of the system on which the file is located.

- ? **Schematic Directory:** Enter the directory where the file is located.
- ? **Filename:** Enter the full file name.
- ? (Optional; if you want to provide SSH credentials) **Username:** Enter the user name associated with the directory.
- ? (Optional; if you want to provide SSH credentials) **Password:** Enter the password associated with the user name.

Continue to step 6.

5. (For a local file upload) In the **Local File** field, click **Browse**, and select a file on your local machine.

Note: If you don't know how to find the CSV file, refer to the instructions in [MOS document 2231081.1](#). In particular, you need to raise an SR with My Oracle Support.

6. Click **Next**.

The Enter System Name page appears. A sample is provided in [Figure 5–2](#).

Figure 5–2 Supplying Engineered System Information

System Install

✓ 1. Add System **2. System Information** 3. Network Check 4. Set Credentials 5. Full Network Check 6. Compliance Check Complete

System Information
Supply information about the Engineering System

Type: exadata System Name *: DB Machine seldb3 * required fields

Back Exit Install Settings Next

Add System View System Info

7. Supply the Engineered System information as follows:
 - a. The **Type** field is automatically completed with the type of Engineered System. This field cannot be edited.
 - b. The **System Name** field is automatically completed with the name of the Engineered System. Edit as required.
8. Click **Next**.

The View System Information page appears.

Figure 5–3 Viewing System Information

System Information
View, Edit, Add or Delete the information collected from source.

▼ Physical Compute Nodes

Search + Add

Admin Name	Admin IP	ILOM Name	ILOM IP	System Type	Actions
aeib3db04.acs.oracle.com	10.146.28.7	aeib3db04-ilom.acs.oracle.com	10.146.28.29	Exadata DB Node	✎ ✕
aeib3db03.acs.oracle.com	10.146.28.6	aeib3db03-ilom.acs.oracle.com	10.146.28.28	Exadata DB Node	✎ ✕

► Exadata Storage Servers

Select new Target to add

OVS Compute Nodes + Add

← Back Exit Install Settings Next

Modify System Info Check Network Connectivity

9. Confirm the information collected from the source file.

For example, in the Physical Compute Nodes and Exadata Storage Servers sections, review the systems defined by admin name, admin IP, ILOM name, and ILOM IP.

10. (Optional) Select a new target to add from the following target types:

- OVS compute nodes

To add an OVS compute node, complete the *Admin Name*, *Admin IP*, *ILOM Name*, *ILOM IP* and *System Type* fields.

- Agent only nodes

To add an agent only node, complete the *Admin Name*, *Admin IP* and *System Type* fields.

- InfiniBand switches

To add an InfiniBand switch, complete the *Admin Name*, *Admin IP* and *System Type* fields.

- Power Distribution Unit (PDU)

To add a PDU, complete the *Admin Name*, *Admin IP* and *System Type* fields.

- Cisco switch

To add a Cisco switch, complete the *Admin Name*, *Admin IP* and *System Type* fields.

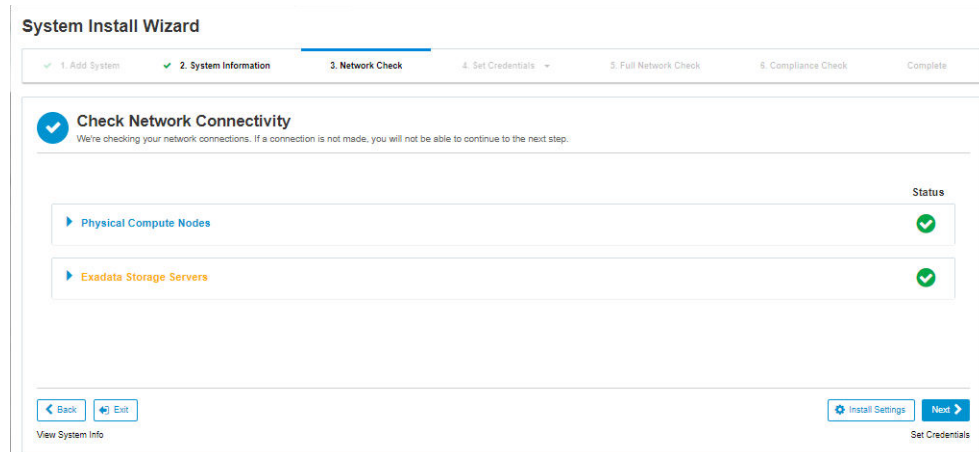
Note: Warning messages may be displayed if you do not add certain target types. For example, you may see a warning message such as:

PDU target type node is not added. Do you wish to continue?

Select **Yes** or **No**.

11. Click **Next**.

The Check Network Connectivity page appears.

Figure 5–4 Checking Network Connectivity

12. Review the connectivity checks (Netcheck) back to the Gateway for all of the targets uploaded through the schematic file. Expand the type sections, for example, Exadata Storage Servers, to review the details.

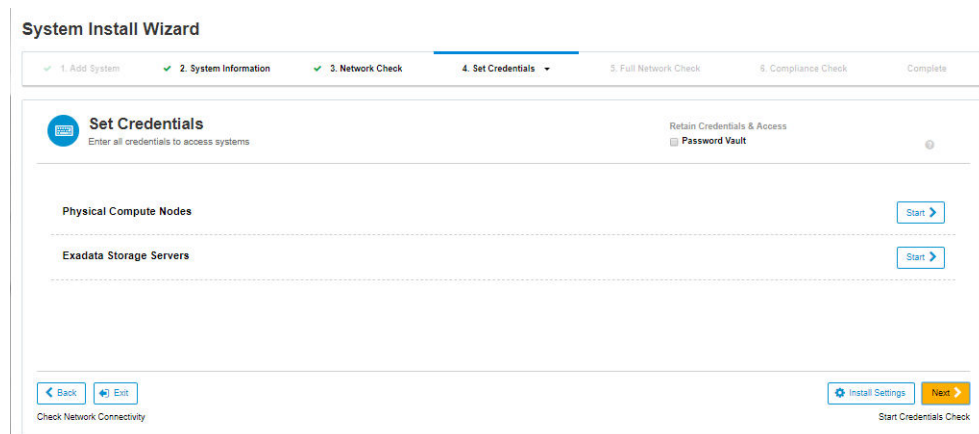
Note: If any mandatory test fails, it is not possible to proceed to the next stage of adding the Engineered System.

A typical message advises that “Mandatory tests failed and must be resolved to continue. Please check [Oracle Advanced Support Gateway Security Guide](#)”.

Note: If any non-mandatory test fails, you should review the warning message and take appropriate action before proceeding to the next stage of adding the Engineered System.

- a. (Optional) Click **Back** to change system details.
- b. (Optional) Click **Retest** to run the connectivity tests again.
- c. Click **Next**.

The Set Credentials page appears.

Figure 5–5 Setting Engineered System Credentials

13. Supply user credentials for each target to perform validation.

For database servers and compute nodes:

- a. Click **Start** to begin the validation process for the target group, that is, database servers or compute nodes.
- b. (Optional) In the **Credentials** field, select the **Same for All** check box to apply the credentials to all servers of the same type (database servers).
- c. In the **Host Username** field, enter the name of the system.
- d. In the **Host Password** field, enter the password associated with the system.
(Optional) Toggle the eye icon to view or hide the details.
- e. In the **Priv Mode** field, select the mode to be used to gain the required root level privilege on the system. The options are *sudo*, *su*, and *pfexec*.
- f. In the **Root Password** field, enter the root password associated with the system.
(Optional) Toggle the eye icon to view or hide the details.
- g. In the **ILOM Username** field, enter the ILOM username.
- h. In the **ILOM Password** field, enter the password associated with the ILOM.
(Optional) Toggle the eye icon to view or hide the details.

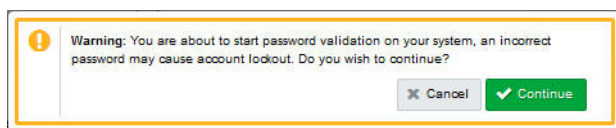
In the Monitoring Credentials credentials section, you need to provide details for monitoring that are saved for future usage but which are not validated.

Complete the following fields to configure monitoring credentials for the Physical Compute Nodes:

- a. In the **Database** field, enter the database name.
- b. In the **DBSNMP Password** field, enter the SNMP password associated with the database.
(Optional) Toggle the eye icon to view or hide the details.
- c. In the **ASM Cluster Name** field, enter the name of the Automatic Storage Management (ASM) Cluster.
- d. In the **ASMSNMP Password** field, enter the SNMP password associated with the Automatic Storage Management (ASM) Cluster.
(Optional) Toggle the eye icon to view or hide the details.
- e. Click **Next**.

A warning popup appears: supplying incorrect passwords may result in being locked out of your account.

Figure 5–6 Target Validation Warning



For Exadata storage servers:

- a. (Optional) In the **Credentials** field, select the **Same for All** check box to apply the credentials to all servers of the same type (Exadata storage servers).
- b. The **Host Username** field contains the value, *root*. This field cannot be edited.
- c. In the **Host Password** field, enter the root password.

(Optional) Toggle the eye icon to view or hide the details.

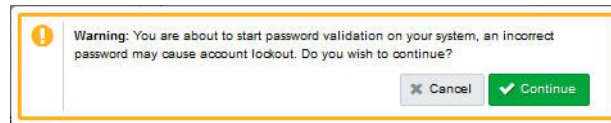
- d. In the **ILOM Username** field, enter the ILOM username.
- e. In the **ILOM Password** field, enter the password associated with the ILOM.

(Optional) Toggle the eye icon to view or hide the details.

- f. Click **Next**.

A warning popup appears: supplying incorrect passwords may result in being locked out of your account.

Figure 5–7 Target Validation Warning



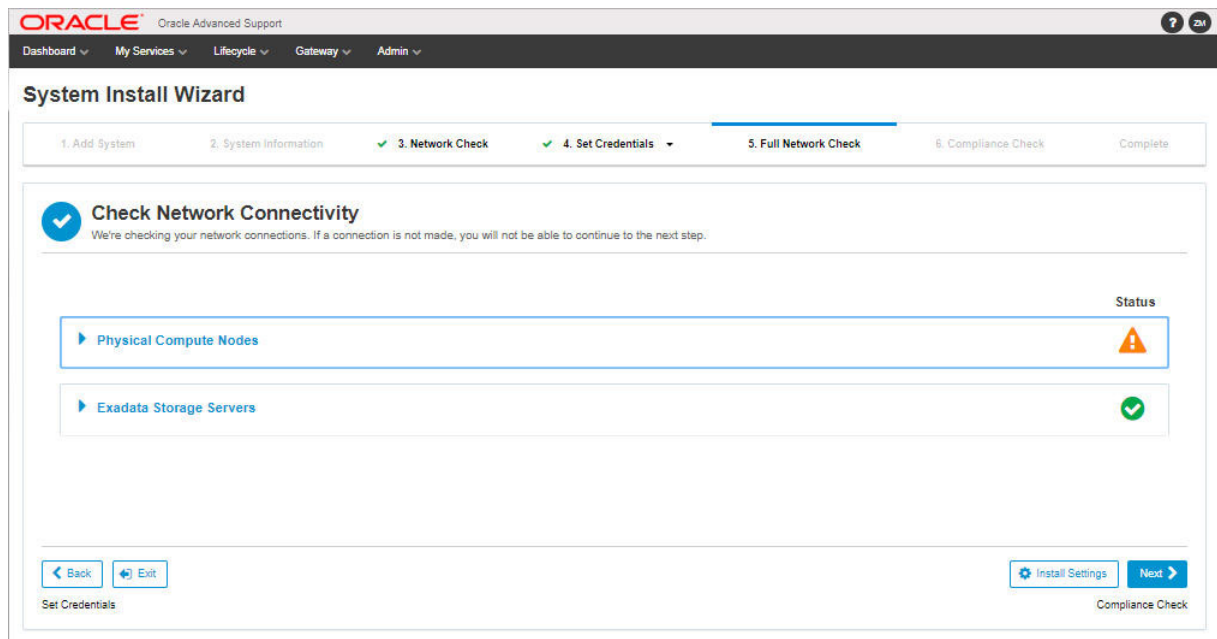
- g. Click **Continue**.

The validation check is run and a message appears, stating that the credentials have been validated.

- h. Click **Next**.

The Check Network Connectivity page appears.

Figure 5–8 Checking Whole Network Connectivity

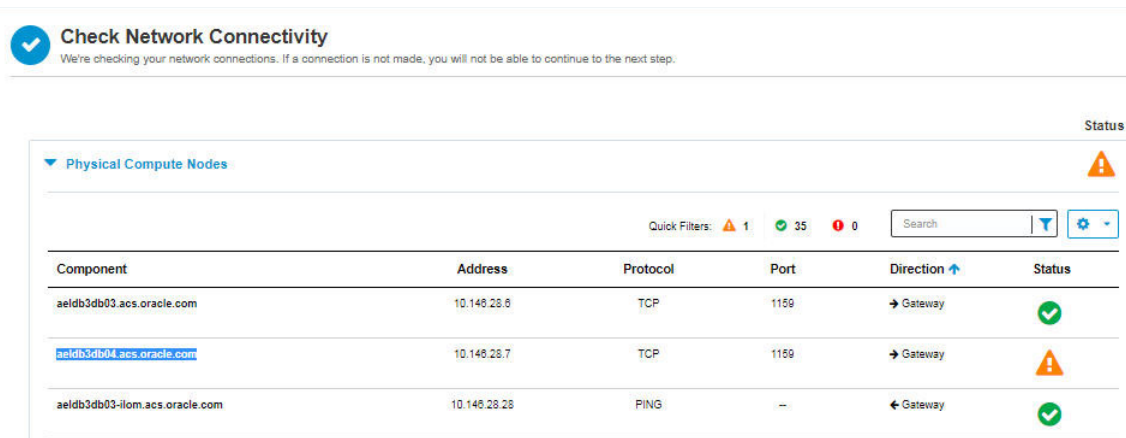


All network connections (that is, to *or* from the Gateway to the device) are checked.

If a connection is not made, then a status of *Failed* is displayed as shown for the Physical Compute Nodes in [Figure 5–8](#).

Expand the Physical Compute Nodes to view the node, in this case, *aeldb3db04.acs.oracle.com*, that is failing the connectivity check. See [Figure 5–9](#).

Figure 5–9 Viewing Failing Network Connectivity

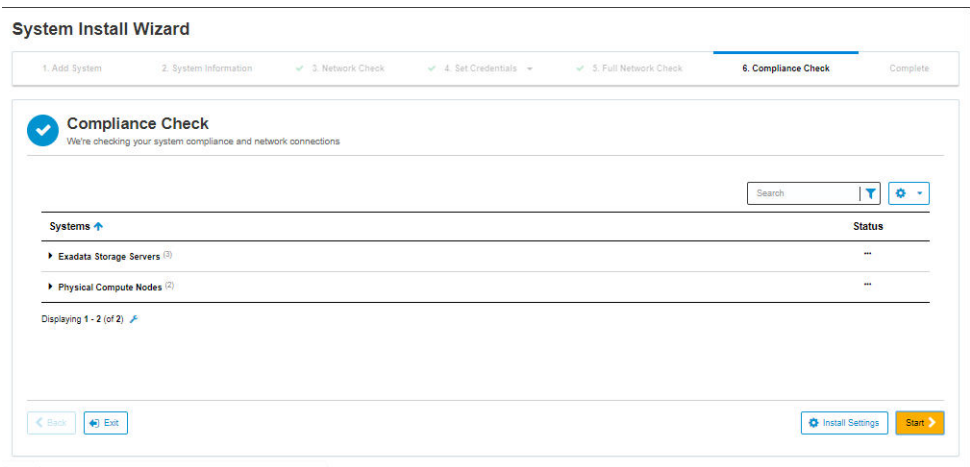


Reconfigure the failing connection and validate it before continuing. When all connectivity passes, continue to the next step.

- i. Click **Next**.

The Compliance Check page appears.

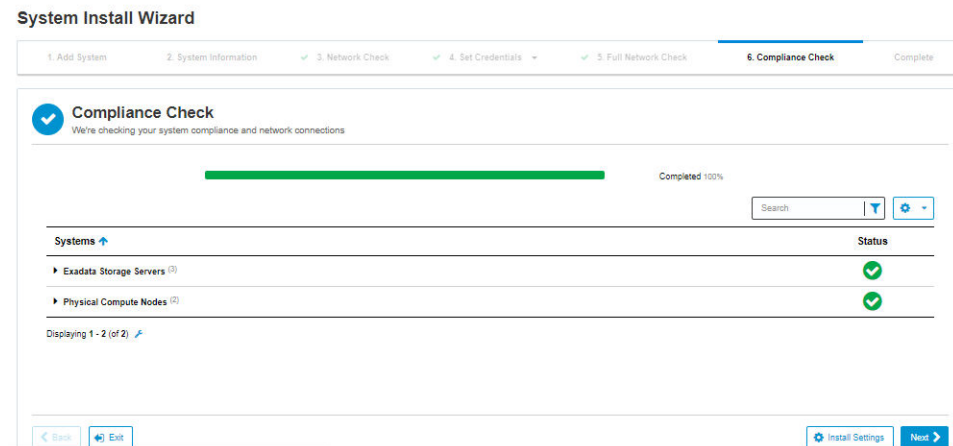
Figure 5–10 Checking System Compliance and Network Connections



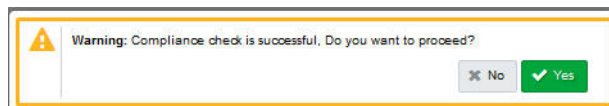
- 14. To enable Oracle to validate system compliance and network connections:

- a. Click **Start**.

A progress bar measures the rate of system validation. When it reaches 100%, system status displays as complete and a message appears stating that the compliance check passed successfully.

Figure 5–11 System Compliance Validated**b. Click Next.**

A warning message appears stating that the compliance check is successful, and asking whether you would like to proceed.

Figure 5–12 Completing System Installation**c. Click Yes.**

The Submit Provisioning Request to Oracle page appears.

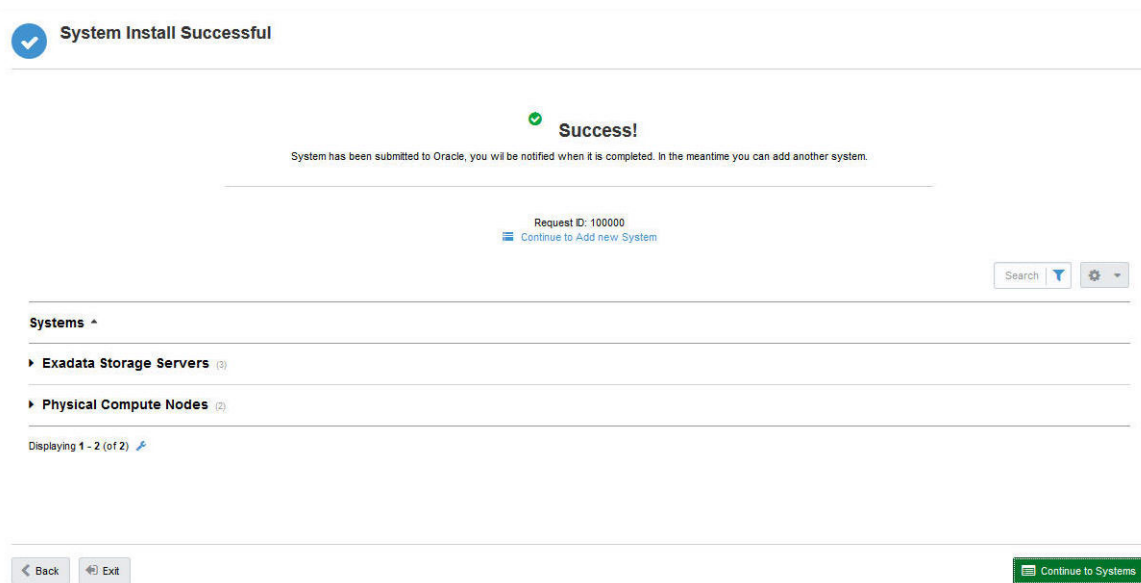
This page states that the system precheck has been completed (that is, all system information has been validated.)

To proceed with system installation, submit the provisioning request for the Engineered System to Oracle.

15. Click Submit Details to Oracle.

A provisioning request is submitted to Oracle. You will be notified when it is completed.

The System Install Successful page appears.

Figure 5–13 System Installation Successful

16. A service activation request summary is sent to the customer contact by email. It states:

Dear Customer,

We have received your request and will start the planning process for <Service Name> Activation on your Exadata system <Exa_system_name>. Below is a summary of your Service Activation request.

See the following table which provides a sample summary response from Oracle.

Note: Certain values in the table have been obfuscated for security reasons.

Field	Sample value
Request ID	4
System Type	Exadata
System Name	<Exadata_system_name>
HW CSI	15262999
Rack Serial Number	<Exa_serial_number>
Gateway	<Gateway_name>
Requested Date DD/MM/YYYY	For example, 11/04/2023
Customer	<Customer_name>
Customer Contact	<Customer_contact_name>
Implementation Contact	<Oracle_Implementation_Engineer_contact_name>

17. At this point, you can perform one of the following actions:

- ? Select **Continue to Add new System** to install a monitoring agent on a standalone system or to create a request for the monitoring of an Oracle Engineered System.
- ? Select **Continue to Systems** to revert to the Systems and Hosts page.

See [Chapter 5, "Managing Systems and Hosts."](#)

- ? Select **Exit** to revert to the Systems and Hosts page.
See [Chapter 5, "Managing Systems and Hosts."](#)

Adding an Oracle Exalogic Engineered System

To add an Exalogic system:

1. Follow the initial steps in ["About Adding a New Engineered System."](#)

Note: You can review the screenshots referred to in the following steps in the section on ["Adding an Oracle Exadata Engineered System."](#)

2. From the Select System Type field, select **Exalogic**.
3. From the System Information field, select one of the following options:
 - ? **File Upload.** This option enables you upload a local file.
Go to step 4.
 - ? **Remote Upload.** This option enables you to use the file URL from a remote system.
Go to step 5.
4. (For a remote file upload) Complete the following fields:
 - ? **Host IP Address:** Enter the IP address of the host on which the file is located.
 - ? **Schematic Directory:** Enter the directory where the file is located.
 - ? **Filename:** Enter the full file name.
 - ? (Optional; if you want to provide SSH credentials) **Username:** Enter the user name associated with the directory.
 - ? (Optional; if you want to provide SSH credentials) **Password:** Enter the password associated with the user name.

Continue to step 6.

5. (For a local file upload) In the **Local File** field, click **Browse**, and select a file on your local machine.
6. Click **Next**.
The Enter System Name page appears.
7. Supply the Engineered System information as follows:
 - a. The **Type** field is automatically completed with the type of Engineered System. This field cannot be edited.
 - b. The **System Name** field is automatically completed with the name of the Engineered System. Edit as required.
8. Click **Next**.

The System Information page appears.

You can view, edit, add to or delete the information collected from source.

9. Confirm the information collected from the source file.
10. (Optional) Select a new target to add from the following target types:
 - ? Physical compute nodes
To add a physical compute node, complete the *Admin Name*, *Admin IP*, *ILOM Name*, *ILOM IP* and *System Type* fields.

⌵ Exadata storage servers

To add an Exadata storage server, complete the *Admin Name*, *Admin IP*, *ILOM Name*, *ILOM IP* and *System Type* fields.

⌵ OVS compute nodes

To add an OVS compute node, complete the *Admin Name*, *Admin IP*, *ILOM Name*, *ILOM IP* and *System Type* fields.

⌵ InfiniBand switches

To add an InfiniBand switch, complete the *Admin Name*, *Admin IP* and *System Type* fields.

⌵ Agent only nodes

To add an agent only node, complete the *Admin Name*, *Admin IP* and *System Type* fields.

⌵ Power Distribution Unit (PDU)

To add a PDU, complete the *Admin Name*, *Admin IP* and *System Type* fields.

⌵ Cisco switch

To add a Cisco switch, complete the *Admin Name*, *Admin IP* and *System Type* fields.

⌵ Ethernet switch

To add an Ethernet switch, complete the *Admin Name*, *Admin IP* and *System Type* fields.

11. Click Next.

The Check Network Connectivity page appears.

12. Review the connectivity checks (Netcheck) back to the Gateway for all of the targets uploaded through the schematic file.

Note: If any mandatory test fails, it is not possible to proceed to the next stage of adding the Engineered System.

A typical message advises that “Mandatory tests failed and must be resolved to continue. Please check [Oracle Advanced Support Gateway Security Guide](#)”.

Note: If any non-mandatory test fails, you should review the warning message and take appropriate action before proceeding to the next stage of adding the Engineered System.

- a. (Optional) Click **Back** to change system details.
- b. (Optional) Click **Retest** to run the connectivity tests again.
- c. Click **Next**.

The Set Credentials page appears.

13. Supply user credentials for each target to perform validation.

For database servers:

- a. (Optional) In the **Credentials** field, select the **Same for All** check box to apply the credentials to all servers of the same type (database servers).
- b. In the **Host Username** field, enter the name of the system.
- c. In the **Host Password** field, enter the password associated with the system.
(Optional) Toggle the eye icon to view or hide the details.

- d. In the **Priv Mode** field, select the mode to be used to gain the required root level privilege on the system. The options are **sudo**, **su**, and **pfexec**.
 - e. In the **Root Password** field, enter the root password associated with the system.
(Optional) Toggle the eye icon to view or hide the details.
 - f. In the **ILOM Username** field, enter the ILOM username.
 - g. In the **ILOM Password** field, enter the password associated with the ILOM.
(Optional) Toggle the eye icon to view or hide the details.
 - h. In the Retain Credentials and Access section in the top-right corner of the page, select the **Password Vault** check-box to upload the credentials into Oracle Password Vault once validation is complete.
 - i. Click **Validate**.
A warning popup appears: supplying incorrect passwords may result in being locked out of your account.
 - j. Click **Continue**.
The validation check is run and a message appears, stating that the credentials have been validated.
 - k. Click **Next**.
The Check Network Connectivity page appears.
14. To check end-to-end connectivity:
- a. All network connections (that is, *to* or *from* the Gateway to the device) are checked.
If a connection is not made, then a status of *Failed* is displayed.
Reconfigure the failing connection and validate it before continuing. When all connectivity passes, continue to the next step.
 - b. Click **Next**.
The Compliance Check page appears.
15. To enable Oracle to validate system compliance and network connections:
- a. Click **Start**.
A progress bar measures the rate of system validation. When it reaches 100%, system status displays as complete and a message appears stating that the compliance check passed successfully.
 - b. Click **Next**.
A warning message appears stating that the compliance check is successful, and asking whether you would like to proceed.
 - c. Click **Yes**.
The Submit Provisioning Request to Oracle page appears.
16. Click **Submit Details to Oracle**.
The System Install Successful page appears.
System prechecks are complete, and a provisioning request is submitted to Oracle.
A service activation request summary is sent to the customer contact by email.

Adding an Oracle SuperCluster Engineered System

To add a SuperCluster system:

1. Follow the initial steps in ["About Adding a New Engineered System."](#)
Note: You can review the screengrabs referred to in the following steps in the section on ["Adding an Oracle Exadata Engineered System."](#)
2. From the Select System Type field, select **SuperCluster**.
3. From the System Information field, select one of the following options:
 - ? **File Upload.** This option enables you upload a local file.
Go to step 5.
 - ? **Remote Upload.** This option enables you to use the file URL from a remote system.
Go to step 4.
4. (For a remote file upload) Click **Remote Upload File** and complete the following fields:
 - ? **Host IP Address:** Enter the IP address of the system on which the file is located.
 - ? **Schematic Directory:** Enter the directory where the file is located.
 - ? **Filename:** Enter the full file name.
 - ? **Username:** Enter the user name associated with the directory.
 - ? **Password:** Enter the password associated with the user nameContinue to step 6.
5. (For a local file upload) In the **Local File** field, click **Browse**, and select a file on your local machine.
6. Click **Next**.
The Enter System Name page appears.
7. Supply the Engineered System information as follows:
 - a. The **Type** field is automatically completed with the type of Engineered System. This field cannot be edited.
 - b. The **System Name** field is automatically completed with the name of the Engineered System. Edit as required.
8. (Optional) Select a new target to add from the following target types:
 - ? OVS compute nodes
To add an OVS compute node, complete the *Admin Name*, *Admin IP*, *ILOM Name*, *ILOM IP* and *System Type* fields.
 - ? Agent only nodes
To add an agent only node, complete the *Admin Name*, *Admin IP* and *System Type* fields.
 - ? InfiniBand switches
To add an InfiniBand switch, complete the *Admin Name*, *Admin IP* and *System Type* fields.
 - ? Power Distribution Unit (PDU)
To add a PDU, complete the *Admin Name*, *Admin IP* and *System Type* fields.

7 Cisco switch

To add a Cisco switch, complete the *Admin Name*, *Admin IP* and *System Type* fields.

9. Click **Next**.

The View System Information page appears.

10. Confirm the information collected from the source file.

11. Click **Next**.

The Check Network Connectivity page appears.

12. Review the connectivity checks (Netcheck) back to the Gateway for all of the targets uploaded through the schematic file. Expand the type sections, such as ZFS Storage or Compute Nodes, to review the details.

Note: If any mandatory test fails, it is not possible to proceed to the next stage of adding the Engineered System.

A typical message advises that “The service on the destination must be available and any firewalls between the Gateway and the endpoint must have the required firewall rules (IP address, port, and protocol) that allow for remote connectivity. The ports and protocols are specified in the Network Protocol and Port Matrix of [Oracle Advanced Support Gateway Security Guide](#)”.

Note: If any non-mandatory test fails, you should review the warning message and take appropriate action before proceeding to the next stage of adding the Engineered System.

- a. (Optional) Click **Back** to revise the system details.
- b. (Optional) Click **Retest** to run the connectivity tests again.
- c. Click **Next**.

The Set Credentials page appears.

13. Supply user credentials for each target to perform validation.

For database servers:

- a. (Optional) In the **Credentials** field, select the **Same for All** check box to apply the credentials to all servers of the same type (database servers).
- b. In the **Host Username** field, enter the name of the system.
- c. In the **Host Password** field, enter the password associated with the system.
(Optional) Toggle the eye icon to view or hide the details.
- d. In the **Priv Mode** field, select the mode to be used to gain the required root level privilege on the system. The options are **sudo**, **su**, and **pfexec**.
- e. In the **Root Password** field, enter the root password associated with the system.
(Optional) Toggle the eye icon to view or hide the details.
- f. In the **ILOM Username** field, enter the ILOM username.
- g. In the **ILOM Password** field, enter the password associated with the ILOM.
(Optional) Toggle the eye icon to view or hide the details.

For Exadata storage servers and ZFS storage arrays:

- a. (Optional) In the **Credentials** field, select the **Same for All** check box to apply the credentials to all servers of the same type (Exadata storage servers).
- b. The **Host Username** field contains the value, *root*. This field cannot be edited.

- c. In the **Host Password** field, enter the root password.
(Optional) Toggle the eye icon to view or hide the details.
 - d. In the **ILOM Username** field, enter the ILOM username.
 - e. In the **ILOM Password** field, enter the password associated with the ILOM.
(Optional) Toggle the eye icon to view or hide the details.
 - f. Click **Validate**.
A warning popup appears: supplying incorrect passwords may result in being locked out of your account.
 - g. Click **Continue**.
The validation check is run and a message appears, stating that the credentials have been validated.
 - h. Click **Next**.
The Check Network Connectivity page appears.
- 14. To check end-to-end connectivity:
 - a. All network connections (that is, *to* or *from* the Gateway to the device) are checked.
If a connection is not made, then a status of *Failed* is displayed.
Reconfigure the failing connection and validate it before continuing. When all connectivity passes, continue to the next step.
 - b. Click **Next**.
The Compliance Check page appears.
- 15. To enable Oracle to validate system compliance and network connections:
 - a. Click **Start**.
A progress bar measures the rate of system validation. When it reaches 100%, system status displays as complete and a message appears stating that the compliance check passed successfully.
 - b. Click **Next**.
A warning message appears stating that the compliance check is successful, and asking whether you would like to proceed.
 - c. Click **Yes**.
The Submit Provisioning Request to Oracle page appears.
- 16. Click **Submit Details to Oracle**.
System prechecks have been completed, and a provisioning request is submitted to Oracle.
The System Install Successful page appears.
- 17. A service activation request summary is sent to the customer contact by email.
- 18. At this point, you can perform one of the following actions:
 - ⌵ Select **Continue to Add new System** to install a monitoring agent on a standalone host or to create a request for the monitoring of an Oracle Engineered System.
 - ⌵ Select **Exit** to revert to the Systems and Hosts page.

Adding an Oracle ZDLRA Engineered System

To add a Zero Data Loss Recovery Appliance (ZDLRA) system:

1. Follow the initial steps in ["About Adding a New Engineered System."](#)

Note: You can review the screengrabs referred to in the following steps in the section on ["Adding an Oracle Exadata Engineered System."](#)

2. From the Select System Type field, select **ZDLRA**.
3. From the System Information field, select one of the following options:
 - ? **File Upload.** This option enables you upload a local file.
Go to step 5.
 - ? **Remote Upload.** This option enables you to use the file URL from a remote system.
Go to step 4.
4. (For a remote file upload) Click **Remote Upload File** and complete the following fields:
 - ? **Host IP Address:** Enter the IP address of the system on which the file is located.
 - ? **Schematic Directory:** Enter the directory where the file is located.
 - ? **Filename:** Enter the full file name.
 - ? **Username:** Enter the user name associated with the directory.
 - ? **Password:** Enter the password associated with the user name

Continue to step 6.
5. (For a local file upload) In the **Local File** field, click **Browse**, and select a file on your local machine.
6. Click **Next**.
The Enter System Name page appears.
7. Supply the Engineered System information as follows:
 - a. The **Type** field is automatically completed with the type of Engineered System. This field cannot be edited.
 - b. The **System Name** field is automatically completed with the name of the Engineered System. Edit as required.
8. Click **Next**.
The View System Information page appears.
9. Confirm the information collected from the source file.
10. (Optional) Select a new target to add from the following target types:
 - ? OVS compute nodes
To add an OVS compute node, complete the *Admin Name*, *Admin IP*, *ILOM Name*, *ILOM IP* and *System Type* fields.
 - ? Agent only nodes
To add an agent only node, complete the *Admin Name*, *Admin IP* and *System Type* fields.
 - ? InfiniBand switches

To add an InfiniBand switch, complete the *Admin Name*, *Admin IP* and *System Type* fields.

- 7 Power Distribution Unit (PDU)

To add a PDU, complete the *Admin Name*, *Admin IP* and *System Type* fields.

- 7 Cisco switch

To add a Cisco switch, complete the *Admin Name*, *Admin IP* and *System Type* fields.

11. Click Next.

The Check Network Connectivity page appears.

- 12.** Review the connectivity checks (Netcheck) back to the Gateway for all of the targets uploaded through the schematic file. Expand the type sections, such as ZFS Storage or Compute Nodes, to review the details.

Note: If any mandatory test fails, it is not possible to proceed to the next stage of adding the Engineered System.

A typical message advises that “Mandatory tests failed and must be resolved to continue. Please check [Oracle Advanced Support Gateway Security Guide](#)”.

Note: If any non-mandatory test fails, you should review the warning message and take appropriate action before proceeding to the next stage of adding the Engineered System.

- a. (Optional) Click **Back** to revise the system details.
- b. (Optional) Click **Retest** to run the connectivity tests again.
- c. Click **Next**.

The Set Credentials page appears.

- 13.** Supply user credentials for each target to perform validation.

For database servers:

- a. (Optional) In the **Credentials** field, select the **Same for All** check box to apply the credentials to all servers of the same type (database servers).
- b. In the **Host Username** field, enter the name of the system.
- c. In the **Host Password** field, enter the password associated with the system.
(Optional) Toggle the eye icon to view or hide the details.
- d. In the **Priv Mode** field, select the mode to be used to gain the required root level privilege on the system. The options are **sudo**, **su**, and **pfexec**.
- e. In the **Root Password** field, enter the root password associated with the system.
(Optional) Toggle the eye icon to view or hide the details.
- f. In the **ILOM Username** field, enter the ILOM username.
- g. In the **ILOM Password** field, enter the password associated with the ILOM.
(Optional) Toggle the eye icon to view or hide the details.

For Exadata storage servers and ZFS storage arrays:

- a. (Optional) In the **Credentials** field, select the **Same for All** check box to apply the credentials to all servers of the same type (Exadata storage servers).
- b. The **Host Username** field contains the value, *root*. This field cannot be edited.
- c. In the **Host Password** field, enter the root password.

(Optional) Toggle the eye icon to view or hide the details.

- d. In the **ILOM Username** field, enter the ILOM username.
- e. In the **ILOM Password** field, enter the password associated with the ILOM.

(Optional) Toggle the eye icon to view or hide the details.

- f. Click **Validate**.

A warning popup appears: supplying incorrect passwords may result in being locked out of your account.

- g. Click **Continue**.

The validation check is run and a message appears, stating that the credentials have been validated.

- h. Click **Next**.

The Check Network Connectivity page appears.

14. To check end-to-end connectivity:

- a. All network connections (that is, *to* or *from* the Gateway to the device) are checked.

If a connection is not made, then a status of *Failed* is displayed.

Reconfigure the failing connection and validate it before continuing. When all connectivity passes, continue to the next step.

- b. Click **Next**.

The Compliance Check page appears.

15. To enable Oracle to validate system compliance and network connections:

- a. Click **Start**.

A progress bar measures the rate of system validation. When it reaches 100%, system status displays as complete and a message appears stating that the compliance check passed successfully.

- b. Click **Next**.

A warning message appears stating that the compliance check is successful, and asking whether you would like to proceed.

- c. Click **Yes**.

The Submit Provisioning Request to Oracle page appears.

16. Click **Submit Details to Oracle**.

System prechecks have been completed, and a provisioning request is submitted to Oracle.

The System Install Successful page appears.

17. A service activation request summary is sent to the customer contact by email.

18. At this point, you can perform one of the following actions:

- Select **Continue to Add new System** to install a monitoring agent on a standalone host or to create a request for the monitoring of an Oracle Engineered System.
- Select **Continue to Systems** to revert to the Systems and Hosts page.
- Select **Exit** to revert to the Systems and Hosts page.

Viewing Target Configurations

This section provides information about viewing configuration details about discovered systems and hosts, for example: status, last backup time, lifecycle type, supported services, open SRs, health report details, and so on.

To use Oracle Advanced Support Gateway to manage discovered systems and hosts:

1. Log in to Oracle Advanced Support Gateway.

The Oracle Advanced Support Gateway Home page appears.

2. From the **Admin** menu, click **Manage Systems**.

The Systems and Hosts page appears.

Figure 5–14 Viewing Systems and Hosts

Name	Type	Lifecycle	Monitoring Level	Status	Services	Configuration	Installation	Actions
DB Machine aeldb1.acs.oracle.com_gw189195 (7)	Oracle Database Machine	N/A	N/A	Unreachable	N/A	N/A	Installed	View Details
ZDLRA Hardware zdlisc.in.oracle.com_gw189195	Oracle Database Machine	N/A	N/A	Down	3	Needs Review	Installed	View Details
exadata-test-2(100201)	Exadata	N/A	N/A	Pending	N/A	N/A	Draft	View Details

You use this page to manage existing systems and hosts.

3. Click any listed target.

The target configuration appears.

You can use this page to view the target configuration and to manage the target details.

This section contains the following topics:

- ? [Viewing Target Details](#)
- ? [Viewing Statistics](#)
- ? [Viewing Service Requests](#)
- ? [Viewing Recommendations](#)

Viewing Target Details

The Target Details landing page offers a consolidated view of target information that is important to the customer. You can review key performance and SR information about the target in a series of intuitive, graphical displays.

Among the details provided are:

- ? **Status:** Uses icons to indicate that the target is in one of the following states:
 - ? *Up:* The target is active and reachable
 - ? *Pending:* The target is not active, and the target details cannot yet be displayed on the Oracle Advanced Support Gateway user interface
 - ? *Unreachable:* The target was formerly active, but is now unreachable
- ? **Last Backup:** Provides a timestamp of the last database backup.

- ⌵ **Up Time:** Provides the duration of database machine uptime.
- ⌵ **Lifecycle:** Provides the lifecycle associated with the database. The options are *Test*, *Production*, *Development*, *Stage*.
- ⌵ **Services:** Provides a list of supported Oracle connected services. Examples might include: Oracle Platinum Services, Business Critical Support, and Advanced Monitoring and Resolution.

Note: Where more than one instance of a particular service runs on a target, each instance is differentiated by a specific identifier, for example, *Oracle Platinum Service (ID: 100080)*.

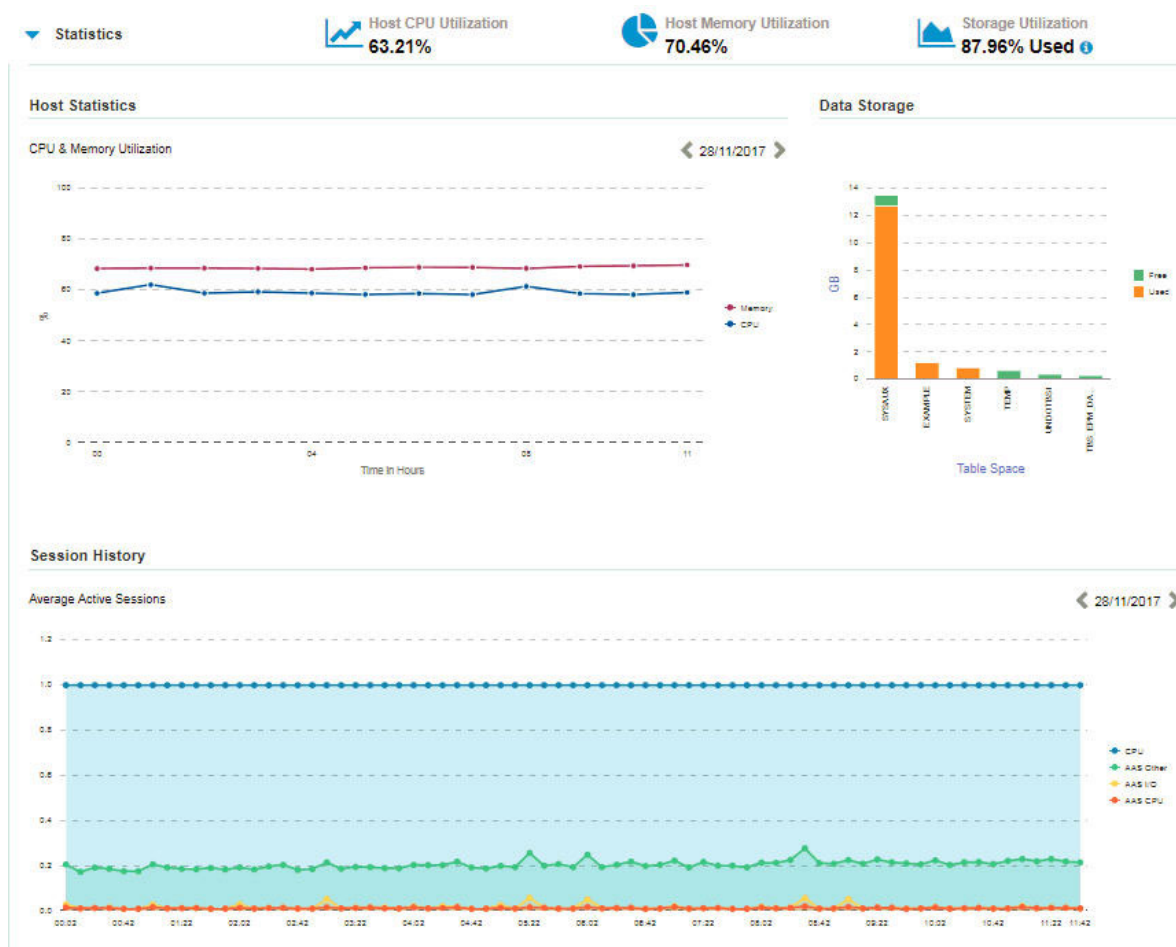
Viewing Statistics

You can expand the Statistics window to review and track CPU, memory, and storage utilization values for the chosen host. See [Figure 5–15](#).

Use the arrows beside the date value to select the required date.

Hover the cursor over the graphs to review further details about the host series CPU group, the host series memory group, and the exact utilization percentages.

Figure 5–15 Viewing the Statistics Details



Viewing Service Requests

See ["Viewing Service Requests"](#).

Viewing Recommendations

Recommendations are made following a review by an Oracle engineer of a current customer scenario or engagement.

Note: Recommendations apply only to certain, paid, customer engagements, services, and scenarios.

A typical scenario might involve a customer engaging Oracle for a paid performance review, for example, of a number of database instances. The engineer investigates the system and issues a set of results and a series of recommendations.

You can expand the Recommendations window to review:

- *Findings:* The results of the review of the system or host by an Oracle engineer. For example, CPU usage was consistently high and was a bottleneck;
- *Recommendations:* The solution proposed by an Oracle engineer to any issues in the findings; for example, in response to the high CPU usage, the recommendation is to add another CPU.

Figure 5–16 Viewing Recommendations

Recommendation	Database Instance	Assessment	Impact	Severity	Category	Status
Rec 1	All Instances	Paul H	Medium	Info	DB Time > CPU Time Analysis	In Progress

Displaying 1 - 1 (of 1)

Managing System Passwords

You can manage the passwords associated with the discovered systems and hosts.

1. Log in to Oracle Advanced Support Gateway.

The Oracle Advanced Support Gateway Home page appears.

2. From the **Admin** menu, click **Manage Systems**.

The Systems and Hosts page appears.

3. Click **Manage Passwords**.

The Password Management appears. Periodic rotation of passwords for production systems is recommended. Use this page to update stored passwords in Oracle Password Vault.

Refer to the following topic:

- ["Managing Credentials and Passwords."](#)

Deactivating Services

You can use Oracle Advanced Support Gateway to deactivate an Engineered System, that is, to stop monitoring of, for example, an Oracle Exadata Database Machine (Exadata), or Oracle Database Machine.

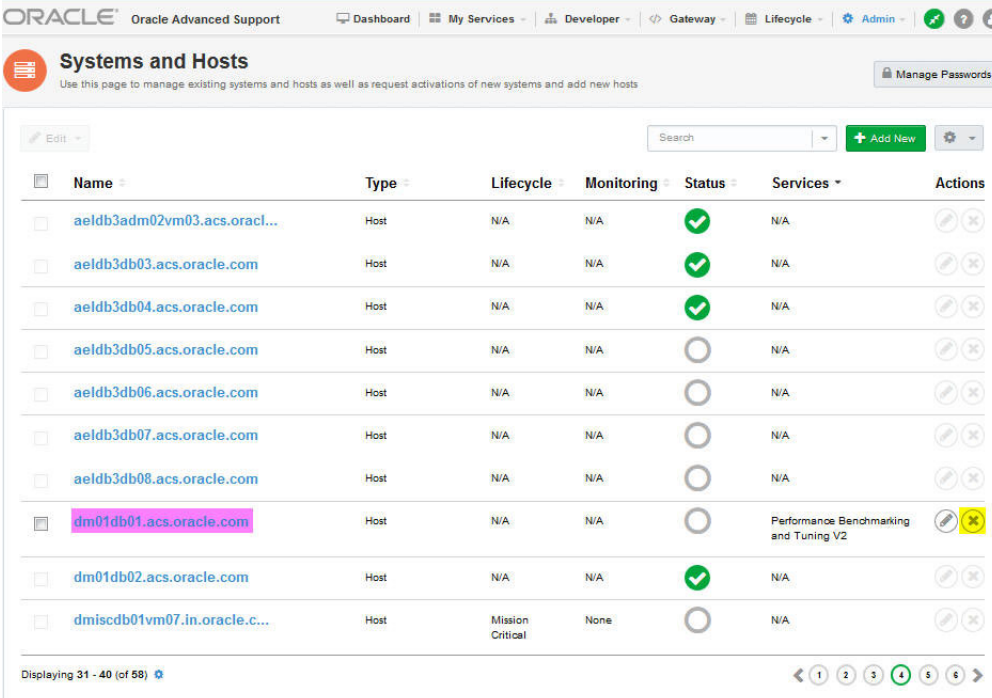
You can only deactivate a service on a target (system or host) on which services are running.

To deactivate an Engineered System:

1. From the Systems and Hosts page, select a target on which a service is running.

In the example shown in [Figure 5–17](#), the *dm01db01.acs.oracle.com* host is selected for deactivation.

Figure 5–17 Systems and Hosts Page



Name	Type	Lifecycle	Monitoring	Status	Services	Actions
aeldb3adm02vm03.acs.oracle.com	Host	N/A	N/A	✓	N/A	[Edit] [X]
aeldb3db03.acs.oracle.com	Host	N/A	N/A	✓	N/A	[Edit] [X]
aeldb3db04.acs.oracle.com	Host	N/A	N/A	✓	N/A	[Edit] [X]
aeldb3db05.acs.oracle.com	Host	N/A	N/A	○	N/A	[Edit] [X]
aeldb3db06.acs.oracle.com	Host	N/A	N/A	○	N/A	[Edit] [X]
aeldb3db07.acs.oracle.com	Host	N/A	N/A	○	N/A	[Edit] [X]
aeldb3db08.acs.oracle.com	Host	N/A	N/A	○	N/A	[Edit] [X]
dm01db01.acs.oracle.com	Host	N/A	N/A	○	Performance Benchmarking and Tuning V2	[Edit] [X]
dm01db02.acs.oracle.com	Host	N/A	N/A	✓	N/A	[Edit] [X]
dmiscdb01vm07.in.oracle.com	Host	Mission Critical	None	○	N/A	[Edit] [X]

Displaying 31 - 40 (of 58)

2. From the **Actions** column, click the **Deactivate (X)** icon, as highlighted.

A warning dialog asks you to confirm deactivation.

Click **Yes** to confirm. The host is deactivated.

Activating Services

This chapter provides information about using Oracle Advanced Support Gateway to activate services.

This chapter consists of the following sections:

- ? [About Activating Services](#)
- ? [Selecting a Service for Activation](#)
- ? [Viewing Discovered Databases](#)
- ? [Deactivating Services](#)

About Activating Services

Service activation is the process by which an Oracle Service is enabled and configured on your targets. Once agents are installed on your host systems, they will automatically discover any new software targets like databases or Automatic Storage Managements, (ASMs) which are installed on these hosts.

In order to activate a service, you first need to select a service for which service activation is to be performed. The list of available services displayed for service activation is based on the contract which you have with Oracle for the services on the gateway.

So, for example, to activate the Oracle Platinum service, you can first select Platinum for activation, and then use the Oracle Advanced Support Gateway user interface to select databases from the list of automatically discovered database targets. Databases can be added singly or in groups. After selecting the required databases, you need to enter the database credentials required to enable monitoring prior to service activation. The term *database* can refer to single instances of databases as well as High Availability databases, Clusters, ASM Clusters, and Grids. The activation method, as well as the corresponding wizard steps, varies according to selected targets.

The next activation step for Platinum is that Oracle Advanced Support Gateway enables the delivery and validation of all required database implementation information using the Gateway user interface. These collection and validation steps then enable an Oracle engineer to prepare the system and make it ready for activation.

The database activation workflow consists of three principal stages:

- ? Selecting available databases to activate
- ? Supplying and testing database credentials
- ? Activating the databases for your selected service

Selecting a Service for Activation

To use Oracle Advanced Support Gateway to activate a service:

1. Log in to Oracle Advanced Support Gateway.

The Oracle Advanced Support Gateway Home page appears.

2. From the **My Services** menu, click **Activate Service**.

The Welcome Message page appears.

Review this page to ensure that you have the following information:

- ⌘ *asmsnmp* credentials for ASM instances that have not yet been promoted
- ⌘ *dbsnmp* credentials for databases that have not yet been promoted

Note: For security reasons, Oracle does not store passwords.

3. Click **Get Started**.

The Service Activation: Select Service page appears.

You use this page to select the service you wish to activate.

4. (Optional) You can also activate services from the Manage Databases page that is used to manage all databases and their related cluster and ASM infrastructure.

To view the Manage Databases page, select **Admin**, then **Manage Databases**, and click **Activate New Service**.

5. Complete the following fields:

- ⌘ From the **Select Service** field, select your required service, for example, *Platinum (ID: XXXXXX)*.

The list displayed for service activation is based on the contract which the customer has for supported services on the gateway.

- ⌘ From the **Activation** field, select whether to promote the target and activate the service using the wizard, or just promote the target (and activate the service later.)

a. Activate; activate service with promotion, *or*

b. Promote; promote targets without service activation

If you select (a), continue to step 6.

If you select (b), continue to step 16.

- ⌘ In the **Username** field, enter the Oracle Single Sign-On (SSO) username of the My Oracle Support (MOS) account associated with the CSI (Customer Support Identifier) shown in the previous field.

- ⌘ In the **Password** field, enter the Oracle Single Sign-On (SSO) password of the My Oracle Support (MOS) account associated with the CSI (Customer Support Identifier) shown in the previous field.

6. (Optional: If you choose to activate targets with promotion) Add one or more database targets for service activation. Activation of a service on targets which are not eligible for activation is prohibited, and the reason these targets are not eligible is displayed, for example, *Cluster not ready* or *Cluster already activated for different instance of same service*.

To add a database:

- a.** Select the check box associated with the database.

(To add multiple databases, select all associated check boxes.)

Note: If the database to be activated is not on the list, contact Oracle to complete the manual installation of the agent and perform a discovery. To request Oracle discoveries, contact My Oracle Support (MOS).

b. Click Next

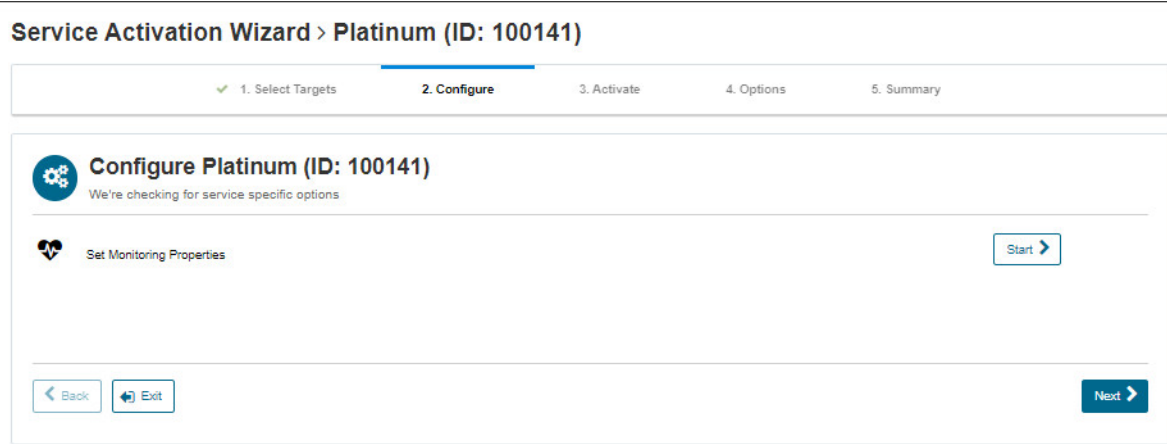
The Service Activation: Database/Grid/ASM page appears. The selected databases are displayed.

c. Click Validate & Next.

Note: In the case of grids, ASM clusters, database clusters, and so on, you are required to validate on multiple pages.

The Service Activation: Configure page appears. This page enables you to specify service-specific options.

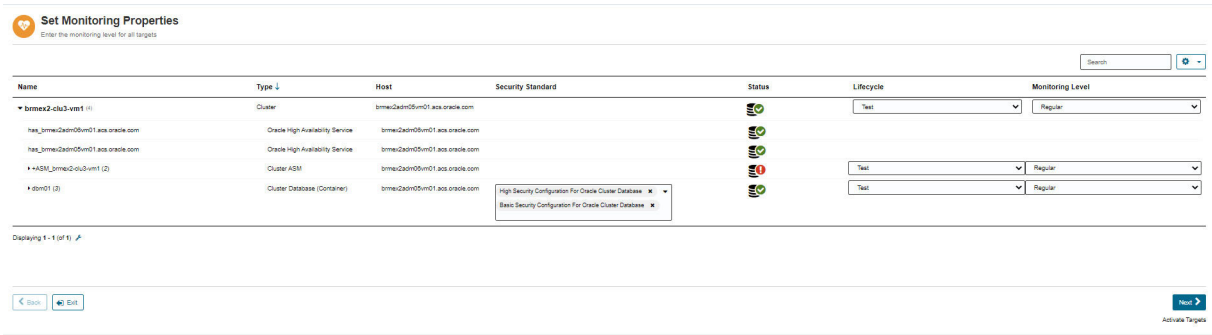
Figure 6–1 Supplying Database Options



7. Click Next to set the monitoring properties.

The Set Monitoring Properties page appears.

Figure 6–2 Setting Monitoring Properties



8. Supply the credentials for each database:

- a. In the Lifecycle field, select the lifecycle associated with the database. The options include Test, Production, Stage, or Development.**

- b. In the **Monitoring Level** field, select the monitoring level associated with the database. Monitoring levels are restricted to valid monitoring levels for the target, for example, *None*, *Low*, *Regular*, *High*, or *Intensive*.
- c. (Optional; depending on the target type) In the **DBSNMP** field, enter the SNMP password associated with the database.
- d. (Optional; depending on the target type) In the **ASMSNMP Password** field, enter the Automatic Storage Management (ASM) SNMP password associated with the database.
- e. (Optional) You can copy credentials from row to row by clicking the arrows icon in the **Actions** section of the page.

Note: Users are notified if a credential has already been entered for a particular target.

9. Click **Next**.

The Service Activation: Review page appears.

Figure 6–3 Reviewing Activation Options

Targets are ready for service activation
Review before activation begins. Once activation begins, this cannot be reversed.

Platinum (ID: 100141)

0 ACTIVATED 0 FAILED 6 WAITING

STARTED: 06-16-2023 10:10:44
DURATION: [icon]

Additional Details: Monitoring Properties, Levels Set

Name	Type	Host	Status	Activated
lrmex2-cls3-vml	Cluster	lrmex2ap05m01.sas.oracle.com	[icon]	[icon]

Displaying 1 - 1 (of 1)

Back Edit Complete Later Activate Service

Select whether to use the activation wizard to activate the service now, or postpone completion:

- a. **Activate Service**, or
- b. **Complete Later**

If you select (a), continue to step 10.

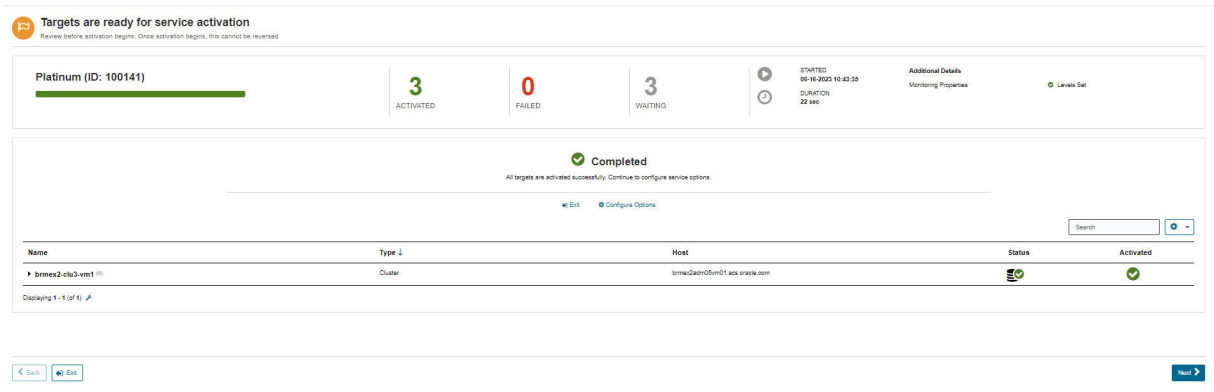
If you select (b), continue to ["Viewing Discovered Databases"](#).

10. Click **Activate Service**.

After activating the service, tests are triggered for all untested databases. This may take a few minutes.

Results are displayed at the top of the page. See [Figure 6–4](#).

Figure 6–4 Reviewing Service Activation Options



Review the progress check.

- a. The **Activated** field displays the number of databases that were successfully activated.
 - b. The **Failed** field displays the number of databases that were not successfully activated.
 - c. The **Waiting** field displays the number of databases pending completion of the activation process.
 - d. The **Started** field displays the time at which activation commenced.
 - e. The **Duration** field displays the time taken for activation.
 - f. The **Additional Details** field displays whether monitoring levels are set.
 - g. (Optional) If activation is successful, click **Continue to Service** to display the new service.
11. Click **Next** to configure options to include on the activated hosts. These options are:
- ⌵ **Validate Monitoring Configuration:** to validate, you will need to provide privileged credentials for each host;
 - ⌵ **Install/Update Trace File Analyzer (TFA):** To install, you will need to provide privileged credentials for each host.

Each configuration option follows the same pattern.

The Select Options to Configure page appears.

Figure 6–5 Selecting Options to Configure



12. Click **Selected**.

Note: The option to install Trace File Analyzer (TFA) is no longer supported. Consequently, the Validating Monitoring Configuration is the only option supported in this release.

The Select Hosts page appears.

Figure 6–6 Selecting Hosts

13. Select the hosts where you would like to install options by choosing one of the following:

- ? **All Hosts**, which is the standard installation option, *or*
- ? **Specific Hosts**, which enables you to customize installation options

14. Click **Next**.

The Enter Credentials page appears.

Figure 6–7 Entering Credentials for the Selected Hosts

Host Name	Privilege	Username	Password	Status	Action
acslogicextrnl.acs.oracle.com	sudo			Refresh	Edit

Create or update credentials for the following hosts to run diagnostics. Enter root credentials or a user that has sudo privileges:

- a. In the **Privilege** field, select the mode to be used to gain the required level privilege on the host. The options are **sudo**, **Normal**, and **None**.
- b. In the **Username** field, enter the password associated with the host.
- c. In the **Password** field, enter the password associated with the host.

15. Click **Next**.

The Summary page appears. Review the activation details.

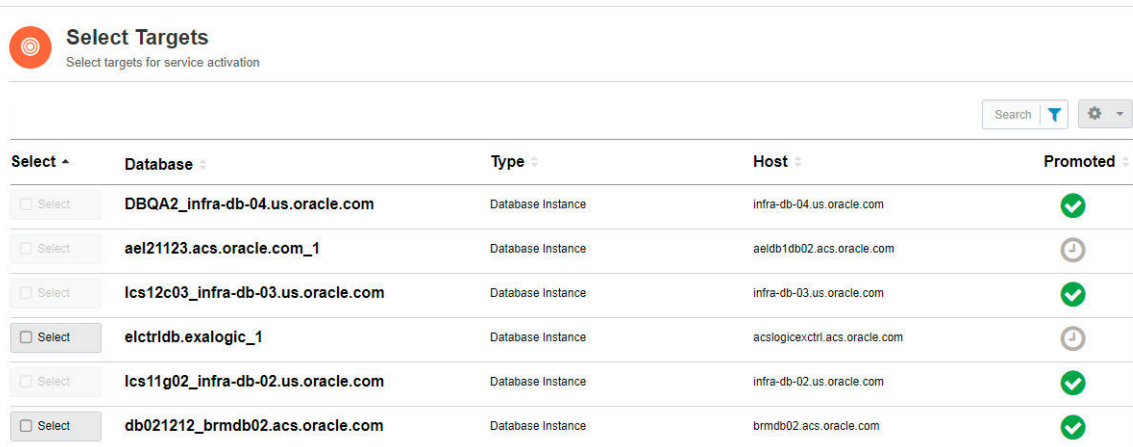
16. (Optional: If you choose to promote targets without service activation)

Select **Promote; promote targets without service activation**.

Click **Next**.

The Service Promotion: Targets page appears.

Figure 6–8 Selecting Service Promotion Targets



Select Targets
Select targets for service activation

Search [] [] []

Select	Database	Type	Host	Promoted
<input type="checkbox"/>	DBQA2_infra-db-04.us.oracle.com	Database Instance	infra-db-04.us.oracle.com	<input checked="" type="checkbox"/>
<input type="checkbox"/>	acl21123.acs.oracle.com_1	Database Instance	acldb1db02.acs.oracle.com	<input type="checkbox"/>
<input type="checkbox"/>	lcs12c03_infra-db-03.us.oracle.com	Database Instance	infra-db-03.us.oracle.com	<input checked="" type="checkbox"/>
<input type="checkbox"/>	elctrdb.exalogic_1	Database Instance	acslogicexctrl.acs.oracle.com	<input type="checkbox"/>
<input type="checkbox"/>	lcs11g02_infra-db-02.us.oracle.com	Database Instance	infra-db-02.us.oracle.com	<input checked="" type="checkbox"/>
<input type="checkbox"/>	db021212_brmdb02.acs.oracle.com	Database Instance	brmdb02.acs.oracle.com	<input checked="" type="checkbox"/>

17. Add one or more database targets for service promotion.

To add a database:

- a. Select the check box associated with the database.

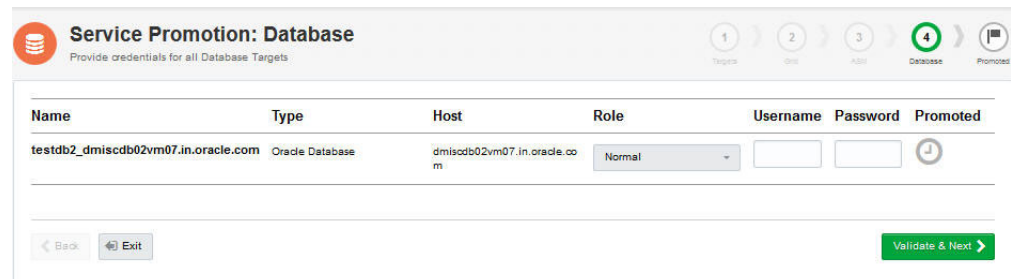
(To add multiple databases, select all associated check boxes.)

Note: If the database you need to activate is not on the list, you need to contact Oracle to complete the manual installation of the agent and perform a discovery. To request Oracle discoveries, contact My Oracle Support (MOS).

- b. Click **Next**.

The Service Promotion: Databases page appears.

Figure 6–9 Providing Credentials for Service Promotion Targets



Service Promotion: Database
Provide credentials for all Database Targets

1 2 3 4 5
Targets DB Host Database Promoted

Name	Type	Host	Role	Username	Password	Promoted
testdb2_dmisdb02vm07.in.oracle.com	Oracle Database	dmisdb02vm07.in.oracle.com	Normal			<input type="checkbox"/>

Back Exit Validate & Next

You use this page to provide credentials for all database targets:

In the **Role** field, select the role associated with the database. The options are *Normal* or *SYSDBA*.

In the **Username** field, enter the username associated with the database.

In the **Password** field, enter the password associated with the database.

c. Click **Validate & Next**.

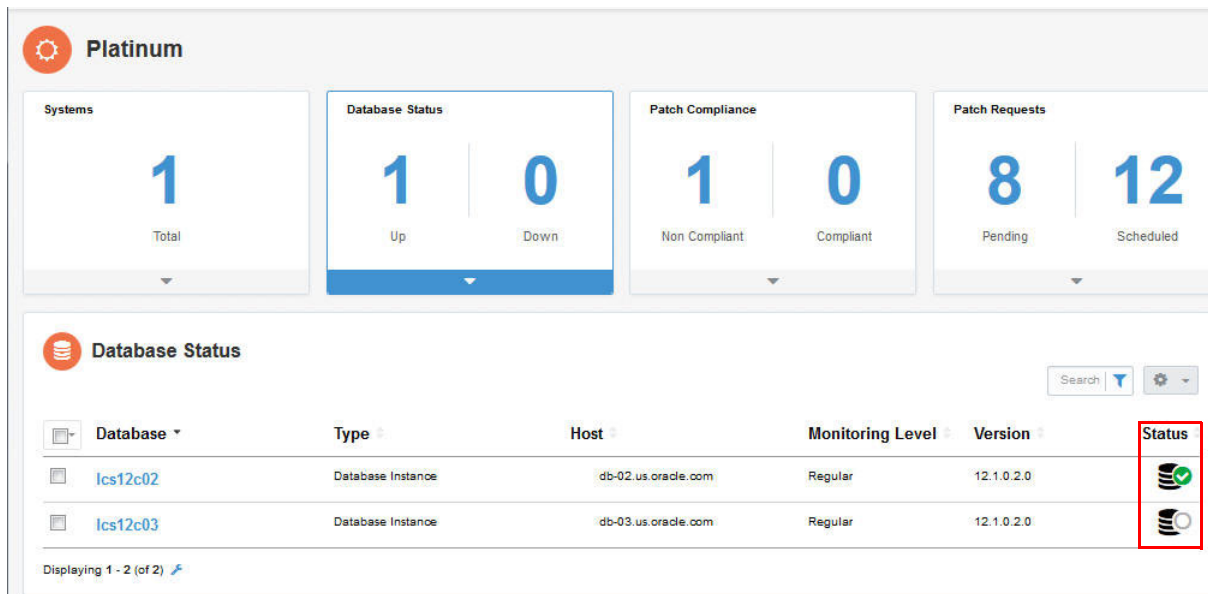
The Service Activation: Promoted page appears. Use this page to specify service-specific options.

Viewing Discovered Databases

This section provides information about viewing discovered databases.

Select the **Database Status** badge to display your discovered databases in the Database Status list.

Figure 6–10 *Displaying Discovered Databases*



As highlighted in the Status column in the example in [Figure 6–10](#), the database *lcs12c02* is up, denoted by the check mark on its database icon, while *lcs12c03* is unreachable, denoted by the gray circle.

Once the databases are activated, monitoring commences.

Deactivating Services

You can use Oracle Advanced Support Gateway to deactivate a service, that is, to deactivate the targets on which the service is running.

Note: Oracle recommends that Platinum Service customers first refer to their Oracle representative before deactivating a service on an Engineered System. When a service is deactivated, the databases remain in the list of managed databases, but no longer have a service associated with them. To formally remove a database from the list of managed databases, please refer to your Platinum Infrastructure Team representative.

To deactivate a service:

1. Log on to Oracle Advanced Support Gateway.

The Oracle Advanced Support Gateway Home page appears.

2. From the **My Services** menu, click **Deactivate Service**.

The Deactivate Service: Select Service page appears.

You use this page to select the service you wish to activate.

3. Select the service you want to deactivate (services must be selected singly.)

4. Click **Next**.

The Select Targets page appears.

5. Select the check box associated with the database.

(To add multiple databases, select all associated check boxes.)

6. Click **Next**.

The Service Deactivation page appears.

You use this page to review targets for service deactivation.

7. Select **Start Deactivation**.

A warning dialog asks you to confirm deactivation.

Click **Yes** to confirm. The database is deactivated.

Validating Connections

This chapter provides information about using the Connectivity Tests (Netcheck) to validate whether the required firewall ports and connections between Oracle Advanced Support Gateway and the Oracle database, Engineered System, ILOM or individual component, such as cell node or InfiniBand, are open.

This chapter consists of the following sections:

- ? [About Gateway Connectivity](#)
- ? [About System Tests](#)
- ? [Viewing System Test Status](#)
- ? [Verifying the External Connection](#)
- ? [Verifying an Internal Connection](#)
- ? [Verifying an ILOM Connection](#)
- ? [Configuring New System Test Targets](#)

About Gateway Connectivity

In order for Oracle to deliver Oracle Connected Services, the following requirements need to be met:

- ? All monitored devices must be network accessible from the Gateway.
- ? Oracle must have the level of access to the monitored devices necessary for Oracle to implement and deliver the service.
- ? The Gateway must be continuously accessible from Oracle Advanced Support Platform using the secure protocols.

The Netcheck feature provides a mechanism to test connectivity between the Gateway and the Oracle Advanced Support Platform and also between the Gateway and the customer monitored systems.

Connectivity tests are used to validate the ports and connections between the Gateway and the following Oracle Engineered Systems:

- ? Exadata
- ? Exalogic
- ? SuperCluster

Connectivity tests are also used to validate self-monitoring by connection to the ILOM on the Gateway.

These tests help to secure and successfully complete the implementation of services running on the Gateway.

Related Information

[Verifying the External Connection](#)

[Verifying an Internal Connection](#)

[Verifying an ILOM Connection](#)

About System Tests

You can use the Gateway to run three separate types of connectivity system test:

- ? Internal system tests. See "[About Internal System Tests.](#)"
- ? External system tests. See "[About External System Tests.](#)"
- ? ILOM test. See "[About ILOM Tests.](#)"

About Internal System Tests

An internal system test verifies the connectivity between the Gateway and the Oracle Engineered System. You can optionally specify a HTTP proxy if the traffic between the Gateway and the Engineered System is routed through a proxy server (depending on the customer's network configuration).

You can also verify the network traffic between the Gateway and the Engineered System in both directions, that is, from the Gateway to the Engineered System, and from the Engineered System to the Gateway. This test typically requires the root password for the system. The connectivity test requires the same root account to work on all of the target systems. After supplying the system details, you select the applicable *databasemachine.csv* file.

Related Information

[Verifying an Internal Connection](#)

About External System Tests

An external system test verifies the connectivity between the Gateway and Oracle (VPN, Monitoring, CCR, and Oracle patch accessibility).

Related Information

[Verifying the External Connection](#)

About ILOM Tests

The ILOM system test verifies the connectivity between the Gateway and its ILOM. The test is performed using HTTPS, SNMP, TCP and other protocols.

Related Information

[Verifying an ILOM Connection](#)

Viewing System Test Status

To use Oracle Advanced Support Gateway to view system test status:

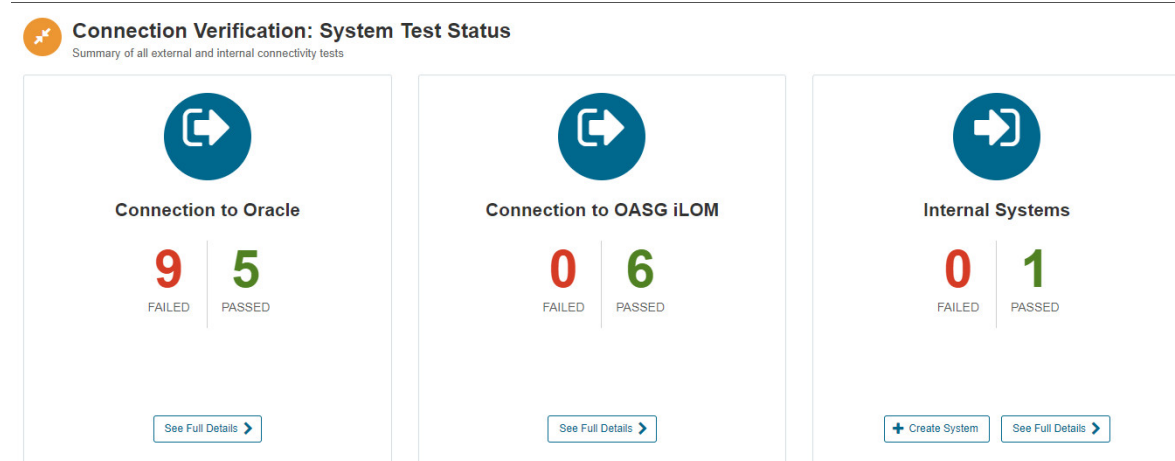
1. Log in to Oracle Advanced Support Gateway.

The Oracle Advanced Support Gateway Home page appears.

2. From the **Gateway** menu, select **Connectivity Tests**.

The Connection Verification: System Test Status page appears.

Figure 7–1 Connection Verification: System Test Status



This page provides a summary of all external (that is, connections to Oracle) and internal connectivity tests. From this page, you can perform a number of actions:

- Verify the external connection between the Gateway and Oracle. See ["Verifying the External Connection."](#)
- Verify a connection between the Gateway and its ILOM. See ["Verifying an ILOM Connection."](#)
- Verify an internal connection between the Gateway and the Engineered System. See ["Verifying an Internal Connection."](#)
- View a detailed table of internal connectivity tests. See ["Verifying an Internal Connection."](#)

Verifying the External Connection

The external connections between the Gateway and Oracle are established during Gateway installation. You can continue to monitor connectivity as required.

To use the Gateway to verify connectivity between the Gateway and Oracle:

1. Log in to the Gateway.

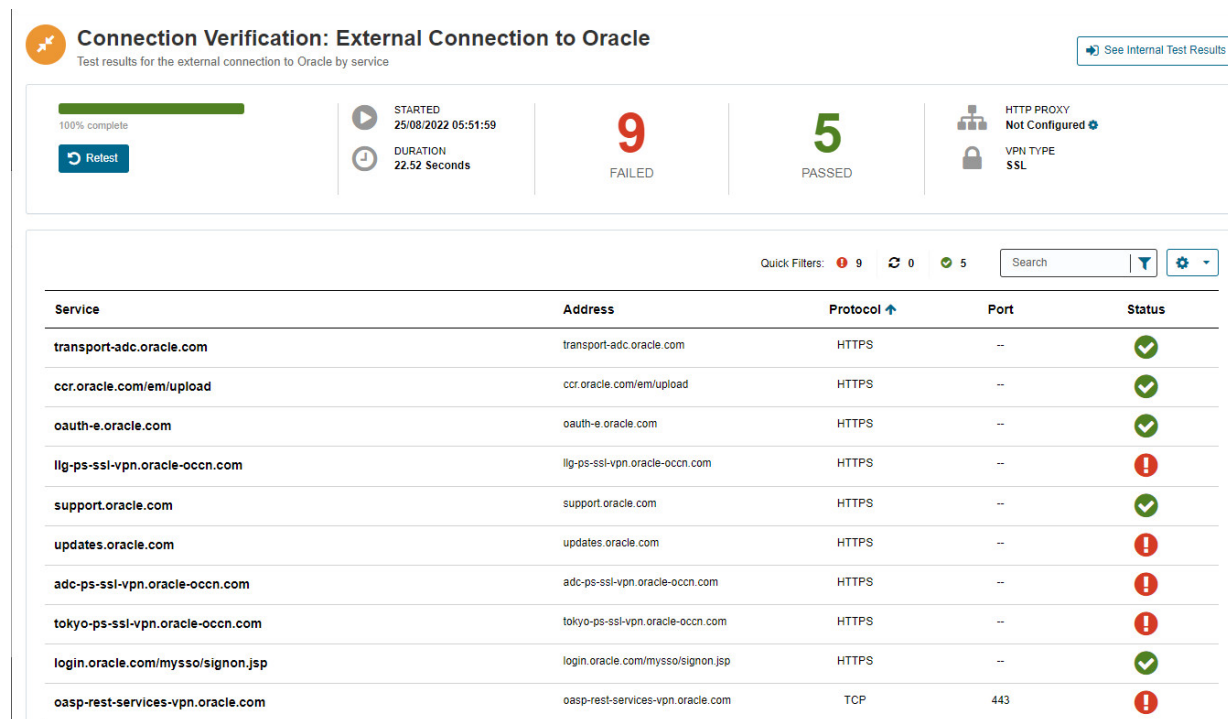
The the Gateway Home page appears.

2. From the **Gateway** menu, select **Connectivity Tests**.

The Connection Verification: System Test Status page appears.

3. From the Connection to Oracle panel, click **See Full Details**.

The Connection Verification: External Connection to Oracle page appears.

Figure 7–2 Connection Verification: External Connection to Oracle

This page displays test results for the external connection to Oracle by service. As shown in [Figure 7–2](#), five of the supported service connections are up.

4. Click **Retest** to verify the connection to Oracle.

If the connection is validated, a success message appears.

Specifying a HTTP Proxy

You can optionally specify a HTTP proxy if the traffic between the Gateway and Oracle is routed through a proxy server (depending on the customer's network configuration).

To configure a HTTP proxy:

1. Log in to the Gateway.
The Oracle Advanced Support Gateway Home page appears.
2. From the **Gateway** menu, select **Connectivity Tests**.
The Connection Verification: System Test Status page appears.
3. From the Connection to Oracle panel, click **See Full Details**.
The Connection Verification: External Connection to Oracle page appears.
4. In the top right of the page, in the HTTP Proxy section, click **Configure**.
The HTTP Proxy Settings page appears.

Figure 7–3 HTTP Proxy Settings

HTTP Proxy Settings
Configure HTTP Proxy Settings

HTTP Proxy Mode ☒ Proxy ?

IP Address * ?

Port * ?

Authentication ☒ Authentication ?

Proxy Username * ?

Proxy Password * ?

Global Proxy ☐ Overwrite Global Proxy ?

5. Complete the following parameters on the HTTP Proxy server if http-proxy is required for outbound communication.
 - a. (Optional) If HTTP Proxy mode is required, select the **Proxy** check-box.
 - b. In the **IP Address** field, enter your customer IP address.
You can use the hostname or fully-qualified domain name (FQDN) as Oracle Advanced Support Gateway is configured to use Domain Name Service (DNS.)
 - c. In the **Port** field, enter the port associated with the HTTP proxy server.
 - d. (Optional) If authentication is required for the HTTP proxy server, select the **Authentication** check-box, and then enter the proxy username and password.
 - e. (Optional) If you want to overwrite the global proxy mode, select the **Overwrite Global Proxy** check-box.
 - f. Click **Save** to complete the HTTP proxy configuration.

Verifying an Internal Connection

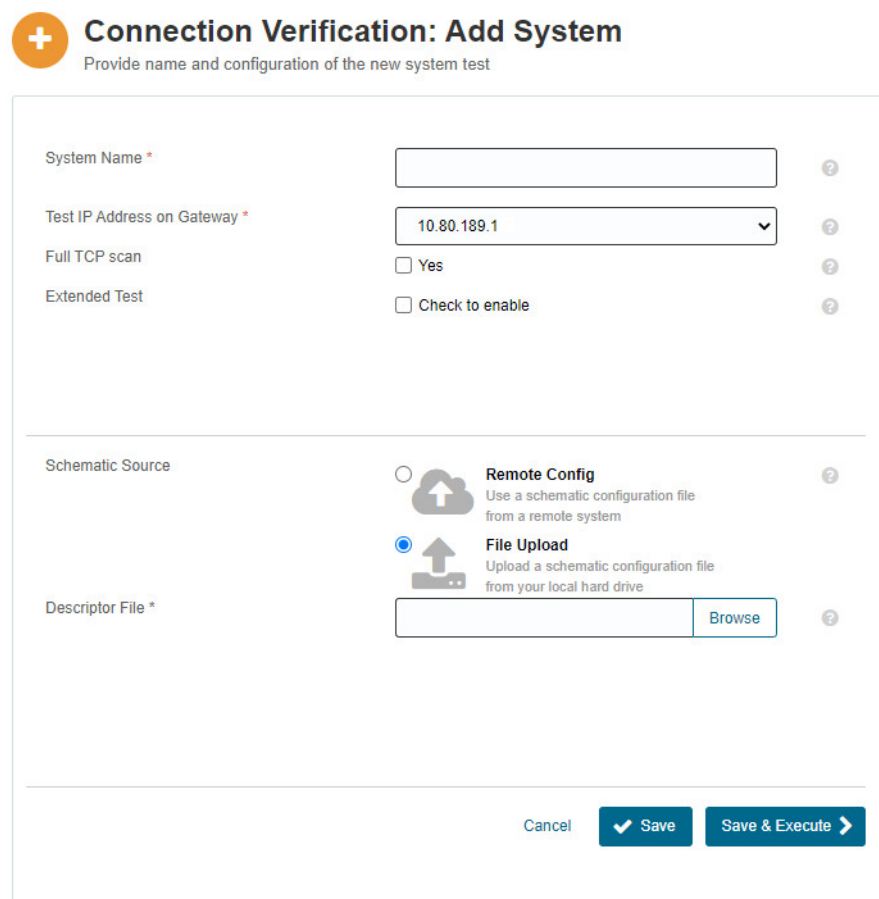
External connections verify the connectivity between the Oracle Advanced Support Gateway and an Engineered System.

To use Oracle Advanced Support Gateway to verify connectivity between Oracle Advanced Support Gateway and an Engineered System:

1. Log in to Oracle Advanced Support Gateway.
The Oracle Advanced Support Gateway Home page appears.
2. From the **Gateway** menu, select **Connectivity Tests**.
The Connection Verification: System Test Status page appears.
3. From the Internal Systems panel, click **Create System**.
The Connection Verification: Add System page appears.

A sample configuration is provided in [Figure 7-4](#).

Figure 7-4 Connection Verification: Add System



Connection Verification: Add System
Provide name and configuration of the new system test

System Name * ?

Test IP Address on Gateway * ?

Full TCP scan ☐ Yes ?

Extended Test ☐ Check to enable ?

Schematic Source

☐ Remote Config ?
Use a schematic configuration file from a remote system

☒ File Upload ?
Upload a schematic configuration file from your local hard drive

Descriptor File * Browse ?

Cancel Save Save & Execute

4. Complete the following parameters to add a system.
 - a. In the **System Name** field, enter the name of the Engineered System.
 - b. In the **IP Address** field, enter the IP address of the Engineered System.
You can use the hostname or fully-qualified domain name (FQDN) as Oracle Advanced Support Gateway is configured to use Domain Name Service (DNS.)
 - c. (Optional) In the **Full TCP scan** field, if you require a full TCP scan of the target system to discover which TCP ports are open, select the **Yes** check-box.
 - d. (Optional) In the **Extended Test** field, if you require a test of the connection from the target system to Oracle Advanced Support Gateway *and* from Oracle Advanced Support Gateway back to the target system, select the **Check to Enable** check-box, and then enter the SSH username and password.
 - e. In the **Schematic Source** field, select a schematic source file from either a remote or a local source.
Select **Remote Config** to choose a schematic source file from a remote source.
Continue to step f.
Select **File Upload** to choose a schematic source file from a local source. Skip to step g.

f. (Remote Config only)

In the **HOST IP Address** field, enter the IP address of the remote source.

You can use the hostname or fully-qualified domain name (FQDN) as Oracle Advanced Support Gateway is configured to use Domain Name Service (DNS.)

In the **Schematic Directory** field, enter the path to the schematic directory.

In the **Filename** field, enter the name of the schematic source file.

In the **SSH Credentials for Remote Source File Transfer** section, enter the SSH username and password required for file transfer, or select the **Check to copy extended test SSH credentials** to automatically fill the SSH username and password fields using the input from the **Extended Test** field.

g. (File Upload only)

In the **Descriptor File** field, click **Browse** to navigate to the schematic source file on your local machine.

h. Click **Save and Execute to run the system test or click **Save** to save the test details for execution at a later point.**

After executing the test, it appears on the Connection Verification: Internal Systems page that shows all test results for the internal connections by system.

Figure 7–5 Connection Verification: Internal Systems

Service	Passed	Failed	Skipped	Started	Duration	Actions
Check-1	19	0	3	28/02/2022 08:40:16	5.10 sec	

Displaying 1 - 1 (of 1)

- Click the test name to list all components of the system test. This might include databases, cell nodes, InfiniBand switches, and so on.

Figure 7–6 Connection Verification: Internal Connection

Component	Type	Address	Protocol	Port	Direction	Status
shimasw-pdub0	PDU	192.0.2.0	PING	--	← Gateway	!
shimasw-pdub0	PDU	192.0.2.0	HTTP	--	← Gateway	!
shimasw-pdua0	PDU	192.0.2.0	PING	--	← Gateway	!
shimasw-pdua0	PDU	192.0.2.0	HTTP	--	← Gateway	!
ibb-cpima200	IB	192.0.2.0	TCP	22	← Gateway	!
ibb-cpima200	IB	192.0.2.0	TCP	6481	← Gateway	!
ibb-cpima200	IB	192.0.2.0	PING	--	← Gateway	!
ibb-cpima200	IB	192.0.2.0	HTTPS	--	← Gateway	!
ibs-cpima200	IB	192.0.2.0	PING	--	← Gateway	!
ibs-cpima200	IB	192.0.2.0	HTTPS	--	← Gateway	!

The Status column provides a visual indicator whether an individual component test passed or failed. The filters also provide a snapshot of successful, failed, skipped, or in progress tests.

The Direction column provides a visual indicator whether the connection is *to* or *from* the Gateway.

Oracle recommends that the network administrator should resolve any failed tests.

Click **Retest** to run the system test again.

Click **Back to Internal Test Results** to return to the Connection Verification: Internal Systems page.

Related Information

[About Gateway Connectivity](#)

[About System Tests](#)

Verifying an ILOM Connection

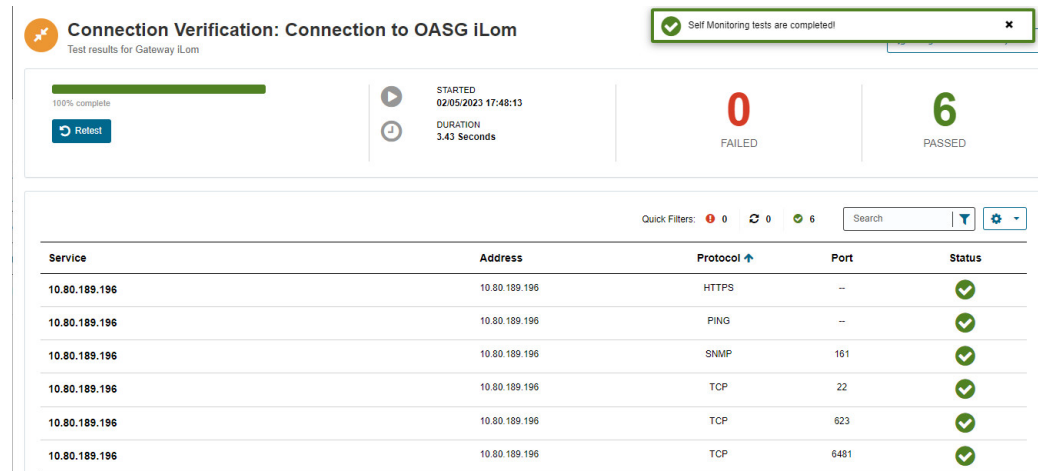
ILOM connections verify the connectivity between the Oracle Advanced Support Gateway and its constituent ILOM.

To use Oracle Advanced Support Gateway to verify connectivity between Oracle Advanced Support Gateway and an ILOM:

1. Log in to Oracle Advanced Support Gateway.
The Oracle Advanced Support Gateway Home page appears.
2. From the **Gateway** menu, select **Connectivity Tests**.
The Connection Verification: System Test Status page appears.
3. From the Connection to OASG iLOM panel, click **See Full Details**.
The Connection Verification: Connection to OASG iLOM page appears.

See [Figure 7–7](#).

Figure 7–7 Connection Verification: Connection to OASG iLom



- a. Click **Retest** to run the system test.

After executing the test, a message is displayed that “Self Monitoring tests are completed”. The Connection Verification: Connection to OASG iLom page shows all test results for the connections by protocol.

Related Information

[About Gateway Connectivity](#)

[About System Tests](#)

Configuring New System Test Targets

An Oracle engineer can map new targets for connectivity tests by customizing a mapping file.

The file, `netcheck_mappings.properties`, maps target types from the input file to targets in the `connections.tbl` file. The engineer must perform the following actions:

1. Add a key value pair per target. The key is the connectivity result value that the customer wants to display in the Connection Verification: Internal Systems page. The value is the new target type, for example: InfiniBand Switch, Cell Node, PDU.
2. Update the `connections.tbl` file to add the tests required for the new target type.

After the files have been modified and saved, the customer can start the connectivity test, select the new target type, and run tests for the target.

The contents of the `netcheck_mappings.properties` file are as follows:

```
IB=ib, Infiniband Switch, \.*Infiniband\.*Switch\.*, IBSwitch, oracle_ibswitch
DB=db, computenode, \.*DB\.*Node\.*, \.*Compute\.*Node\.*, Exadata OVS Compute Node, Exadata DB VM, host
CELL_NODE=cel, cellnode, \.*Cell\.*Node\.*, Exadata Cell Node, oracle_exadata
CISCO=cisco, \.*Cisco\.*Switch\.*, oracle_exa_cisco_switch
PDU=pdu, PDU, oracle_exa_pdu
KVM=kvm, oracle_exa_kvm
```

```
ZFS=zfs,StorageHead,\.*ZFS\.*Storage\.*  
ETHERNET_SWITCH=ethernet_switch  
ZFS_ORACLE_ENDPOINTS=zfs_oracle_endpoints[root@ct-testimadsi-59 setup]#
```

Managing Service Requests

This chapter provides information about using the Gateway to monitor and manage Service Requests (SRs).

This chapter consists of the following sections:

- [Viewing Service Requests](#)
- [Viewing Service Requests Associated with a Managed System](#)

Viewing Service Requests

After activating databases (see [Chapter 6, "Activating Services"](#)), you can view SRs associated with issues occurring on a monitored database instance or a RAC database.

To view service requests:

1. Log in to Oracle Advanced Support Gateway.

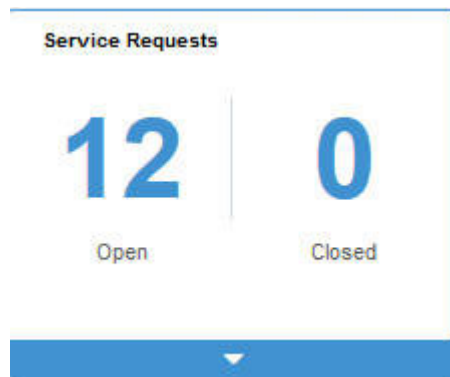
The Oracle Advanced Support Gateway Home page appears.

2. Select one of the following options:

- From the **My Services** menu, click the required service.

The service page displays information about the managed databases, including a **Service Requests** badge shown in [Figure 8–2](#).

Figure 8–1 *Selecting Service Requests*



Click the **Service Requests** badge to display a table of SRs as shown in [Figure 8–2](#).

Figure 8–2 Viewing Service Requests

My Services > Advanced Database Support > Service Requests

Service Requests

Search [] [Filter] [Settings]

SR # ^	Description ^	Target Name ^	Type ^	Host ^	Created On ^	Closed On ^	Duration ^	Status ^
3-16561232246	ORA 700 [TEST_SR-IGNORE-DO_NOT_CLOSE_I] more	E3DE0003	Database Instance	brmgsadb02	03/01/2018 22:39:04		466 Days	
3-16561731467	ORA 700 [TEST_SR-IGNORE-DO_NOT_CLOSE_I] more	E3DE0003	Database Instance	brmgsadb02	04/01/2018 00:20:59		466 Days	
3-16562132897	ORA 700 [TEST_SR-IGNORE-DO_NOT_CLOSE_I] more	E3DE0003	Database Instance	brmgsadb02	04/01/2018 01:20:59		466 Days	

Displaying 1 - 3 (of 3)

You can view both open and closed SRs.

The example in [Figure 8–2](#) shows open SRs associated with a monitored database. The SR listing provides a link to the SR in MOS, a description of the SR, outlines the target name, type, and host, and lists when the SR was created, when it was closed (not applicable in this case), how long it has been open for, its current status.

You can sort SRs by type, number, or status, for example. You can search for an SR using a keyword in the SR description, or by referencing the host name, for example.

You can use the Quick Filters to quickly assess the number of open and closed SRs associated with a particular target.

You can update an SR by clicking the link to the SR in the table. The SR opens in My Oracle Support.

Viewing Service Requests Associated with a Managed System

To view service requests associated with a particular managed system:

1. Log in to Oracle Advanced Support Gateway.

The Oracle Advanced Support Gateway Home page appears.

2. From the **Admin** menu, select **Service Requests**.

The Service Requests page appears as shown in [Figure 8–3](#).

Figure 8–3 Viewing Service Requests

The screenshot shows the Oracle Advanced Support Service Requests page. The page has a navigation bar with links to Dashboard, My Services, Gateway, and Admin. The main content area is titled 'Service Requests' and includes a summary of targets and service requests. Below this is a table of service requests.

SR #	SR Type	Status	Severity	Description	Host								
3-27323023951 (1)	Patch Request	Open (74 Days)	2-Significant	1628NM101N ASHOK LEYLAND LIMITED(4132324) ED April 2023	brmex2db03								
<table border="1"> <thead> <tr> <th>Target</th> <th>Target Type</th> <th>Host</th> <th>Services</th> </tr> </thead> <tbody> <tr> <td>DB Machine</td> <td>Oracle Database Machine</td> <td>brmex2db03.acs.oracle.com</td> <td>Platinum, Oracle Advanced Database Support, Platinum,</td> </tr> </tbody> </table>						Target	Target Type	Host	Services	DB Machine	Oracle Database Machine	brmex2db03.acs.oracle.com	Platinum, Oracle Advanced Database Support, Platinum,
Target	Target Type	Host	Services										
DB Machine	Oracle Database Machine	brmex2db03.acs.oracle.com	Platinum, Oracle Advanced Database Support, Platinum,										
3-27310888461	Patch Request	Open (106 Days)	2-Significant	1630NM10WW ASHOK LEYLAND LIMITED(4132324) ED October 2023									
3-25264356471 (1)	Patch Request	Open (41 Days)	2-Significant	1628NM101N ASHOK LEYLAND LIMITED(4132324) ED July 2023	brmex2db03								
3-32658053461 (1)	Patch Request	Open (6 Days)	2-Significant	1628NM101N ASHOK LEYLAND LIMITED(4132324) ED July 2023	brmex2db03								
3-32637672171 (1)	Patch Request	Open (26 Days)	2-Significant	1628NM101N ASHOK LEYLAND LIMITED(4132324) ED July 2023	brmex2db03								

You use this page to manage service requests associated with a particular managed system.

3. Expand an individual SR.

The example in Figure 8–3 shows an open SR associated with a target, *DB Machine*. The SR listing provides a link to the SR in MOS, the SR type, its current status and severity, a description of the SR, and the host machine.

Managing Databases and Database Patches

This chapter provides information about using the Oracle Advanced Support Gateway to manage databases and database patches.

This chapter consists of the following sections:

- ? [About Database Management](#)
- ? [Activating a Service on a Database](#)
- ? [About Patching Requests](#)
- ? [Managing Database Patch Compliance](#)

About Database Management

You can use Oracle Advanced Support Gateway to manage all supported databases and their related cluster and ASM infrastructure as well as requesting the activation of new services on the databases.

Refer to the following sections:

- ? [Viewing Managed Databases](#)
- ? [Editing Managed Databases](#)

Viewing Managed Databases

You can view all managed databases on Oracle Advanced Support Gateway.

To use Oracle Advanced Support Gateway to view managed databases:

1. Log in to Oracle Advanced Support Gateway.

The Oracle Advanced Support Gateway Home page appears.

2. From the **Admin** menu, click **Manage Databases**.

The Manage Databases page appears. So, for example, as shown in [Figure 9–1](#), you can expand a Cluster ASM to view and link to all ASM instances, or expand a database cluster target to view and navigate to its children.

Figure 9–1 Viewing Managed Databases

Manage Databases

Use this page to manage all databases and their related cluster and ASM infrastructure

Actions

Quick Filters: 1 0 0 0 16

Search

Activate New Service

	Name	Type	Status	Host	Lifecycle	Services	Actions
	▼ +ASM_brmex2-clu3-vm1 (2)		Down	brmex2adm08vm01.acs.oracle.com	Test	N/A	
	▼ Automatic Storage Management (2)						
	+ASM1_brmex2adm05vm01.acs.oracle.com		Down	brmex2adm05vm01.acs.oracle.com		N/A	
	+ASM2_brmex2adm08vm01.acs.oracle.com		Down	brmex2adm08vm01.acs.oracle.com		N/A	
	▼ dbm05 (2)		Up	brmex2adm05vm05.acs.oracle.com	Production	N/A	
	▼ Database Instance (2)						
	dbm05_dbm051		Up	brmex2adm05vm05.acs.oracle.com		N/A	
	dbm05_dbm052		Up	brmex2adm05vm05.acs.oracle.com		N/A	
	▶ dbm04 (2)		Up	brmex2adm05vm03.acs.oracle.com	Production	1	
	▶ dbm03 (2)		Up	brmex2adm08vm02.acs.oracle.com	Production	1	
	▶ dbm02 (2)		Up	brmex2adm08vm02.acs.oracle.com	Production	1	
	▶ dbm01 (3)		Up	brmex2adm05vm01.acs.oracle.com	Production	1	
	▶ brmex2-clu3-vm5 (2)		Up	brmex2adm05vm05.acs.oracle.com	Production	N/A	
	▶ brmex2-clu3-vm4 (2)		Up	brmex2adm08vm04.acs.oracle.com	Production	N/A	
	▶ brmex2-clu3-vm3 (2)		Up	brmex2adm08vm03.acs.oracle.com	Production	N/A	
	▶ brmex2-clu3-vm2 (2)		Up	brmex2adm08vm02.acs.oracle.com	Production	N/A	

Databases are defined by:

- **Name:** Displays the database name. You can click any database to display all of its information.

See [Figure 9–2](#) that provides details of a database instance, including database status, support status, the time of the last backup, the number of days for which the database has been up, the database version, its associated targets, and the services running on it.

Furthermore, the Manage Databases page displays other sections that enable users to view and edit database information. For example, these sections include:

The **Configuration** section that displays database monitoring configuration details such as Oracle Home, the database lifecycle, database monitoring level, service name, listener host, and listener port.

All of these values can be edited in the Configuration section. See ["Editing the Monitoring Configuration."](#)

The **Statistics** section provides information about database CPU, memory, and storage utilization in the form of interactive graphs.

For some databases, the session history (number of average active sessions) is also displayed in graphical form.

The **Service Requests** section presents a count of open and closed service requests applicable to the database.

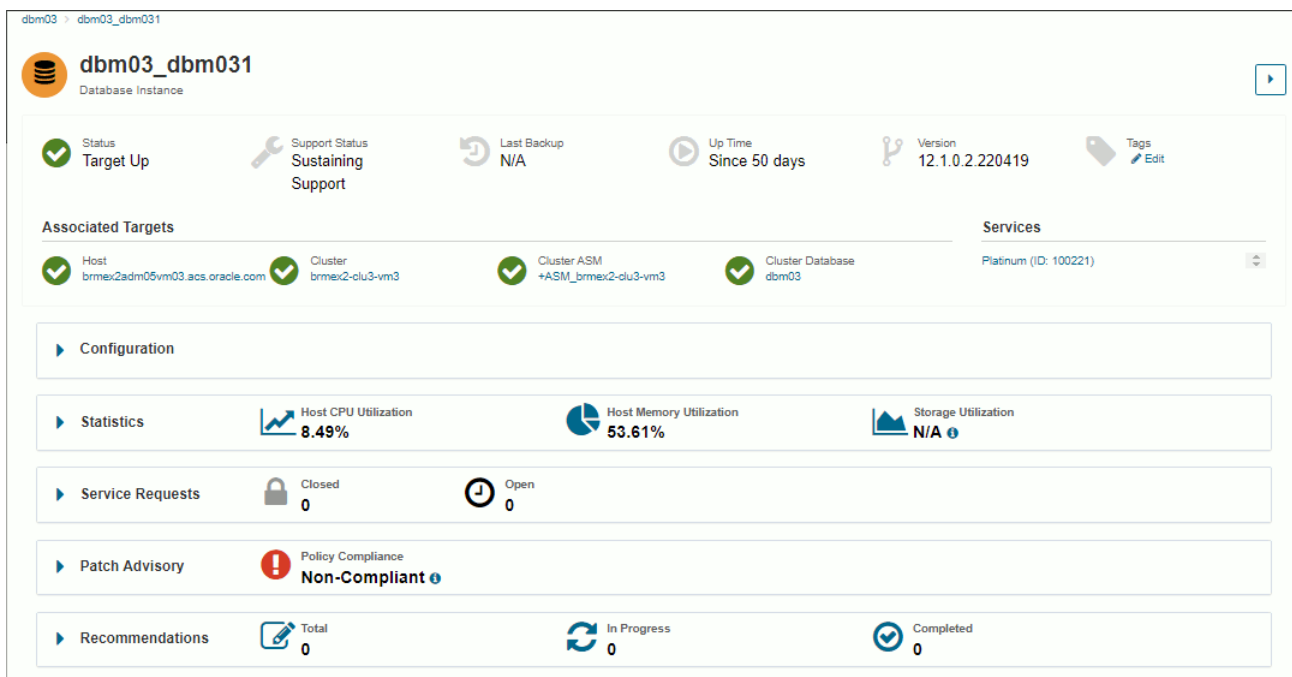
The **Patch Advisory** section displays the patch compliance summary for the database and enables the user to create patching requests if the patching service is activated for the database.

Furthermore, recommended interim patches for the database are displayed in this section.

The **Health Check Report** section displays the output from a selection of lightweight Oracle tools - ORAchk, EXAchk, and Diagnostics Logs tools - that are integrated into

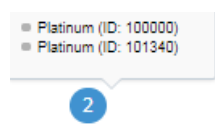
Oracle Advanced Support Gateway and used to analyze and collect data on the health of database infrastructure.

Figure 9–2 Viewing an Individual Database Configuration



- ? **Type** - Database Instance, Cluster Database, Cluster ASM, Cluster, Cluster Database Container, and so on - each type denoted by a different icon.
- ? **Status**: Displays whether the database is currently up, down, or unreachable.
- ? **Host**: Displays the database host name.
- ? **Lifecycle**: Displays the lifecycle associated with the database. The values are *Test*, *Production*, *Stage*, or *Development*.
- ? **Services**: Displays the number of services running on the database. Hover over the number to display a list of individual services. Refer to [Figure 9–3](#) that shows two separate Platinum Services instances running on the database.

Figure 9–3 Displaying the Services Running on a Database



- ? **Actions**: Displays a number of actions that can be performed on the database.

Related Information

[Editing Managed Databases](#)

Editing Managed Databases

You can perform a number of actions on managed databases:

- ✎ Use the **Edit** list to edit databases, including bulk edits on multiple databases.
See ["Editing Managed Databases Using the Edit Icon"](#).
- ✎ Use the icons in the **Actions** column for a particular database to set the database lifecycle or fault monitoring level, edit its DBSNMP or ASMSNMP passwords, or validate the Platinum service running on the target.
See ["Editing Managed Databases Using the Actions List"](#).
- ✎ Edit monitoring configuration details such as Oracle Home, the database lifecycle, database monitoring level, service name, listener host and listener port.
See ["Editing the Monitoring Configuration"](#).

Editing Managed Databases Using the Edit Icon

To use Oracle Advanced Support Gateway to edit a database using the Edit icon:

1. Log in to Oracle Advanced Support Gateway.
The Oracle Advanced Support Gateway Home page appears.
2. From the **Admin** menu, click **Manage Databases**.
The Manage Databases page appears.
3. Select the checkbox(es) corresponding to one or more databases on the Manage Databases page to enable the **Edit** (pencil) icon under Actions on the right of the page.
When multiple selections are made, bulk edit functionality is automatically enabled.
Note: The bulk edit overwrites the existing values for all selected targets.
4. Click the **Edit** icon to display the Edit Lifecycle and Monitoring dialog box. Select from the following options:
 - ✎ **Lifecycle:** The lifecycle associated with the database. Select from the following values: *Test, Production, Stage, Development*, or *None*.
 - ✎ **Monitoring Level:** The monitoring level associated with the database. Select from the following values: *None, Low, Regular, High*, or *Intensive*.
5. Click **Save** to commit.

Editing Managed Databases Using the Actions List

To use Oracle Advanced Support Gateway to edit a database using the Actions icons:

1. Log in to Oracle Advanced Support Gateway.
The Oracle Advanced Support Gateway Home page appears.
2. From the **Admin** menu, click **Manage Databases**.
The Manage Databases page appears.
3. Select the checkbox(es) corresponding to one or more databases on the Manage Databases page to enable the Actions list at the top of the page.
When multiple selections are made, bulk edit functionality is automatically enabled.
Note: The bulk edit overwrites the existing values for all selected targets.
4. From the **Actions** column on the top of the page, select one of the options:
 - ✎ **Monitoring Level:** The monitoring level associated with the database. Select from the following values: *None, Low, Regular, High*, or *Intensive*.

Note: If there are no services running on the selected target, you are unable to edit the monitoring level.

- ⌘ **Lifecycle:** The lifecycle associated with the database. Select from the following values: *Test*, *Production*, *Stage*, *Development*, or *None*. See
- ⌘ **DBSNMP Password:** Change the DBSNMP password in Oracle Password Vault to reflect the database password.
- ⌘ **ASMSNMP Password:** Change the ASMSNMP password in Oracle Password Vault to reflect the database password.
- ⌘ **Validate Activation:** Select a database which has at least one Platinum service activated on it. Enter the credentials for the root user on the host, specify the privilege, for example, *sudo*, and click **Validate** to validate the service running on the database by performing a JDBC connection test.

Note: Service validation applies only to databases on which at least one Platinum service is running.

- ⌘ **Manage Tags:** Add and apply custom tags such as *test* to the database.

Editing the Monitoring Configuration

To use Oracle Advanced Support Gateway to edit the monitoring configuration on the database:

1. Log in to Oracle Advanced Support Gateway.
The Oracle Advanced Support Gateway Home page appears.
2. From the **Admin** menu, click **Manage Databases**.
The Manage Databases page appears.
3. Select a database.
On the database instance page, expand the **Configuration** section.
4. Edit the following values:
 - ⌘ **Oracle Home:** Edit the path to the Oracle Home for the database.
 - ⌘ **Lifecycle:** The lifecycle associated with the database. Select from the following values: *Test*, *Production*, *Stage*, *Development*, or *None*. See
 - ⌘ **Monitoring Level:** The monitoring level associated with the database. Select from the following values: *None*, *Low*, *Regular*, *High*, or *Intensive*.
Note: If there are no services running on the selected target, you are unable to edit the monitoring level.
 - ⌘ **Service Name:** Update the service identifier associated with the database.
 - ⌘ **Listening Host:** Update the host associated with the database monitoring.
 - ⌘ **Listening Port:** Update the port associated with the database monitoring.
5. Click **Save** to commit the changes.

Activating a Service on a Database

In order to activate an Oracle service, you first select available databases to activate, then use the Oracle Advanced Support Gateway user interface to supply and test database credentials. Finally, you activate the databases for your selected service.

For further information, see [Chapter 6, "Activating Services."](#)

About Patching Requests

Automated patch scheduling is provided through Oracle Advanced Support Gateway and optimizes both time and resources for the patch coordinator and the patching manager. Automation also enables the customer to participate in the scheduling process in a transparent manner, in real time.

Note: In this release, automated patch scheduling is supported for Exadata, ZDLRA and database targets for Oracle Platinum Service. In order to schedule patches for other Oracle Engineered Systems, such as Exalogic or SuperCluster, PR requests must be submitted manually.

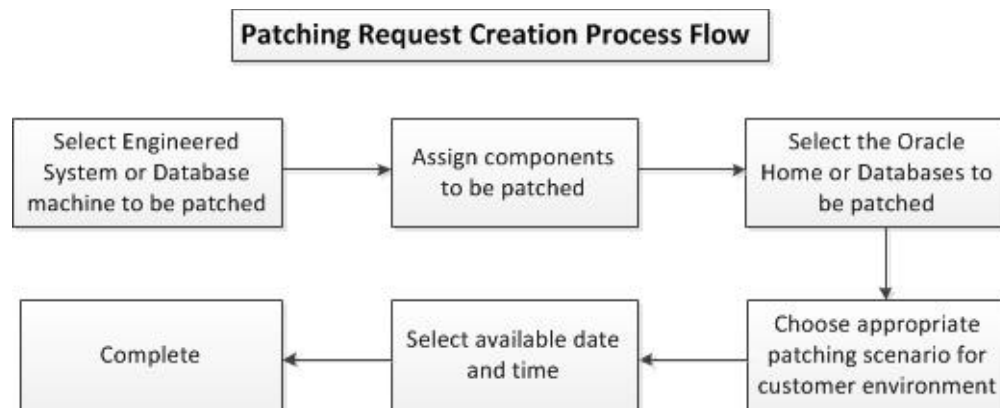
Refer to the following sections:

- ? ["Creating a Patching Request"](#)
- ? ["Editing a Patching Request"](#)

From a customer perspective, scheduling a patch event is now a simple, intuitive process that takes the customer through a number of interactive UI steps:

- ? Review the prerequisites to creating a patching request:
 - ? Patching requests are supported only on Gateways connected via an SSLVPN network.
If your Gateway is connected via IPSec, please reach out to your patch coordinator to create the patching request.
 - ? If your Gateway has the Remote Access Control (Green Button) feature enabled, ensure the VPN is enabled before proceeding to create the patching request.
See [Chapter 14, "Enabling Remote Access to the Oracle Advanced Support Gateway."](#)
 - ? If the Exadata/ZDLRA machine that is required to be patched is still connected to an Oracle Linux version 6.x (OL6) Gateway, then the Exadata/ZDLRA racks cannot be upgraded to the latest Exadata image, that is, version 23.x.
In this case, you need to contact the Platinum Infrastructure team to migrate the Gateway to Oracle Linux version 8.x (OL8) as soon as possible.
- ? Select the Oracle Engineered System or Database machine to be patched.
- ? Assign the components (such as Cell Node, Compute Node, and so on) to be patched.
- ? Select the Oracle Home or Databases to be patched.
- ? Complete a mandatory Pre-Patch template - for Exadata/ZDLRA systems only - prior to completing the scheduling details.
- ? Choose the patching scenario appropriate for the customer environment.
- ? Select the available date and time.

See [Figure 9–4](#) that displays the process flow for Patching Request creation.

Figure 9–4 Patching Request Creation Process Flow

Customer requests for patching are then automatically assigned to Oracle Engineers based on their availability, and this information is visible on the Gateway. Requests for patches from patch coordinators for any date, irrespective of availability, are also accepted. In this case, Engineers are not assigned.

Furthermore, the Resource Manager can create Platinum Resource Teams and Members to manage the Engineer time table associated with each day. Assignment hours for Engineers working in Patching Requests can be assigned, deassigned, updated, or reviewed. Additionally, Engineers can be assigned to non-delivery activities such as holidays, training, internal meetings, etc.

Patching automation provides significant features such as:

- Automatic SR creation from the Gateway portal as soon as the patching request is created. This is a hardware SR using the CSI of the Engineered System that has been scheduled for application of the patch.
- Automated running of EXAchk scripts against the Exadata target 4 weeks prior to the Patching event date.
- Following the implementation of the EXAchk scripts, the EXAchk output is automatically attached to the Patching SR to enable customers and Oracle users to view it and take appropriate action.
- The ability to create, update, and test Patching Scenarios on the Oracle Advanced Support Platform portal. As patching scenarios are created or modified, they are transferred to all connected Gateways.

NOTE: SR creation takes place about 10 minutes after the successful creation of a patching request.

However, you can manually create an SR by clicking an action button on the Gateway user interface. In this case, SR creation is instantaneous.

Furthermore, there is also a workaround of manually running EXAchk by clicking an action button on the Gateway user interface.

Creating a Patching Request

To create a patching request:

1. Log in to Oracle Advanced Support Gateway.

The Oracle Advanced Support Gateway Home page appears.

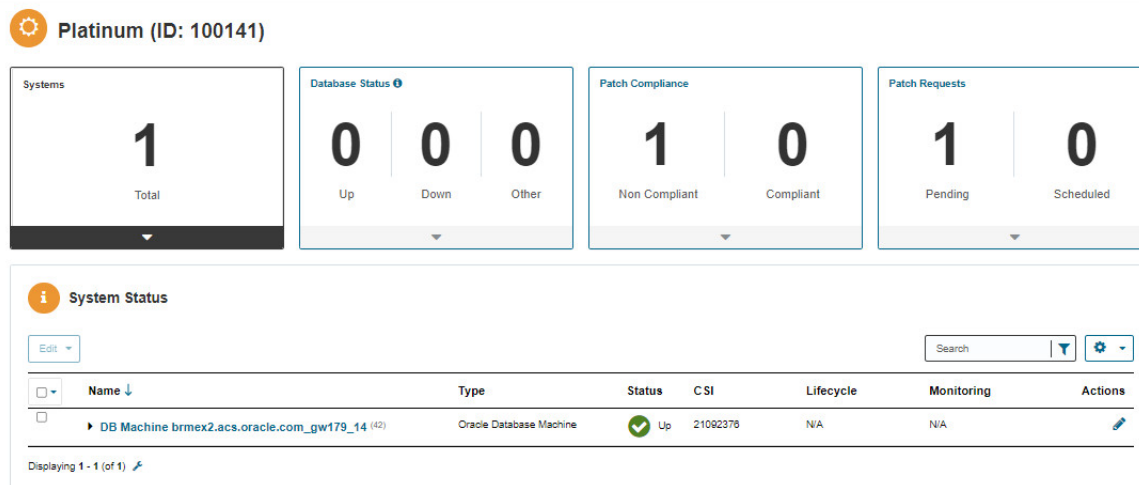
2. From the **My Services** menu, click **All Services**, and then select a service, for example, **Platinum (ID: XXXXXX)**.

The service page appears.

3. Click **Patch Requests/Patch Compliance**.

The Current Requests/Patch Compliance page appears.

Figure 9–5 Viewing Patch Compliance



4. Click **Create Patching Request**.

The Welcome to Platinum Patch Scheduling page appears.

Figure 9–6 Learning about the Patching Request Tool

Platinum (ID:100141) Patching Request

1. Engineered Systems 2. Virtual Racks & Homes 3. Oracle Homes 4. Pre Patch Details 5. Patch Options 6. Schedule 7. Matching Patches 8. Review

Welcome to Platinum Patch Scheduling
Learn what you'll be doing and what information you'll need access to before getting started

Selected Exadata/ZDLRA rack upgrades to the latest Exadata Image, that is, 23.x require Platinum monitoring Oracle Enterprise Manager (EM) agents running on database nodes to be version 13.5 or higher.

Starting with Oracle Advanced Support Gateway (OASG) version 11.X.X, customers can schedule the Exadata / ZDLRA Platinum patching requests themselves using the secure portal on the Gateway. This only supports Oracle Exadata / ZDLRA patching requests for OASG connected via the Secure Socket Layer (SSL), Internet protocol security (IPSEC) and Virtual private Network (VPN).

11.2.0.4 version of database is no longer eligible for Platinum Services as communicated [here](#). Platinum Services will no longer be monitoring or patching 11.2.0.4 Databases and Oracle Home.

If you have purchased MOS service and your system is only running the 11.2.0.4 Database version, please contact your patch coordinator for scheduling the infrastructure components patching request.

The tool will only display the hosts and database targets currently monitored by the Oracle Enterprise Manager of the gateway. If you wish to patch targets not under Platinum Monitoring kindly create a Service request to get them added under Platinum Monitoring before you continue.

Ensure the CSI and MOSID combination is valid for the Rack to be Patched.

Creating this request, you are authorizing Oracle to push the latest TFA software to the database node and run EXachk report. For TFA To run please ensure relevant Passwords are updated directly at OASG Portal, please refer Doc: Platinum Service Delivery - Credential Management in gateway release 9.X Doc ID 2285834.1

Please reach out to your respective Patch Coordinators for further Questions.

☐ Don't show message again

[< Back](#) [Exit >](#) [Accept and Continue >](#)

Select Exadata

You use this page to review the prerequisites to creating a patching request. So, for Platinum for example:

- The Platinum Patch Scheduling tool supports the creation of Exadata/ZDLRA patching requests for Gateways connected using SSLVPN, IPSec, or Virtual Private Network (VPN).

If your Gateway has the Remote Access Control (“Green Button”) feature enabled, ensure the VPN is enabled before proceeding to create the Patch Request.

- The tool displays only the hosts and database targets currently monitored by the Oracle Enterprise Manager of the Gateway. If you wish to patch targets not under Platinum Monitoring, kindly create a service request (SR) to add them under Platinum Monitoring before you continue.
- By creating this request, you are authorizing Oracle to push the latest Trace File Analyzer (TFA) software to the database node and run the EXAchk report.

The TFA tools bundle runs on all managed hosts on which you want to run health checks. The TFA contains the ORAchk, EXAchk, and Diagnostics Logs tools.

ORAchk and EXAchk are lightweight Oracle tools integrated into Oracle Advanced Support Gateway that are used to analyze and collect data on the health of your system infrastructure.

Please ensure relevant passwords are updated directly on the Gateway. Refer to the document *Password Management on Platinum Gateway Portal* ([MOS article 2285834.1](#)).

- Ensure the CSI and MOSID combination is valid for the rack to be patched.

Note: For any questions please reach out to your designated patch coordinator.

For more details about fulfilling the prerequisites, refer to [MOS article 2190010.1](#).

5. Click **Accept and Continue**.

The Engineered Systems page appears.

You use this page to select an Exadata or ZDLRA machine from the list of non-compliant machines to initiate a patching request submission.

Figure 9–7 Selecting the Engineered System to be Patched

Platinum (ID: 100140) Patching Request

Engineered Systems
Select engineered system from non compliant list to initiate patching request submission

Engineered Systems * * required fields

Machine *

Rack Name *

Rack Size *

CSI

MOS ID *

[More Exadata Information](#)

Component Information
Select one of Compute Node, Cell Node, IB Switch or Oracle Home to proceed

Compute Node * ☒ Yes ☐ No

Cell Node * ☒ Yes ☐ No

Oracle Home * ☒ Yes ☐ No

Is Exalogic attached to Rack * ☒ Yes ☐ No

Is ZFS attached to Rack * ☒ Yes ☐ No

Virtual Machine * ☒ Yes ☐ No

IB Switches * ☒ Yes ☐ No

Recovery Appliance attached * ☒ Yes ☐ No

For more details refer to MOS document Doc ID 2190010.1

[Back](#) [Exit](#) [Next](#)

Oracle Homes

6. Complete the following parameters:

- In the **Engineered Systems** field, select *EXADATA* or *ZDLRA*.
- In the **Machine** field, select the Exadata machine to be patched.
Note: Ensure that the components to be patched have been added to Platinum monitoring before continuing.
- In the **Rack Name** field, enter the name of the rack for the selected Exadata machine.
- In the **Rack Size** field, select the rack size from the options provided: *Eighth*, *Quarter*, *Half*, or *Full*.
- In the **MOS ID** field, enter the MOS username associated with the CSI that is associated to this system.

Note: Ensure that the MOS username has the *SR Create* privilege, as this MOS ID and CSI combination is used to create the automatic patching SR in the final step of this wizard.

- f. (Optional) Select **More Exadata Information** to display a My Oracle Support (MOS) Knowledge Base article on “[Exadata Database Machine and Exadata Storage Server Supported Versions](#)”.
- g. In the Component Information section, complete the following parameters by selecting **Yes** or **No** for each of the components (the default for each is *No*):
 - a. In the **Compute Node** field, select whether compute nodes are required to be patched.
If you select **Yes**, from the **Compute Node Quantity** field, select the number of compute nodes in the range 1-16.
 - b. In the **Cell Node** field, select whether cell nodes are required to be patched.
If you select **Yes**, from the **Cell Node Quantity** field, select the number of cell nodes in the range 1-24.
 - c. In the **Oracle Home** field, select whether Oracle Homes are required to be patched.
Note: If you select *No*, then the Oracle Homes step in the workflow is skipped.
 - d. In the **Is Exalogic attached to Rack** field, select whether the Exalogic is attached to the rack being patched.
 - e. In the **Is ZFSSA attached to Rack** field, select whether the ZFSSA is attached to the rack being patched.
 - f. (Optional) In the **Virtual Machine** field, select whether the VM is attached to the rack being patched.
 - g. In the **IB Switches** field, select whether InfiniBand switches are required to be patched.
If you select **Yes**, from the **Switches Quantity** field, select the number of InfiniBand switches in the range 1-6. The default is 2.
 - h. In the **Recovery Appliance attached** field, select whether the recovery appliance is required to be patched.
 - i. (Optional) Select **For more details refer to MOS document Doc ID 2190010.1** to display the My Oracle Support (MOS) Knowledge Base article on “How to Schedule Exadata Patching Request using Oracle Advanced Support Gateway for Platinum Customers”.

7. Click Next.

Select one of the following options:

- ⌚ If you selected to patch Oracle Homes in the Component Information section above, then the Oracle Homes & Databases page appears.
Skip to Step 10.
(Optional) Select **More OJVM Patching Details** to display a MOS Knowledge Base article on “[Oracle JavaVM Component Database PSU](#)” ([OJVM PSU](#)) [Patches](#)”.
- ⌚ If you select to patch Virtual Racks, then the Virtual Racks and Homes page appears and you then skip the Oracle Homes step and continue to patching instead.
Continue to Step 14.
- ⌚ If you selected *not* to patch Oracle Homes in the Component Information section above, then the Patch Option page appears.
Skip to Step 14.

(Optional) Select **More OJVM Patching Details** to display a MOS Knowledge Base article on “[Oracle JavaVM Component Database PSU](#)” (OJVM PSU) Patches”.

8. Click **Next**.

The Virtual Racks and Homes page appears.

Figure 9–8 *Selecting the Virtual Racks to be Patched*

Virtual Rack

Maximum of 4 Virtual Racks can be selected. If you don't see the expected Oracle homes or Databases on this page, please add them to Platinum Monitoring by following the steps in the Reference Article id 2246149.1

<input type="checkbox"/> Select	VRACK_brmex2adm06	i
<input type="checkbox"/> Select	VRACK_brmex2adm06vm05	i
<input type="checkbox"/> Select	VRACK_brmex2adm05	i
<input type="checkbox"/> Select	VRACK_brmex2adm05v	i
<input type="checkbox"/> Select	VRACK_brmex2adm06v	i

[< Back](#) [Exit >](#) [Next >](#)

Exadata & Components Patch Options

9. In the Virtual Rack page, select virtual racks (to a maximum of 4).

- a. Expand the required virtual rack by clicking the appropriate **Select** checkbox:

Figure 9–9 Selecting the Virtual Racks to be Patched

Virtual Rack
Maximum of 4 Virtual Racks can be selected. If you don't see the expected Oracle homes or Databases on this page, please add them to Platinum Monitoring by following the steps in the Reference Article id 2246149.1

☐ Select **VRACK** ⓘ

Select Oracle Grid Homes
Maximum of one Grid Homes can be selected

Search

<input type="checkbox"/> Grid Home ↑	Bundle Patch	Upgrade
<input type="checkbox"/> /u01/app/21.0.0.0/grid	<input type="checkbox"/>	<input type="checkbox"/> ⚙

Displaying 1 - 1 (of 1) [↗](#)

Select Oracle Homes
Maximum of two Oracle Homes can be selected

Search

<input type="checkbox"/> Oracle Home ↑	BP	OJVM	EBS	Data Vault	New Home	Database
<input type="checkbox"/> /u01/app/oracle/product/21.0.0.0/dbhome_1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> ⚙	0/1 + Select

Displaying 1 - 1 (of 1) [↗](#)

- b. (Optional) Select the components on a particular Virtual Rack that require patching:

- ? In the **Select Oracle Grid Homes** field, select databases (to a maximum number of Grid Homes, depending on the customer contract).

The available Grid Homes are displayed on the Homes page showing Grid Home location, and providing a bundle patch application option and (if applicable) an upgrade option.

For the Grid Home, select whether to apply a bundle patch.

A bundle patch is a cumulative collection of fixes for a specific product or component. A patch of this type is released as needed depending on the product's requirements. You may also know a bundle patch as: maintenance pack, service pack, MLRs, cumulative patch, or update release.

For the Grid Home, select whether to apply an upgrade.

If you select to upgrade, provide a new name for the Grid Home and choose the target grid version.

- ? In the **Select Oracle Homes** section, select databases (to a maximum number of Oracle Homes, depending on the customer contract).

Select from the following options:

- a. Select individual databases by clicking **Select** in the **Oracle Home** column.
- b. (Optional) Select the components on a particular Oracle Home that require patching or update the Oracle Home configuration as follows:

Select **BP** to apply a bundle patch.

A bundle patch is a cumulative collection of fixes for a specific product or component. A patch of this type is released as needed depending on the product's requirements. You may also know a bundle patch by one of the following names: *maintenance pack*, *service pack*, *MLRs*, *cumulative patch*, or *update release*.

Select **OJVM** to patch Oracle Java Virtual Machine.

Note: Selecting OJVM may add an additional 90 minutes outage time to Oracle Home, assuming the databases to be patched are configured as a resource in cluster.

For further information, refer to [OJVM Patching Details on My Oracle Support](#).

Select **EBS** to patch Oracle E-Business Suite.

Select **Data Vault** to patch Oracle Database Vault.

Select **New Home** to specify a new Oracle Home. Provide a new name for the target and select a target version, for example, *12.1* or *12.2*.

In the **Database** field, click **+Select** to select constituent databases from the Oracle Home.

From the database list, select the required database and configure it as follows:

Select **Dataguard** to apply Oracle Data Guard. From the **DB Type** field, select *Primary* or *Standby* to specify the database type.

Note: Oracle Data Guard ensures high availability, data protection, and disaster recovery for enterprise data.

Select **Datapatch** to apply the particular scripts that need to run for installation or rollback of each patch in the bundle series.

After patching Virtual Racks, you then skip the Oracle Homes step and continue to patching instead.

Continue to Step 14.

10. Click Next.

The Oracle Homes page appears.

Figure 9–10 Selecting the Oracle Homes, Grid Homes, and Databases to be Patched

Select Oracle Homes
Select maximum of 2 Oracle Homes

Ora Home Limit: 1 / 2

Oracle Home	BP	OJVM	EBS	Databases
<input checked="" type="checkbox"/> /u01/app/oracle/product/12.1.0.2/dbhome_1	<input checked="" type="checkbox"/> Yes <input checked="" type="checkbox"/> No	<input checked="" type="checkbox"/> Yes <input checked="" type="checkbox"/> No	<input checked="" type="checkbox"/> Yes <input checked="" type="checkbox"/> No	0 / 1

Displaying 1 - 1 (of 1)

Grid Homes

Database	Installed	Target	Upgrade
<input type="checkbox"/> /u01/app/11.2.0.4/grid	11.2	12.1	<input checked="" type="checkbox"/> Yes <input checked="" type="checkbox"/> No
<input type="checkbox"/> /u01/app/12.1.0.2/grid	12.1	12.2	<input checked="" type="checkbox"/> Yes <input checked="" type="checkbox"/> No

Displaying 1 - 2 (of 2)

Exadata & Components Patch Options

11. In the Select Oracle Homes section, select databases (to a maximum number of Oracle Homes, depending on the customer contract).

Select from the following options:

- a. Select individual databases by clicking **Select** in the **Oracle Home** column.
 - b. (Optional) Select the components on a particular Oracle Home that require patching:
 - ? In the **BP** field, click **Yes** to apply a bundle patch.
 A bundle patch is a cumulative collection of fixes for a specific product or component. A patch of this type is released as needed depending on the product's requirements. You may also know a bundle patch as: maintenance pack, service pack, MLRs, cumulative patch, or update release.
 - ? In the **OJVM** field, click **Yes** to patch Oracle Java Virtual Machine.
Note: Selecting OJVM may add an additional 90 minutes outage time to Oracle Home, provided the databases to be patched are configured as a resource in cluster.
 For further information, refer to [OJVM Patching Details on My Oracle Support](#).
 - ? In the **EBS** field, click **Yes** to patch Oracle E-Business Suite.
12. (For Oracle Homes) Click **+Select** to select constituent databases from the Oracle Home.
 - a. Select individual databases by clicking **Select** in the **Databases** column.
 - b. (Optional) Select the components on a particular Oracle Home that require patching:
 - ? In the **Datapatch** field, click **Yes** to apply the particular scripts that need to run for installation or rollback of each patch in the bundle series.
13. (Optional) In the Grid Homes section, select databases (to a maximum number of Grid Homes, depending on the customer contract. Typically customers have a maximum of 5 Grid Homes.)
 A list of grid homes is displayed on the Homes page - showing grid home location, installed grid version, whether an upgrade is required, and if so, the target grid version.
 You can select to upgrade those required.
 Select from the following options:
 - a. Select individual databases by clicking **Select** in the **Databases** column.
 - b. (Optional) Select the installed grid versions that require updating:
 - ? In the **Upgrade** field, click **Yes** to enable the **Target** field.
 - ? In the **Target** field, select the required grid version, for example, *12.1* or *12.2*.
14. Click **Next**.
 The Pre-Patch Details page appears.
 You use this page to supply information for pre-patching prior to completing the scheduling details.

Figure 9–11 Supplying Pre-Patch Information, Part 1

PrePatch Details
Details required for Pre Patching

System Function *

- Select Functio ▾

OJVM Options*

☒ Apply OJVM patch (1 Hr downtime) -Recommended

☐ Apply Mitigation patch (Can interfere with other Java Applications) -Recommended for short term only if OJVM downtime is not possible

☐ None -Not Recommended

i Please review note 1929745.1 and select one of the options. Applying the OJVM requires 1Hr of downtime per RAC for both primary and stand-by environments. Mitigation and OJVM patches can coexist. The mitigation patch can be turned on and off at will.

Owner and Group details of Grid & Oracle Homes to be patched* (500 characters left)

Enter Owner & Group

i Execute below command as root/ sudo user in 1st DB node of cluster:
Command: `egrep -v "^[^$]agent" /etc/oratab | cut -d ":" -f2 | sort | uniq | while read home;do echo -n "$home==>"; stat -c "%U:%G $home/inventory;done`

Agent Details* (500 characters left)

Enter Agent Details

i Execute below command as root/ sudo user in 1st DB node of cluster:
Command: `ps -ef | grep agent | grep java | sed 's/s/+/' | cut -d ":" -f1,8 | sed 's/|jdk:*/'`

15. Complete the following parameters:

- a. In the **System Function** field, select the functional nature of the patch, for example, production, development, test, and so on.
- b. In the **OJVM Options** field, select from the following options:

Note: Mitigation and OJVM patches can coexist. The mitigation patch can be turned on and off, at will.

Review My Oracle Support (MOS) [note 1929745.1](#) and select one of the options below (applying the OJVM requires approximately one (1) hour of downtime per RAC for both primary and stand-by environments):

Option 1: Apply the OJVM patch (This is the recommended option.)

Option 2: Apply a Mitigation patch.

This process can interfere with other Java applications and is recommended for short-term patching only if OJVM downtime is not possible.

Option 3: Apply no patch. This option is **not recommended**.

- c. In the text box labeled **Owner and Group details of Grid & Oracle Homes to be patched***, enter the owner and group of Grid & Oracle Home.
- d. Execute the following command as the *root/sudo* user in the first database node of the cluster:


```
egrep -v "^[^$]agent" /etc/oratab | cut -d ":" -f2 | sort | uniq | while read home;do echo -n "$home==>"; stat -c "%U:%G $home/inventory;done
```
- e. In the text box labeled **Agent Details***, enter information about the agent.
- f. Execute the following command as the *root/sudo* user in the first database node of the cluster:



```
ps -ef | grep agent | grep java | sed 's/\s+//g' | cut -d " " -f 1,8 | sed 's/\jdk.*//
```

Figure 9–12 Supplying Pre-Patch Information, Part 2

EBS database home present in the environment*

☐ Yes

☐ No

 If Yes, please provide special instructions that need to be taken in consideration for EBS patching, please review MOS DOC ID 1392527.1

SAP database home present in the environment*


☐ Yes

☐ No

Redundancy*

☐ Normal

☐ High

 For Rolling events, High Redundancy is recommended

Oracle Homes Patch Options

- g.** In the **EBS database home present in the environment** field, select **Yes** if an EBS database home is present, or select **No** if this option is not applicable in this instance.

If you select **Yes**, please provide in the text box any special instructions that need to be taken in consideration for EBS patching.

Note: First review the relevant [MOS document](#), ID 1392527.1.

- h.** In the **SAP database home present in the environment** field, select **Yes** if a SAP database home is present, or select **No** if this is not applicable in this instance.
- i.** In the **Redundancy*** field, select **Normal** or **High**.

Note: For rolling events, high redundancy is recommended.

16. Click Next.

The Patching Request: Patch Option page appears.

You use this page to select a patching scenario based on database, patch type, and time.

Figure 9–13 Selecting the Patch Option

Patch Option
Select scenario based on database, patch type and time

[Patch Parameters](#)

Info: NR = Non-Rolling, R = Rolling, M = Maintenance Mode, P = Production Mode, OOP = Out of Place.

Search

Select	Patch Option	Estimated Duration ↑	Outage Window	Description
<input type="radio"/>	Split-Patching			Split patching scenario
<input type="radio"/>	Patching-scenario-1	0 Hrs 15 Mins	0 Hrs 30 Mins	test
<input type="radio"/>	testScenario9Dec	0 Hrs 15 Mins	NA	test
<input type="radio"/>	testScenario_6Jan	0 Hrs 15 Mins	NA	testing
<input type="radio"/>	Hybrid-1-Exadata	0 Hrs 45 Mins	NA	TESTIn Hybrid - 1 Mode, Cells are done rolling to save some dow... more
<input type="radio"/>	Hybrid-2-Exadata	0 Hrs 45 Mins	NA	In Hybrid - 2 Mode, Catbundles also done outside of maintenance... more
<input type="radio"/>	Hybrid-3-Exadata	0 Hrs 45 Mins	NA	In Hybrid - 3 Mode, IB switches also done outside of maintenanc... more
<input type="radio"/>	Hybrid-4-Exadata	0 Hrs 45 Mins	NA	In Hybrid - 4 Mode, OS and DB done rolling and Cells and IB non... more
<input type="radio"/>	Hybrid-5-Exadata	0 Hrs 45 Mins	NA	In Hybrid - 5 Mode, Same as 4 except IB done outside maintenanc... more

17. Select the applicable patch option using a combination of the following parameters:

- The **Patch Option** column displays the patch type.
- The **Estimated Duration** column displays the time taken for the patching process.
- The **Outage Window** column displays the outage time for the device.
- The **Description** column provides a full explanation of the patch types listed in the **Patch Option** column, using the following abbreviations:

NR = Non-Rolling, **R** = Rolling, **M** = Maintenance Mode, **P** = Production Mode

(Optional) Click **More** to display the full details of the patch type.

For example, *In Hybrid - 4 Mode, OS and DB done rolling and Cells and IB non-rolling. Compute Nodes = R, Grid Home = R, Database Homes = R, Catbundles = P, Storage Cells = NR, IB Switch = M and OJVM = NR Modified at 2.41.*

18. Click **Next**.

The Patching Request: Schedule page appears.

You use this page to set the patching time and date. All estimates may vary and the final period may change.

Figure 9–14 Selecting the Patch Schedule

Platinum Patching Request

✓ 1. Engineered Systems 2. Virtual Racks & Homes ✓ 3. Oracle Homes ✓ 4. Pre Patch Details ✓ 5. Patch Options

6. Schedule 7. Matching Patches 8. Review

Schedule
Set patching time and date with additional comments for the patching request

[Patch Parameters](#)

Estimated Duration: 0 Hrs 15 Mins Outage Window: 0 Hrs 30 Mins Estimated Period: 11/05/2023 to 11/05/2023 Start Time Patch Option: Patching-scenario-1

[< Back](#) [Exit](#) [Next >](#)

Patch Options Review & Complete

19. Select the time and date for the patching request using the following parameters:

- ⌘ Schedule a patching date a minimum of four (4) weeks from the present date
- ⌘ Use the calendar to select available dates within an estimated period.
- ⌘ You cannot schedule a patch within 90 days of an existing Patch Request on the same database.

If you attempt to generate a conflicting patch request, an error message appears, requesting you to cancel previous patch request(s) before scheduling another one.

- ⌘ Complete all required fields successfully (you cannot submit a patching request in the next step until the configuration is complete)


Note: Preferred time and date formats are based on the browser time zone.


Note: If you receive a message stating that a system error has occurred, please contact your patch coordinator for help. See ["Contacting the Patch Coordinator"](#).


20. Click **Next**.


The Review Patching Request page appears.


Figure 9–15 Reviewing the Patch Schedule Request Details



Review Patching Request
 Review submitted Patch Request below


 Exadata Machine
 DB Machine


 Target Patch Version


 Progress
 Draft


 SR #
 NA


 CM #

Oracle Homes & Databases

Cell Node	Compute Node	IB Switches	Oracle Home	Database	Exalogic	ZFSSA Attachment	Data Vault	Data Guard Configuration
No	No	No	Yes	No	No	No	No	No

Virtual Machine	Virtual RAC	Recovery Appliance Attached	Patch Option
No	0	No	Patching-scenario-1

N/A

Actual Period	Actual Duration	Estimated Period	Estimated Duration	Outage Window	Started
			0 Hrs 15 Mins	0 Hrs 30 Mins	

Additional Comments

Pre Patch Details

System Function	Redundancy	Owner & Group	Agent Details	OJVM Options
Test	Normal	Test	Test	Apply OJVM patch (1 Hr downtime) - Recommended

EBS database home present in the environment	EBS details	SAP database home present in the environment	SAP Path
No		No	

Additional Comments

(255 characters left)

This page requires you to review and confirm the details of the patching request prior to submission.

The page lists the machine name and patch version. It specifies the components to be patched, such as computer nodes, cell nodes, switches, databases, and so on.

Furthermore, the page specifies the estimated duration and outage window associated with the patching process, the period during which it is likely to take place, the start time, the nature of the patch process, for example, whether rolling or non-rolling, and so on.

Finally, the applicable Oracle Homes, (Grid Homes), and databases are listed.

21. Click **Submit Request**.

Note: Do not close the window until submission is completed and the confirmation page appears.

The Complete Patching Request page appears.

This page displays a message stating that the patch creation has been successful:

Request #123456 submitted successfully. Please wait for 15 minutes for SR to appear on the Current Requests page.

The Complete Patching Request page also provides details of the patching request as outlined in Step 20.

22. As the patching Request has been created successfully, click **Continue to Current Requests** to review the list of current patching requests.

The Current Requests page appears.

You use this page to:

- 7 Edit an existing patching request that is in draft mode.
See ["Editing the CM for a Patching Request"](#).
- 7 Cancel an existing patching request.

Figure 9–16 Viewing Current Patching Requests

Current Requests							
Bulk Actions ▾		Quick Filters: 4 7 7 17 0 0				Search	+ Create Patching Request ⚙
<input type="checkbox"/>	Request # ↓	Created	Scheduled	SR #	CM # ↓	Progress	Actions
<input type="checkbox"/>	100344	05-11-2023				Draft	
<input type="checkbox"/>	100323	05-04-2023				Draft	
<input type="checkbox"/>	100322	05-03-2023	09-19-2023 08:00 IST (GMT +01:00)	3-3288053481	21707	Scheduled	
<input type="checkbox"/>	100321	05-02-2023				Draft	
<input type="checkbox"/>	100303	04-14-2023				Draft	
<input type="checkbox"/>	100302	04-14-2023				Draft	
<input type="checkbox"/>	100301	04-14-2023	09-13-2023 08:00 IST (GMT +01:00)	3-32837872171	21451	Scheduled	
<input type="checkbox"/>	100282	03-30-2023	09-09-2023 08:00 IST (GMT +01:00)	3-25284356471	21330	Scheduled	
<input type="checkbox"/>	100281	03-29-2023				Draft	
<input type="checkbox"/>	100261	03-24-2023		3-27333481321		Cancelled	

Displaying 1 - 10 (of 35) 1 / 4 < >

Related Information

[Editing the CM for a Patching Request](#)

[Canceling Patching Requests](#)

Editing the CM for a Patching Request

You can edit an SR associated with a patching request by assigning a new CM number to be associated with the patch.

To edit an SR:

1. Log in to Oracle Advanced Support Gateway.
The Oracle Advanced Support Gateway Home page appears.
2. From the **My Services** menu, click **All Services**, and then select a service, for example, **Platinum**.
The Platinum Service page appears.
3. Click **Patch Requests**.
The Current Requests page appears.

Figure 9–17 Viewing Patching Requests

Request #	Created	Scheduled	SR #	CM #	Progress	Actions
100344	05-11-2023				Draft	Edit Delete Toggle
100323	05-04-2023				Draft	Edit Delete Toggle
100322	05-03-2023	09-19-2023 08:00 IST (GMT +01:00)	3-32858053461 Edit	21707 Edit	Scheduled	Edit Delete Toggle
100321	05-02-2023				Draft	Edit Delete Toggle
100303	04-14-2023				Draft	Edit Delete Toggle
100302	04-14-2023				Draft	Edit Delete Toggle
100301	04-14-2023	09-13-2023 08:00 IST (GMT +01:00)	3-32837672171 Edit	21461 Edit	Scheduled	Edit Delete Toggle
100282	03-30-2023	09-09-2023 08:00 IST (GMT +01:00)	3-25264356471 Edit	21330 Edit	Scheduled	Edit Delete Toggle
100281	03-29-2023				Draft	Edit Delete Toggle
100261	03-24-2023		3-27333481321		Cancelled	Edit Delete Toggle

Displaying 1 - 10 (of 35)

- For a request for which an SR has already been created, for example, the request numbered 10081, under the CM# column, click **Edit**.

An Assign CM# dialog box appears.

Figure 9–18 Assigning the Patching Request CM Number

Assign CM #

Use the field below to update CM #

CM #

[Cancel](#) [Save](#)

- In the **CM #** field, assign a new CM number to be associated with the patch.
- Click **Save**.

Related Information

[Assigning an SR for a Patching Request](#)

[Canceling Patching Requests](#)

Assigning an SR for a Patching Request

You can assign a new SR number to be associated with a patching request.

To assign an SR number to a patch request:

- Log in to Oracle Advanced Support Gateway.
The Oracle Advanced Support Gateway Home page appears.
- From the **My Services** menu, click **All Services**, and then select a service, for example, **Platinum**.
The Platinum Service page appears.
- Click **Patch Requests**.

The Current Requests page appears.

Figure 9–19 Viewing Patching Requests

Request #	Created	Scheduled	SR #	CM #	Progress	Actions
100344	05-11-2023				Draft	[Edit] [Copy] [Link]
100323	05-04-2023				Draft	[Edit] [Copy] [Link]
100322	05-03-2023	09-19-2023 08:00 IST (GMT +01:00)	3-32858053481 [Edit]	21707 [Edit]	Scheduled	[Edit] [Copy] [Link]
100321	05-02-2023				Draft	[Edit] [Copy] [Link]
100303	04-14-2023				Draft	[Edit] [Copy] [Link]
100302	04-14-2023				Draft	[Edit] [Copy] [Link]
100301	04-14-2023	09-13-2023 08:00 IST (GMT +01:00)	3-32837672171 [Edit]	21451 [Edit]	Scheduled	[Edit] [Copy] [Link]
100282	03-30-2023	09-09-2023 08:00 IST (GMT +01:00)	3-25284356471 [Edit]	21330 [Edit]	Scheduled	[Edit] [Copy] [Link]
100281	03-29-2023				Draft	[Edit] [Copy] [Link]
100261	03-24-2023		3-27333481321		Cancelled	[Edit] [Copy] [Link]

Displaying 1 - 10 (of 35)

- For a patching request, under the SR column, click **Assign**.

An Assign SR# dialog box appears.

Figure 9–20 Assigning the Patching Request SR Number

Assign SR #

Use the field below to update SR #

SR #

- In the **SR #** field, assign a new SR number to be associated with the patch.

- Click **Save**.

An email is sent to the Gateway user associated with the SR creation specifying:

- ? The new SR number (from which you can link to the SR on MOS directly);
- ? The hostname;
- ? The CSI of the Engineered System that has been scheduled for application of the patch;
- ? Links to documentation relating to Oracle Auto Service Request (ASR);
- ? Translations of the email in Chinese, Japanese, and Korean.

Related Information

[Canceling Patching Requests](#)

Canceling Patching Requests

To cancel patching requests:

1. Log in to Oracle Advanced Support Gateway.
The Oracle Advanced Support Gateway Home page appears.
2. From the **My Services** menu, click **All Services**, and then select a service, for example, **Platinum**.
The Platinum Service page appears.
3. Click **Patch Requests**.
The Current Requests page appears.

Figure 9–21 Viewing Patching Requests

Request #	Created	Scheduled	SR #	CM #	Progress	Actions
100344	05-11-2023				Draft	[Edit] [Cancel] [Refresh]
100323	05-04-2023				Draft	[Edit] [Cancel] [Refresh]
100322	05-03-2023	09-19-2023 08:00 IST (GMT +01:00)	3-32858053481 [Edit]	21707 [Edit]	Scheduled	[Edit] [Cancel] [Refresh]
100321	05-02-2023				Draft	[Edit] [Cancel] [Refresh]
100303	04-14-2023				Draft	[Edit] [Cancel] [Refresh]
100302	04-14-2023				Draft	[Edit] [Cancel] [Refresh]
100301	04-14-2023	09-13-2023 08:00 IST (GMT +01:00)	3-32837872171 [Edit]	21451 [Edit]	Scheduled	[Edit] [Cancel] [Refresh]
100282	03-30-2023	09-09-2023 08:00 IST (GMT +01:00)	3-25264356471 [Edit]	21330 [Edit]	Scheduled	[Edit] [Cancel] [Refresh]
100281	03-29-2023				Draft	[Edit] [Cancel] [Refresh]
100261	03-24-2023		3-27333481321		Cancelled	[Edit] [Cancel] [Refresh]

Displaying 1 - 10 (of 35)

4. Select the checkboxes corresponding to scheduled requests for which SRs have already been created, for example, the requests numbered 1000322 and 1000301 in Figure 9–21.
5. From the Bulk Actions dropdown, click **Cancel**.
A cancellation request dialog box appears.

Figure 9–22 Confirming the Cancellation of a Patching Request

Are you sure you want to cancel ?

Cancellation Reason

No Yes

6. In the **Cancellation Reason** field, enter a justification for canceling the patching requests.
7. Click **Yes**.

The Current Requests table is refreshed and the patching request status changes to *Canceled* in the Progress column.

Related Information

[Editing the CM for a Patching Request](#)

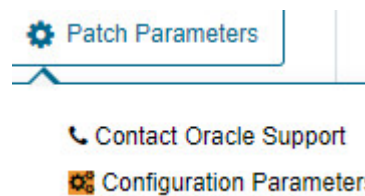
Contacting the Patch Coordinator

If you have issues with a patch request, for example, you are concerned that the status of your patch request is not up to date, contact your patch coordinator for help.

To contact your patch coordinator:

1. Click **Patch Parameters** in the Patch Options or Schedule pages. The following dialog appears:

Figure 9–23 Selecting the Patch Parameters



2. Select **Contact Oracle Support**. The Patch Coordinator Contact Details dialog appears, displaying the patch coordinator name and email address.

Editing a Patching Request

To edit a patching request:

1. Log in to Oracle Advanced Support Gateway.
The Oracle Advanced Support Gateway Home page appears.
2. From the **My Services** menu, click **All Services**, and then select, a service, for example, **Platinum**.
The Platinum Service page appears.
3. Click **Patch Requests**.
The Current Requests page appears.
4. In the Actions column, click the icon signifying **Edit**.
The Prerequisites to Create a Patching Request informational message appears.
5. Follow the steps listed in "[Creating a Patching Request](#)" and edit the details as required.

Related Information

[Creating a Patching Request](#)

Managing Database Patch Compliance

Customers can view the compliance summary for Oracle Engineered Systems activated under Oracle Platinum Service. Compliance is determined by comparing the installed patchset version with the value of the Oracle Advanced Support Gateway setting: *Patch Set Compliance Level*.

Refer to the following section:

7 ["Setting the Database Patchset Compliance Level"](#)

Setting the Database Patchset Compliance Level

You can set the patch set compliance level for your service, for example, for supported Oracle Engineered Systems activated under Oracle Platinum Service.

The Compliance Level setting indicates whether the installed Patch Set version is within the compliance levels as per your patch policy. You can set the compliance level on a database instance. Changing this setting will affect all the targets.

So, for example, if you select the value of the Patch Set Compliance Level setting as *Latest -1*, if the latest Quarterly Full Stack Download Patch (QFSDP) available is Jan 2023 - any engineered system with a QFSDP before Oct 2022 will be considered as “Non-Compliant”.

To set the database patchset compliance level:

1. Log in to Oracle Advanced Support Gateway.

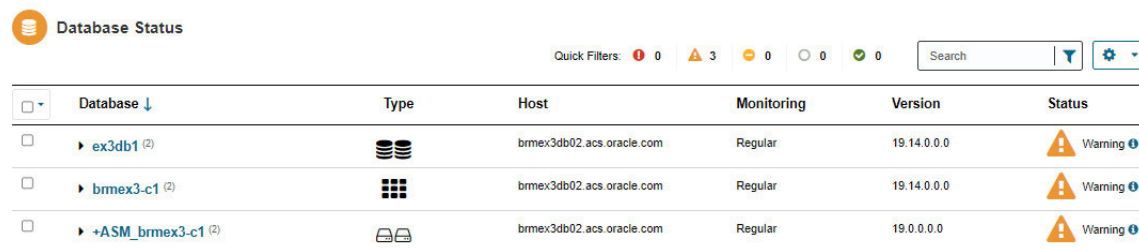
The Oracle Advanced Support Gateway Home page appears.






2. From the **My Services** page, select the required service.

The service home page appears, displaying various database tabs.

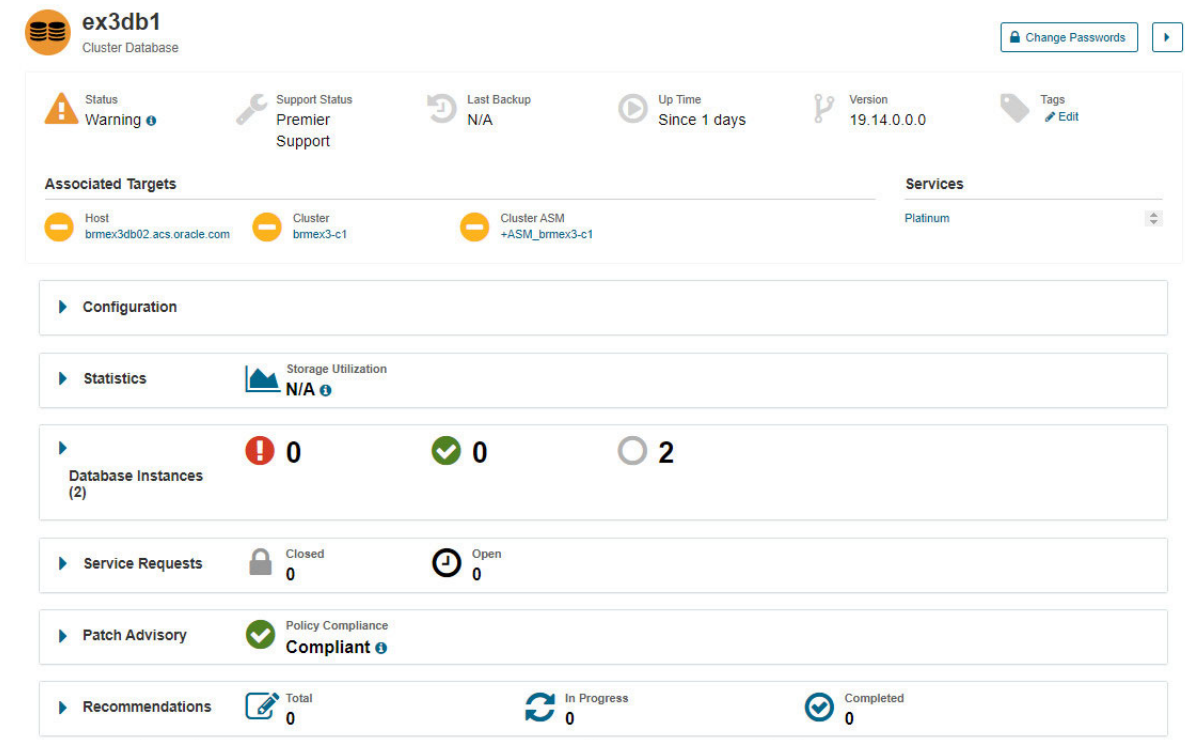
3. Select the **Database Status** badge to display your discovered databases in the Database Status table.

Figure 9–24 Viewing Database Status



Database	Type	Host	Monitoring	Version	Status
ex3db1 (2)		brmex3db02.acs.oracle.com	Regular	19.14.0.0.0	 Warning ⓘ
brmex3-c1 (2)		brmex3db02.acs.oracle.com	Regular	19.14.0.0.0	 Warning ⓘ
+ASM_brmex3-c1 (2)		brmex3db02.acs.oracle.com	Regular	19.0.0.0.0	 Warning ⓘ

4. Select a database instance to display the database configuration.

Figure 9–25 *Displaying the Database Configuration*

- Expand the **Patch Advisory** section.

Figure 9–26 Viewing the Patch Advisory Details

Patch Advisory

Policy Compliance
Non-Compliant

Installed Bundle
N/A

Recommended Bundle
Database Patch Set Update
11.2.0.4.170418

[+ Create Patching Request](#)
[Edit Compliance Level](#)

Recommended Interim Patches for

Oracle Database Release 11.2.0.4.0 - Installed

Bug ID	Patch Name	Doc ID	Severity	Downloads	Affected Features
21967332	A PUBLIC SYNONYM TO A TYPE TAKES PRECEDENCE OVER LOCAL TYPE		Severe Loss of Service	3933	CORE_DB
18841764	Network related error like ORA-12592 or ORA-3137 or ORA-3106 may be signaled	18841764.8	Severe Loss of Service	3401	CORE_DB
18607546	ORA-600 [kdblkcheckerror].[6266] corruption with self-referenced chained row. ORA-600 [kdsgrp1] / W	18607546.8	Severe Loss of Service	3076	CORE_DB
14373728	NOT PURGING OLD STATISTICS FROM SYSAUX TABLESPACE	14373728.8	Severe Loss of Service	2883	CORE_DB
17890099	ORA-2072 AND ORA-2063 ON QUERY VIA DBLINK	17890099.8	Severe Loss of Service	2657	CORE_DB
18665660	High child cursor counts due to OPTIMIZER_MISMATCH with Optimizer_features_enable=9.2.0	18665660.8	Severe Loss of Service	2655	CORE_DB
17325413	Drop column with DEFAULT value and NOT NULL definition ends up with dropped column data hitting disk	17325413.8	Severe Loss of Service	2536	Partitioning (s... +1 more)
19614585	Wrong Results / ORA-600 [kksgaGetNoAlloc_int0] / ORA-7445 / ORA-8103 / ORA-1555 from query on RAC A	19614585.8	Severe Loss of Service	2293	Active Data Gua... +7 more
18235390	ORA-600 [KGHSTACK_UNDERFLOW_INTERNAL_3] AFTER APPLYING PATCH 17897511	18235390.8	Severe Loss of Service	2229	CORE_DB
13931044	ORA-600 [13009], [5000], [1], [17]	13931044.8	Severe Loss of Service	2225	CORE_DB

Displaying 1 - 10 (of 62)

1 / 7

6. Click **Edit Compliance Level**.

The Patch Policy Settings dialog box appears. The Compliance Level setting indicates whether the installed Patch Set version is within the compliance levels as per your patch policy.

Select the required compliance level to set across the targets. Changing this setting will affect all the targets. The options are:

- ⌵ Latest
- ⌵ Latest - 1
- ⌵ Latest - 2
- ⌵ Latest - 3

The default is *Latest-2* and is part of the initial reference schema of the Gateway.

7. Click **Save** to confirm.

Scheduling Database Blackouts

This chapter provides information about using Oracle Advanced Support Gateway to manage database blackouts.

It includes the following topics:

- 7 [About Database Blackouts](#)
- 7 [Creating Database Blackouts](#)
- 7 [Managing Database Blackouts](#)

About Database Blackouts

Blackouts allow Oracle Advanced Support Gateway users and administrators to suspend monitoring of databases for a specified time. If a fault is detected for the database under blackout during this scheduled period, no SR is generated.

A blackout can be defined for an individual database, a group of multiple databases that reside on different hosts (as in a RAC configuration, for example), or for all targets on a host. The blackout can be scheduled to run immediately or in the future, and to run indefinitely or stop after a specific duration. Blackouts can be created on an as-needed basis, or scheduled to run at regular intervals. If, during the maintenance period, the Oracle Advanced Support Gateway administrator discovers that he needs more (or less) time to complete his maintenance tasks, he can easily extend (or stop) the blackout that is currently in effect.

Creating Database Blackouts

You can use Oracle Advanced Support Gateway to create blackouts both for single database instances and for a clustered database. You can set either single or recurring blackouts.

To create a blackout using the Admin screen:

1. Log on to the Oracle Advanced Support Gateway portal.
The Oracle Advanced Support Gateway screen appears.
2. Under Admin, select **Scheduled Blackouts**.
The Scheduled Blackouts screen appears.

Figure 10–1 Scheduled Blackouts Page

The screenshot shows the 'Scheduled Blackout' page. At the top, there's a header with the Oracle logo and the title 'Scheduled Blackout'. Below the header, it says 'Below is the list of scheduled blackouts'. On the right, there's a 'View History' button. The main area contains a list of blackouts. The first row shows a blackout named 'Blackout desc 2' scheduled for 'Once on 01/10/2016 at 14:57:34' for '1 Database(s)'. The second row shows a blackout named 'd2' scheduled 'Every day at 12:15:04 / Next 28/07/2015 to 28/07/2015 at 13:15:04' for '2 Database(s)'. Each row has a 'Cancel' button, a search bar, and a 'Create Blackout' button. There are also icons for editing and deleting each blackout.

3. Click **Create Blackout**.

The Create Blackout screen appears.

Figure 10–2 Create Blackout Screen

The screenshot shows the 'Create Blackout' screen. At the top, there's a header with the Oracle logo and the title 'Create Blackout'. Below the header, it says 'Use the fields below to schedule blackout for selected databases'. The main area contains several fields: 'Description *' (a text area with a character count of 255), 'Start Date *' (a date/time picker set to 24/07/2015 15:49:53), 'End Date *' (a date/time picker set to 25/07/2015 15:49:53), 'Repeat' (a dropdown menu set to 'None'), 'Database(s) *' (a list with 'LCS12C' and an 'Add' button), and 'Scope' (a checkbox for 'Blackout All Related Targets'). There are also 'Cancel' and 'Create' buttons at the bottom right.

- In the **Description** field, enter a name and a description.
- In the **Start Date** field, specify a date and time for the start of the blackout period.
- In the **End Date** field, specify a date and time for the end of the blackout period.
- (Optional) From the **Repeat** list, select an interval for the blackout to execute. The recurrence values are **Daily**, **Weekly**, **Monthly**. The default is **None**.
- In the **Databases** field, select database targets to add to the blackout list.
(Optional) Click **Add** to choose other targets from the **Select Databases** page.
- (Optional) In the **Scope** field, select the **Blackout All Related Targets** check box to enable all related targets for blackout.
- Click **Create**.

After creating the blackout, you can manage it by, for example, editing the recurrence interval, changing the end date, or by adding further databases to be used in the blackout schedule.

See ["Managing Database Blackouts"](#) for more information about editing scheduled blackouts.

Managing Database Blackouts

You can use Oracle Advanced Support Gateway to view a list of scheduled and completed database blackouts. You can edit existing blackouts, create or extend an existing blackout, or cancel a scheduled blackout.

This section consists of the following topics:

- ? [Viewing Scheduled Blackouts](#)
- ? [Viewing Completed Blackouts](#)
- ? [Editing Blackouts](#)
- ? [Canceling Blackouts](#)

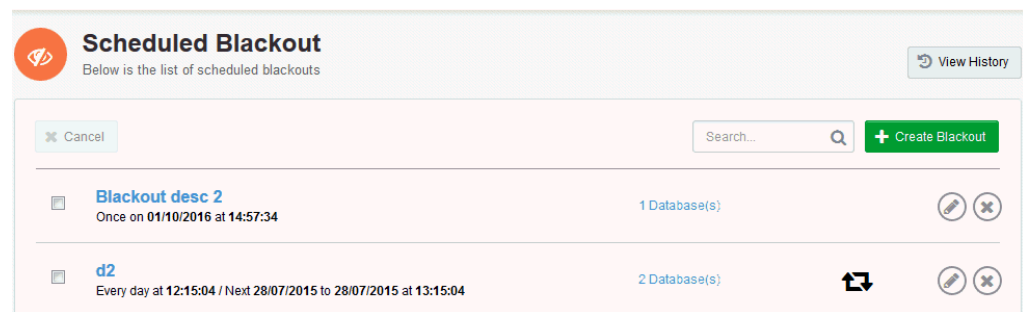
Viewing Scheduled Blackouts

You can use Oracle Advanced Support Gateway to view your scheduled database blackouts.

To use Oracle Advanced Support Gateway to view a blackout:

1. Log on to the Oracle Advanced Support Gateway portal.
The dashboard screen appears.
2. From the top-level **Admin** menu, select **Scheduled Blackouts**.
The Scheduled Blackout page appears.

Figure 10–3 Scheduled Blackout Page



From the list of blackouts, you can search for a particular blackout instance, create a new blackout, edit or cancel an existing blackout, and so on.

Viewing Completed Blackouts

You can use Oracle Advanced Support Gateway to view your database blackout history.

To use Oracle Advanced Support Gateway to view a completed blackout:

1. Log on to the Oracle Advanced Support Gateway portal.
The dashboard screen appears.
2. From the top-level **Admin** menu, select **Scheduled Blackouts**.
The Scheduled Blackouts page appears.

3. Click **View History**.

The Completed Blackouts page appears.

Figure 10–4 Completed Blackouts Page



The screenshot shows the 'Blackout History' page with a search bar and a table of completed blackouts. The table has columns for Description, Start, End, and Databases.

Description	Start	End	Databases
BO Repeat None	14/07/2015 10:00:36	15/07/2015 09:58:46	1
MK Test BO 1	15/07/2015 10:54:50	15/07/2015 10:58:55	1

From the list of completed blackouts, you can search for a particular blackout instance, review the dates between which a blackout occurred, and view the affected databases.

Editing Blackouts

You can use Oracle Advanced Support Gateway to edit an existing database blackout.

To use Oracle Advanced Support Gateway to edit a blackout:

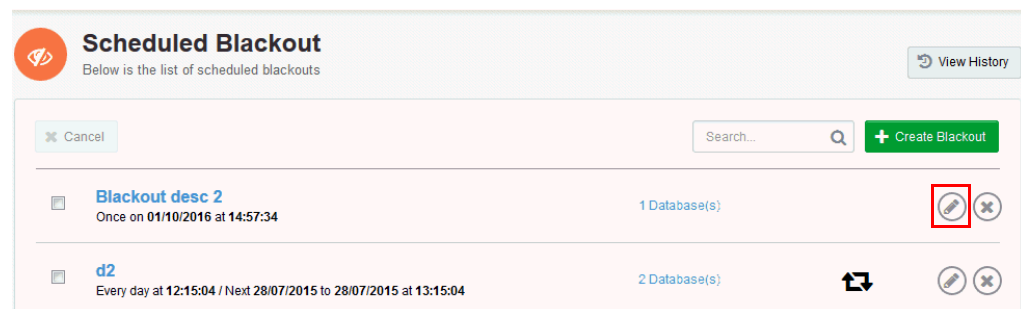
1. Log on to the Oracle Advanced Support Gateway portal.

The dashboard screen appears.






2. From the top-level **Admin** menu, select **Scheduled Blackouts**.

3. For the selected database, click the **Edit** icon as highlighted in [Figure 10–5](#).

Figure 10–5 Editing a Blackout



The screenshot shows the 'Scheduled Blackout' page with a search bar, a 'Cancel' button, and a 'Create Blackout' button. The table lists scheduled blackouts with columns for Description, Start, End, and Databases. The 'Edit' icon (pencil) is highlighted in a red box for the first row.

Description	Start	End	Databases	Actions
Blackout desc 2 Once on 01/10/2016 at 14:57:34			1 Database(s)	 
d2 Every day at 12:15:04 / Next 28/07/2015 to 28/07/2015 at 13:15:04			2 Database(s)	  

The Edit Blackout screen appears.

Figure 10–6 Edit Blackout Screen

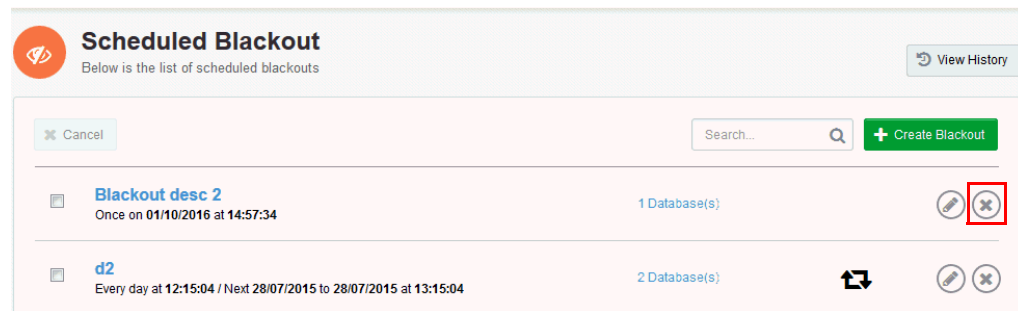
- a. In the **Description** field, enter a name and a description.
- b. In the **Start Date** field, specify a date and time for the start of the blackout period.
- c. In the **End Date** field, specify a date and time for the end of the blackout period.
- d. (Optional) From the **Repeat** list, select an interval for the blackout to execute. The recurrence values are **Daily**, **Weekly**, **Monthly**. The default is **None**.
- e. (Optional) Click **Select** to choose other targets from the **Select Databases** page.
- f. (Optional) In the **Scope** field, select the **Blackout All Related Targets** check box to enable all related targets for blackout.
- g. Click **Save**.

Canceling Blackouts

To cancel a blackout:

1. Log on to the Oracle Advanced Support Gateway portal.
The dashboard screen appears.
2. From the top-level **Admin** menu, select **Scheduled Blackouts**.
The Scheduled Blackouts page appears.
3. For the selected database, click the **Cancel** icon as highlighted in [Figure 10–7](#).

Figure 10–7 Canceling a Blackout



A warning message appears asking you to confirm that you wish to cancel the blackout.

4. Click **Yes** to confirm.

Managing Database Entitlements

This chapter provides information about managing the Oracle Advanced Support Gateway database entitlements.

Note: This chapter applies only to the Patching Service.

This chapter consists of the following sections:

- ? [About Database Entitlements](#)
- ? [About the High Water Mark](#)
- ? [Viewing Database Entitlements](#)

About Database Entitlements

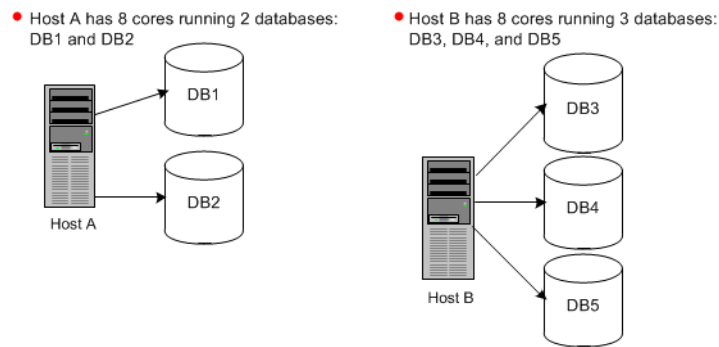
Users and administrators can choose to enable Oracle Advanced Support Gateway on databases at their customer facilities once they ensure they are within the entitled usage limit (measured in database cores per month). Any usage beyond the entitlement limit for the month is then charged separately.

The rules for fair entitlement usage for Oracle Advanced Support Gateway are as follows:

- ? Entitlement usage is based on the number of hardware cores on which databases are running, and is billed on a monthly basis, for example, 60 cores per month.
- ? Entitlement is based on a “use it or lose it” model, that is, there is no carry forward of entitlement from month to month.
- ? Entitlement usage is governed by the High Water Mark. See ["About the High Water Mark"](#).
- ? Entitlement usage metrics are sent to Oracle Advanced Support Platform at regular intervals for consolidated entitlement reporting.
- ? Oracle Advanced Support Portal synchronizes usage across multiple Gateways in accordance with the customer contract.
- ? There is no limit on the number of databases running on a single piece of hardware.

About the High Water Mark

Monthly fair entitlement usage is governed by the “High Water Mark”. To better understand the concept of the high water mark and how it applies to entitlement usage, consider the following example for a customer user with an entitlement of 60 cores, as displayed in [Figure 11–1](#).

Figure 11–1 High Water Mark Example

The customer user network is configured as follows:

- Host A has 8 cores running two databases: *DB1* and *DB2*
- Host B has 8 cores running three databases: *DB3*, *DB4*, and *DB5*

The customer user's usage pattern for August is as follows:

1. On August 1, the user activates *DB1*, *DB3*, and *DB5*. The usage is then calculated on a per-core basis across both hosts as follows:

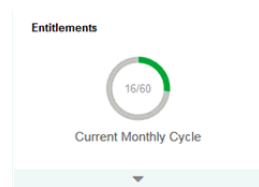
$$8 (DB1) + 8 (DB3, DB5) = 16$$

2. On August 5, *DB2* is activated. As a database (*DB1*) on Host A is already activated, no further usage is added.

Usage remains at 16 (cores).

3. On August 12, *DB3* and *DB5* are deactivated. As both databases are on Host B, and no other database on this host is active, the usage for the day is reduced by 8.

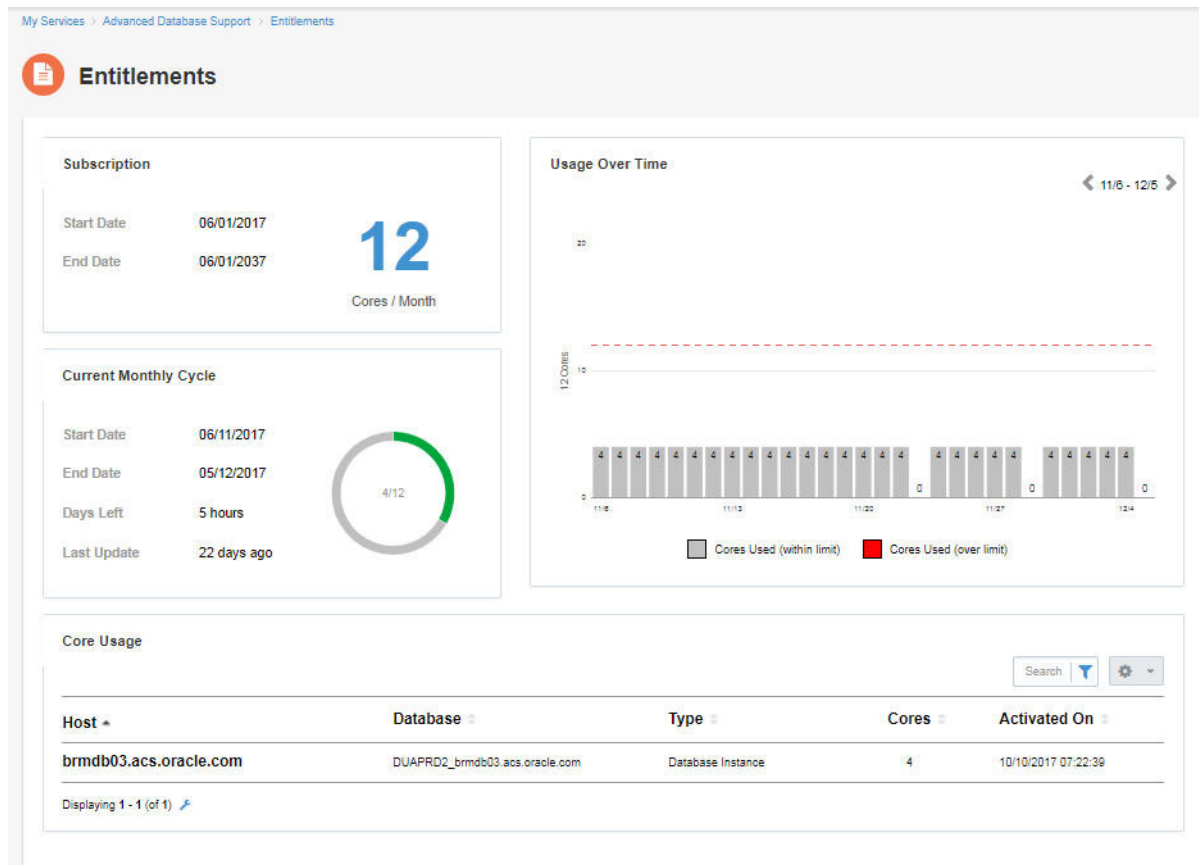
The usage for the day is now 8 (from Host A). However, as the usage for the month to date has already reached 16 (the current high water mark), the entitlement continues to be displayed as 16/60. See [Figure 11–2](#).

Figure 11–2 Entitlements Example

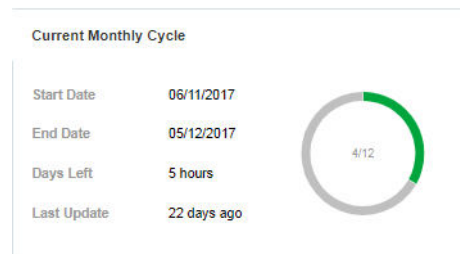
4. Over the remainder of August, the customer user can add further hardware to reach the maximum core usage of 60. However, even if core usage never exceeds the current high water mark of 16, billing is for 60 cores per month.
5. When the August cycle ends, the current usage on the first day of September becomes the initial high water mark for September.

Viewing Database Entitlements

Select the **Entitlements** badge to display your database entitlement contract, based on the core limit for the host database. You can view the current monthly contract cycle in terms of cores used, shown in gray, cores available, shown in green.

Figure 11–3 Viewing Database Entitlements

The sample customer entitlement contract shown is for 12 purchased cores over a one-month duration.

Figure 11–4 Selecting Database Entitlements

You can also view the entitlement usage over time, so that you can determine, for example, the time of month when the demand for cores is highest.

Cores used over the limit are displayed in red.

Setting the HTTP Proxy Server

This chapter provides information about optionally configuring the HTTP Proxy server if http-proxy is required for outbound communication from the Oracle Advanced Support Gateway. Details of the server IP address and port number can be provided by the customer's network administrator.

It includes the following topics:

- [About the HTTP Proxy Server](#)
- [Specifying the HTTP Proxy Server Setting](#)

About the HTTP Proxy Server

Configuration of the HTTP Proxy server is an optional step, but may be required for certain Oracle Advanced Support Gateway customer configurations.

HTTP Proxy server settings can also be configured during Gateway installation. Refer to *Oracle Advanced Support Gateway Installation Guide* for more information.

Specifying the HTTP Proxy Server Setting

To specify the HTTP Proxy server setting:

1. Log in to Oracle Advanced Support Gateway.
The Oracle Advanced Support Gateway Home page appears.
2. From the **Admin** menu, click **Proxy Setting**.
The Configure HTTP Proxy Settings page appears.
3. (Optional) Complete the following parameters on the HTTP Proxy server if http-proxy is required for outbound communication.
 - a. (Optional) If HTTP Proxy mode is required, select the **Enable** check-box.
 - b. In the **IP Address** field, enter your customer IP address.
You can use the hostname or fully-qualified domain name (FQDN) as Oracle Advanced Support Gateway is configured to use Domain Name Service (DNS.)
 - c. In the **Port** field, enter the port associated with the HTTP proxy server.
 - d. (Optional) If authentication is required for the HTTP proxy server, select the **Check if required** check-box.
 - e. In the **Proxy Username** field, enter a valid email address.
 - f. In the **Proxy Password** field, enter the password associated with the user.

4. Complete the configuration as follows:
 - a. Click **Create** to complete the configuration of the HTTP Proxy server, *or*
 - b. Click **Cancel** to exit the Configure HTTP Proxy Settings page.

Specifying a HTTP Proxy During Connectivity Tests

Connectivity Tests (the *Netcheck* feature) are used to validate the required firewall ports and connections between Oracle Advanced Support Gateway and Oracle, which were established during Gateway installation. You can continue to monitor connectivity using Netcheck as required.

In order for Oracle to deliver Oracle Connected Services, the following requirements need to be met:

- ? All monitored devices must be network accessible from the Oracle Advanced Support Gateway.
- ? Oracle must have the level of access to the monitored devices necessary for Oracle to implement and deliver the service.
- ? The Oracle Advanced Support Gateway must be continuously accessible from the Oracle Support Platform using the secure protocols.

The Netcheck feature provides a mechanism to test connectivity between the Gateway and the Oracle Support Platform - external connections, in other words, and also between Oracle Advanced Support Gateway and the customer monitored systems, that is, internal connections.

These tests help to secure and successfully complete the implementation of services running on Oracle Advanced Support Gateway.

You can optionally specify a HTTP proxy if the traffic between the Gateway and the Engineered System is routed through a proxy server (depending on the customer's network configuration).

See ["Specifying a HTTP Proxy."](#)

Managing Server and ILOM Certificates

This chapter describes how to manage and generate server and ILOM certificates for Oracle Advanced Support Gateway.

It includes the following topics:

- 7 [About Server and ILOM Certificates](#)
- 7 [Viewing Server Certificates](#)
- 7 [Managing Server Certificates](#)

About Server and ILOM Certificates

The Oracle Advanced Support Gateway server certificate is a public key certificate. This is a digitally signed statement that binds the value of a public key to the identity of the person, device, or service that holds the corresponding private key. One of the main benefits of certificates is that hosts no longer have to maintain a set of passwords for individual subjects who need to be authenticated as a prerequisite to access. Instead, the host merely establishes trust in a certificate issuer.

The server certificate is valid only for the period of time specified within it; every certificate contains Valid From and Valid To dates, which set the boundaries of the validity period. Once a certificate's validity period has passed, a new certificate must be requested by the subject of the now-expired certificate.

You can use Oracle Advanced Support Gateway to generate new server certificates when required.

Oracle Integrated Lights Out Manager (ILOM) is the service processor embedded on all Oracle's x86 and SPARC servers. Oracle ILOM enables a full in-band management interface and a full out-of-band management interface, which provides a “just like being there” remote management capability. The Oracle Advanced Support Gateway ILOM certificate is a public key certificate.

Oracle ILOM uses self-signed certificates to enable the out-of-the-box use of the SSL and TLS protocols. Whenever possible, replace self-signed certificates with certificates that are approved for use in your environment and signed by a recognized certificate authority. Oracle ILOM supports a variety of methods that can be used to access the digital certificate and private key, including HTTPS, HTTP, SCP, FTP, TFTP, and pasting the information directly into a web browser interface. For more information, refer to *Oracle ILOM Configuration and Maintenance Guide* (see [Additional Oracle ILOM Resources](#)).

Support is available only for Oracle hardware and ILOM version 4.0.0 and above.

Note: You perform the same action for ILOM certificates as for server certificates. Refer to the following sections to view and manage ILOM certificates.

Viewing Server Certificates

The **Server Certificate** page enables you to manage and generate your server certificate.

To view your server certificate information:

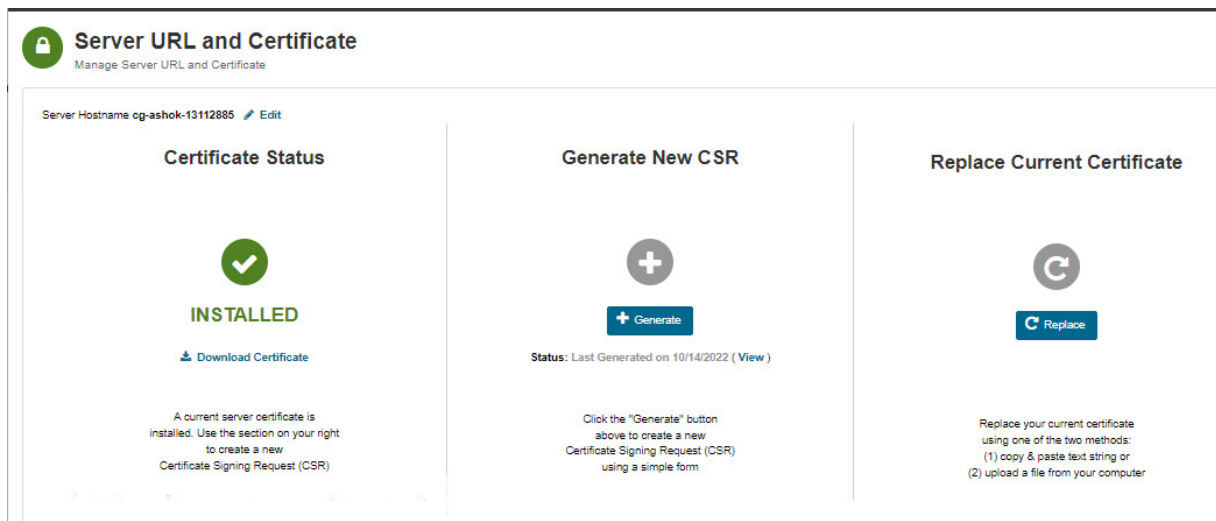
1. Log in to Oracle Advanced Support Gateway.

The Oracle Advanced Support Gateway Home page appears.

2. From the **Gateway** menu, click **Server Certificate**.

The Server Certificate page appears.

Figure 13–1 Server Certificate Page



Viewing Certificate Status

The Server Status section of the **Server Certificate** page enables you to view whether you have a server certificate installed on Oracle Advanced Support Gateway. You can also use the Server Status section to download and review your server certificate.

To view your server certificate status:

1. Log in to Oracle Advanced Support Gateway.

The Oracle Advanced Support Gateway Home page appears.

2. From the **Gateway** menu, click **Server Certificate**.

The Server Certificate page appears.

If a server certificate is installed, an Installed message and corresponding check mark are displayed as shown in [Figure 13–1](#).

If a server certificate is not installed, and you want to install a certificate, see "[Installing Server Certificates](#)".

Managing Server Certificates

There are a number of actions that you can perform on server certificates using Oracle Advanced Support Gateway:

- Downloading server certificates. See "[Downloading Server Certificates](#)".

- 7 Installing server certificates. See ["Installing Server Certificates"](#).
- 7 Generating a certificate signing request. See ["Generating a Certificate Signing Request"](#).
- 7 Replacing the current server certificate. See ["Replacing the Current Server Certificate"](#).

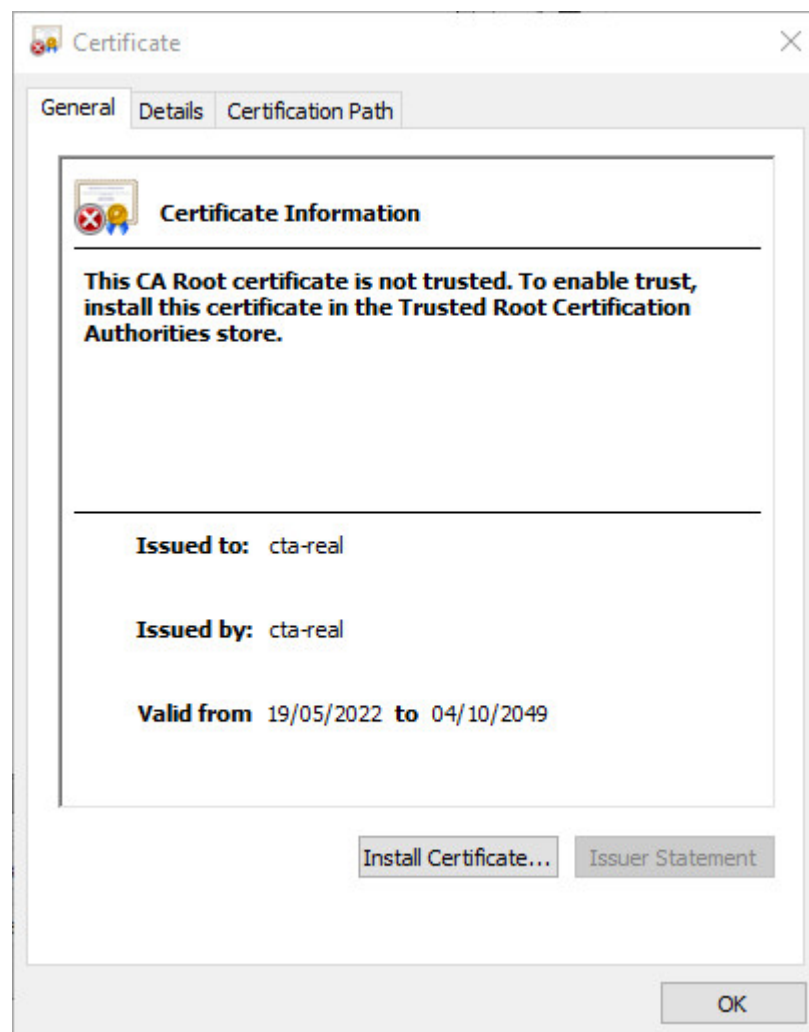
Downloading Server Certificates

You can use the Server Status section of the **Server Certificate** page to download and review your server certificate.

To download your server certificate:

1. Log in to Oracle Advanced Support Gateway.
The Oracle Advanced Support Gateway Home page appears.
2. From the **Gateway** menu, click **Server Certificate**.
The Server Certificate page appears.
3. If a server certificate is installed, click **Download Certificate** and open the file to display the certificate shown in [Figure 13–2](#).

Figure 13–2 Server Certificate



Installing Server Certificates

After downloading the server certificate, you can choose to import it to a certificate store. The wizard helps you to copy certificates, certificate trusts lists, and certificate revocation lists from your disk to a certificate store, which is the system area where certificates are kept.

To install your server certificate:

1. Log in to Oracle Advanced Support Gateway.
The Oracle Advanced Support Gateway Home page appears.
2. From the **Gateway** menu, click **Server Certificate**.
The Server Certificate page appears.
3. If a server certificate is installed, click **Download Certificate** and open the file.
4. On the certificate, click **Install**.
The certificate import wizard Welcome page appears.
5. Click **Next**.
The Certificate Store page appears.
Use this page to allow Windows to automatically select the location for the certificate store, or to enable you to specify another location.
6. Select one of the following options:
 - a. **Automatically select the certificate store based on the type of certificate, or**
 - b. **Place all certificates in the following store**If you select(a), continue to step 7.
If you select(b), continue to step 8.
7. *(For automatic selection of the certificate store)*
Click **Next**.
The Select Certificate Store page appears.
The certificate store is automatically selected.
Continue to step 9.
8. *(For self-selection of the certificate store)*
Click **Browse**.
The Select Certificate Store page appears.
Select the required certificate store.
Click **OK**, and then click **Next**.
9. Click **Finish** to complete the installation of the server certificate.

Generating a Certificate Signing Request

You can use Oracle Advanced Support Gateway to generate a Certificate Signing request (CSR).

A CSR is a block of encrypted text that is generated on the Oracle Advanced Support Gateway server that the certificate will be used on. It contains information that will be included in your certificate such as your organization name, common name (domain name), locality, and country.

To generate a new CSR:

1. Log in to Oracle Advanced Support Gateway.
The Oracle Advanced Support Gateway Home page appears.
2. From the **Gateway** menu, click **Server Certificate**.
The Server Certificate page appears.
3. In the middle pane, Generate New CSR, click **Generate**.
The Server Certificate: Generate CSR page appears.
4. Complete the following parameters to generate a new CSR.
 - a. In the **Server Name** field, enter the fully qualified domain name for your web server.
 - b. In the **Org Unit** field, enter the organization unit.
 - c. In the **Organization** field, enter the exact legal name of your organization. Do not use abbreviated forms of the organization name.
 - d. In the **City** field, enter the name of the city where your organization is legally located.
 - e. In the **State** field, enter the name of the state, county, or region where your organization is legally located. Do not use abbreviated forms of the name.
 - f. In the **Country** field, select the country in which your organization is legally located.
5. Click **Generate** to complete the creation of the CSR.

Replacing the Current Server Certificate

After the end of the validity period for the server certificate, the certificate is no longer considered an acceptable or usable credential. You can use the Certificate Renewal Wizard on Oracle Advanced Support Gateway to replace or renew a certificate issued from a Windows enterprise certification authority (CA) before or after the end of its validity period.

You can replace your current certificate using one of two methods:

- ? Copying and pasting a text string, *or*
- ? Uploading a file from your computer

To replace the current server certificate:

1. Log in to Oracle Advanced Support Gateway.
The Oracle Advanced Support Gateway Home page appears.
2. From the **Gateway** menu, click **Server Certificate**.
The Server Certificate page appears.
3. In the right pane, Replace Current Certificate, click **Replace**.
The Server Certificate: Apply Certificate page appears.
4. In the **Certificate Source** field select one of the methods below.
 - a. **Copy & Paste; paste the text of the certificate, or**
 - b. **File Upload; upload certificate as a file**

If you select(a), continue to step 5.

If you select(b), continue to step 6.
5. *(To copy and paste the text of the server certificate)*

Paste the text of the certificate into the Certificate String field.

Continue to step 7.

6. *(To upload a local certificate)*

Click **Browse**.

Select the required certificate from your local server.

Click **Open**.

7. Click **Apply Certificate** to complete the replacement of the certificate.

Enabling Remote Access to the Oracle Advanced Support Gateway

This chapter provides information about enabling remote VPN access to the Oracle Advanced Support Gateway.

It includes the following topics:

- ? [About the Remote Access Icon](#)
- ? [Enabling Remote Access](#)
- ? [Disabling Remote Access](#)
- ? [Viewing Remote Access History](#)

About Remote Access

Oracle security policies require a VPN between Oracle and the customer so that Oracle can access the customer systems. The Gateway enables the customer to control the firewall settings to determine whether Oracle can log on to the Gateway. The Remote Access icon (a green button) is displayed in the utility menu on the top-right of the Gateway user interface. You can set the duration for allowing remote access to a maximum of 200 minutes, toggle the icon to turn the remote access session on or off, or view a history of remote access control sessions. The default is to allow the connection indefinitely. Remote Access Control functionality is not available for all Oracle Connected Services. Please refer to your Oracle representative for further details.

For more information about Oracle security policy and requirements, see [Oracle Advanced Support Gateway Security Guide](#).

However, in certain limited cases, Oracle Advanced Support Gateway also enables the customer to control remote access by providing the capability to enable and disable VPN connectivity with Oracle.

Note: Remote VPN Access - also referred to as “Green Button” functionality - is not enabled by default and customers that wish to avail of it must first open a Service Request. Please refer to your Oracle representative for further details.

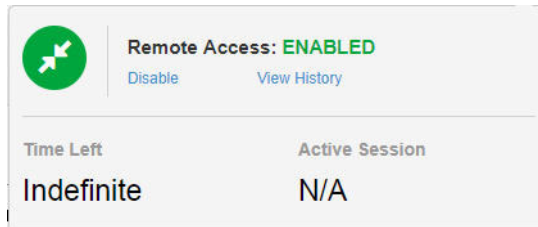
For example, Oracle recommends keeping remote access enabled for smooth delivery of Platinum Services. Not keeping remote access enabled may negatively impact your SLA.

Furthermore, remote VPN Access is not available for all Oracle connected services on Oracle Advanced Support Gateway.

About the Remote Access Icon

The Remote Access icon, also referred to as the *Green Button*, is displayed in the utility section of the navigation menu on the top-right of the Oracle Advanced Support Gateway user interface. See [Figure 14-1](#).

Figure 14-1 Remote Access Icon



The icon is a toggle button that controls VPN connectivity and enables a customer to check VPN connectivity status.

When you click the Remote Access icon, you can enable or disable the remote access session, or view a history of remote access control sessions.

Enabling Remote Access

You can use the Remote Access icon to enable a Remote Access session.

To enable a Remote Access session:

1. Click the Remote Access disabled icon in the utility menu.
2. Select the **Enable** option.

The Gateway VPN Settings page appears. See [Figure 14-2](#).

Figure 14-2 Gateway VPN Settings Page

3. (Optional) Complete the following parameters to specify the VPN duration, and provide a justification for enabling the VPN.
 - a. In the **Duration** field, enter the VPN duration in minutes.
 - b. In the **Justification** field, enter a reason for enabling the VPN.
 - c. Click **Save** to complete the configuration of the VPN.

Note: On subsequent sessions, when you click **Enable**, the saved VPN settings are used by default, and the Gateway VPN Settings page is not displayed.

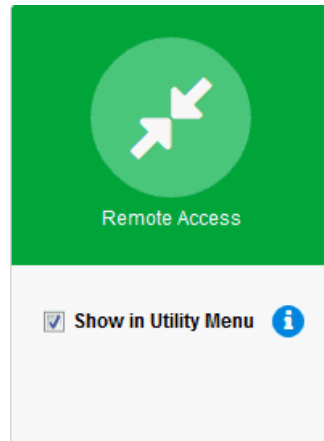
Disabling Remote Access

You can use the Remote Access icon to disable a Remote Access session.

To disable a Remote Access session:

1. Click the Remote Access icon in the utility menu.
2. Select the **Disable** option as shown in [Figure 14-3](#).

Figure 14-3 *Disabling the Remote Access Feature*



The session is disabled after a short period.

Viewing Remote Access History


You can use the Remote Access icon to view a history of remote access control sessions.











To view remote access history:


1. Click the Remote Access icon in the utility menu.
2. Select the **View History** option.

The Remote Access session history table appears, showing the enabling or disabling action, the time at which it was performed, the user that performed the action, as well a justification for the action. See [Figure 14-4](#).

Figure 14–4 Remote Access Session History

**Remote Access Control History**
Detailed information about each remote access session.

Action	Date & Time	User	Justification
 Disabled	09-28-2022 11:35:51	Local setup	
 Enabled	09-28-2022 11:38:15	Local setup	
 Disabled	01-12-2023 06:48:42	Local setup	
 Enabled	01-12-2023 06:50:32	Local setup	
 Disabled	02-07-2023 12:23:37	Local setup	
 Enabled	02-07-2023 12:26:32	Local setup	
 Disabled	03-07-2023 10:29:03	Local setup	
 Enabled	03-07-2023 10:32:02	Local setup	
 Disabled	04-04-2023 08:29:26	Local setup	
 Enabled	04-04-2023 08:31:00	Local setup	

Displaying 1 - 10 (of 146) 

1 / 15 