Oracle® Advanced Support Gateway Installation Guide

Part No: E40642-20
May 2020

ORACLE

Oracle Advanced Support Gateway Installation Guide

Part No: E40642-20

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.

Référence: E40642-20

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

Oracle Advanced Support Gateway Installation Guide

Part No: E40642-20

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.

Référence: E40642-20

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

Contents

Preparing for Installation

This document details how to build Oracle Advanced Support Gateway both in the Cloud (using Oracle Cloud Infrastructure, or OCI) and in an on-premises configuration:

- To deploy the Gateway in the Cloud, see "Deploying the Oracle Advanced Support Gateway on Oracle Cloud Infrastructure" on page 39.
- To install an on-premises Gateway, review the following multi-step process:
  - "Review Host System Requirements for On-Premises Installation" on page 9
  - "Collect Registration Information" on page 15
  - "Obtain the ISO Image From Oracle" on page 16

Changes to the Installation Guide Since the Last Release

This section outlines the principal changes made to *Oracle Advanced Support Gateway Installation Guide* (this guide) since the last release (E40642-19; November 2019.)

- Oracle Advanced Support Gateway can now be installed on a Virtual Machine (VM) that supports installation of Oracle Linux 6.10 and Unbreakable Enterprise Kernel (UEK) 4.x. See "Minimum System Requirements" on page 10.

Review Host System Requirements for On-Premises Installation

This section applies to an on-premises Gateway installation. To review the requirements for deploying the Gateway on the Cloud, see "Deploying the Oracle Advanced Support Gateway on Oracle Cloud Infrastructure" on page 39.

The software gateway can be installed directly onto a server (bare metal install) or within a supported virtual machine. The gateway includes a modified version of Oracle Linux 6.10. It

can be installed in any environment which supports Oracle Linux 6.10 and meets the minimum specifications outlined in the following sections.

Note - Visit the Oracle Linux certified hardware page to see a list of hardware servers that have been certified to run this version of Oracle Linux.

The following topics are covered in this section:

Minimum System Requirements

If you would like to order a server from Oracle for the purpose of running the gateway, Oracle recommends the Oracle Advanced Support Gateway Server X7-2. The gateway software has been certified on this server and has undergone extensive testing and tuning to ensure this configuration achieves the best performance and availability for your service offerings.

This server can be ordered through your Oracle sales representative or Oracle-authorized-distributor.

To order the Oracle Advanced Support Gateway Server X7-2, contact Sales Assistance at +1-888-672-2534.

If you do not wish to purchase the certified server from Oracle, you can use a server or Virtual Machine (VM) that meets the following requirements:

- The Oracle Advanced Support Gateway can be installed in **one of the following ways**:
  - Directly onto any server hardware that is supported by Oracle Linux 6.10 and Unbreakable Enterprise Kernel (UEK) 4.*x*, *or*
  - On Oracle VM, *or*
  - On a VM that supports installation of Oracle Linux 6.10 and Unbreakable Enterprise Kernel (UEK) 4.x. For further information, see MOS Note 417770.1.

    To review the Oracle Support position for Oracle products running on virtualized environments, see MOS Note 249212.1.

  You can view a list of servers that have been certified to run on Oracle Linux from the Oracle Linux certified hardware page at:

  `http://linux.oracle.com/pls/apex/f?p=117:1:489726292744914`

- The server must meet the minimum host system requirements for Advanced Support Gateway installation shown in the following table:

Category	On-premises Minimum	On-premises Recommended	Additional Details
CPU	4 cores	8 cores	The CPU must be 64-bit, x86 architecture (x64 or x86-64). The most common vendors for these processors are Intel and AMD.
Memory	32 GB	48 GB	The recommended configuration supports up to eight (8) full-rack Oracle Engineered Systems (or equivalent products.) The minimum configuration is acceptable for a small installation that provides service for one (1) or (2) full rack Oracle Engineered Systems (or equivalent products.)
Storage	1 disk >=1 TB (if using local storage) 1 disk >=140 GB as local storage minimum. (If using a combination of local and remote storage, the total disk (local + remote) requirements remain 1 TB.) Assume that 15% of a local boot disk will be unusable. That will leave a safe margin of error. See "Gateway Storage Options" on page 12 for more information about usable space.	6 disks >= 600 GB each	■ Multiple disks are recommended to provide fault tolerance using RAID, which is supported by software. Hardware RAID is also supported but not necessary. ■ All disks must be of equal size. A mixture of differently sized disks in the same system is not supported. ■ See "Gateway Storage Options" on page 12 for more detail on the supported disk configurations, including instructions on how to configure network storage (for example, SAN or NAS.) **Note -** Due to compatibility issues, Network File System (NFS) based storage is not supported.
Network	One logical interface. Firewall ports opened.	One logical interface. Firewall ports opened.	Refer to Oracle Advanced Support Gateway Security Guide for details of the specific port and firewall requirements for the gateway to function properly.

Note - Due to incompatibility issues associated with installing the gateway software on Cisco UCS servers, it is recommended that Cisco UCS servers not be used for the gateway hardware.

If the configuration shown in the table is not available, then email acsdirect_us@oracle.com or contact your Oracle sales representative.

If the gateway is required for more than two full rack systems per site, then a custom configuration with more cores, disks, or memory is required and can be configured on the Oracle Store or ordered through your Oracle sales representative or Oracle-authorized distributor. The recommended configuration will support up to eight (8) Oracle Engineered Systems.

Gateway Storage Options

The software gateway automated installation process can work with a wide variety of different disk configurations and make intelligent choices about how to utilize those disks. This topic explains the logic that is used for disk selection, volume creation, and partition creation.

Disk Selection Logic

The installation process makes certain assumptions when choosing the appropriate disk drives to use for installation of the operating system. The assumptions are as follows:

- Any device which is smaller than 100 GB in size is excluded. These are assumed to be removable storage such as USB drives.
- Any device that does not start with `/dev/sd` or `/dev/xvd` is excluded because they are assumed to not be a disk drive.

In the vast majority of cases, these assumptions are correct and the installation proceeds normally. But in certain configurations, the assumptions might be wrong, and the installation fails with a miscellaneous disk error.

If you see an error like the one below during installation, it is likely that your disks are different sizes and this is causing issues trying to setup the RAID. Check to make sure all your disks are the same size and then restart the install process.

Supported Local Disk Configurations

The software gateway supports systems with 1 to 6 disks. The number of disks available during installation affects the level of fault tolerance and performance that can be obtained. The table below describes the way the installer provisions storage for each of the supported disk configurations.

Note - The installer automatically sets up a software RAID configuration if it detects more than one disk. If your system is using a hardware RAID controller, then the RAID volume should appear to the installer as a single disk device to avoid two levels of mirroring, which would negatively affect write performance.

Number of Drives	Minimum Size (Each Drive)	Disk Configuration	Fault Tolerance	Storage Capacity (s = size of each disk)
1	600 GB	All storage on a single disk	None	s
2	600 GB	RAID 1 (mirror)	Can survive a single drive failure.	s
3	600 GB	RAID 1 (mirror or disks 1 and 2) + Spare (disk 3)	Can survive two disk failures	s
4	300 GB	RAID 10 (mirror on disks 1 and 2, mirror on disks 3 and 4, striped across the 2 mirrored sets)	Can survive 1 disk failure in each mirror set. For example: this configuration can survive a failure	2 x s

Number of Drives	Minimum Size (Each Drive)	Disk Configuration	Fault Tolerance	Storage Capacity (s = size of each disk)
			of disks 1 or 2 and 3 or 4, but not 1 and 2 or 3 and 4.	
5	300 GB	RAID 10 (mirror on disks 1 and 2, mirror on disks 3 and 4, striped across the 2 mirrored sets) plus a spare (disk 5).	Can survive one disk failure in each mirror set and one additional failure.	2 x s
6	300 GB	RAID 10 (mirror on disks 1 and 2, mirror on disks 3 and 4, striped across the 2 mirrored sets) plus a spare (disk 5) and a dedicated backup (disk 6).	Can survive one disk failure in each mirror set and one additional failure. Backup disk can be used to recover database should an entire mirror fail.	2 x s

Filesystem Sizes on the ISO

Filesystem sizes on the ISO are set to the following values:

- The `/boot` partition is 2 GB.

  This value should provide ample space for future kernel updates.
- The `/(root)` partition is 20.4 GB.

  This value should prevent any issues with running out of `/`partition space given that many `tmp` files are created on the `/` filesystem.
- *ORAHOME_MAX* (with its value set to 256 GB) has been added.

  If additional disk space is available (beyond the 600 GB minimum requirement specified in "Supported Local Disk Configurations" on page 13), the *ORAHOME_MAX* partition size will be set to the maximum value to provide more space for updates, upgrades, and so on.

Usable Space

This section provides some information on the amount of usable space on the gateway (a 300 GB disk does not have 300 GB of usable space.)

Use the `fdisk` command to view the partition table. There are other unmounted partitions that do not show up in `df` output (perhaps `/swap`, for example). For example, the file system uses some of the disk partition for metadata. Metadata consists of entities like file names, file permissions, which parts of the partition belong to which files, and which parts of the partition are free. This might account for 2% of the partition. Space is also reserved for root and for the master boot record.

For example, on a sample gateway, the `df -k` command shows:

```
Filesystem Size Used Avail Use% Mounted on ----- /dev/mapper/vg_gateway-lv_root
12385456 5556096 6200216 48% /
```

But the `fdisk -l` command shows:

```
Disk /dev/mapper/vg_gateway-lv_root: 12.9 GB, 12884901888 bytes
```

Note - Approximately 4% of the disk storage is not usable. By allocating 15% of the disk as not usable, this should allow sufficient margin of error.

Supported Internet Browsers

Oracle Advanced Support Gateway supports the following internet browsers:

- Mozilla Firefox and Mozilla Firefox ESR (current version; current version-1)
- Google Chrome (current version; current version-1)
- Microsoft Edge
- Safari (on macOS)

Note - Microsoft Internet Explorer 11.*x* is not supported on Oracle Advanced Support Gateway 13.*x* or later releases.

Collect Registration Information

In addition to providing a system that meets the above specifications, collect the information listed in the following table before starting the installation. This information is used during the post-install registration process.

Information Needed	Notes	Your Information
Oracle Single Sign On (SSO) account	The person doing the installation must have an Oracle SSO account to complete the registration. Upon registration, the account name is stored within Oracle's audit logs to provide a record of the user who performed the gateway registration.	

Information Needed	Notes	Your Information
	Following installation, access the Gateway using an Internet-connected Web browser to enable SSO authentication.	
Oracle gateway activation code	The activation code is generated after completion of the Service Implementation Worksheet (SIW). The gateway automatically downloads the gateway hostname, UUID, and other required details during the registration process.	
Primary interface IP address and subnet mask in CIDR notation, for example: 192.0.2.0/24	This is the IP address for the primary interface that is used to manage the gateway. This is provided by the customer's network administrator.	
Default gateway IP address	This is the default gateway IP of the primary interface. This is provided by the customer's network administrator.	
HTTP proxy settings	If http-proxy is required for outbound communication, details of the server IP address and port number, as well as the proxy user name and password, can be entered during gateway installation. These details are provided by the customer's network administrator.	
Gateway user account	The installer uses the *custadmin* account and the default password to initiate the gateway installation. During installation, the installer is prompted to create a new gateway Administrator account (consisting of username, password, and email address). This gateway Administrator account will be used for gateway administration and the *custadmin* account is disabled.	

▼ Obtain the ISO Image From Oracle

You can obtain the ISO image from My Oracle Support by following these steps:

1. **Login to My Oracle Support at `https://support.oracle.com`.**
2. **Click the Patches & Updates tab.**
3. **In the Patch Search box, click Product or Family (Advanced).**

4. **Fill in Product = Oracle Advanced Support Gateway.**

   Select the most recent release in the **Release** field.

5. **Click Search.**

6. **On the search results page, you will be presented with a link that takes you to the download page.**

7. **Click Download on the right side of the page.**

Prepare the ISO Image Install Media

An ISO image is an archive file (also known as a disk image) of an optical disc, composed of the data contents of every written sector of an optical disc, including the optical disc file system. To install the software gateway, you must make the contents of the ISO image available to the machine (physical or virtual) that hosts the gateway.

There are several ways to achieve this, including burning the contents of the ISO image to a DVD drive, which is the Oracle recommended solution as it requires no modifications to the downloaded ISO image.

To burn an ISO image to a DVD for the Windows platform, use one of the following DVD burning utilities:

- A commercial utility such as Roxio or Nero
- A free utility, such as that available for download at Free ISO Burner

You can also prepare the ISO image using ILOM storage redirection. Refer to Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware for further information.

Installing and Activating the Oracle Advanced Support Gateway

Follow these procedures to install and activate the Oracle Advanced Support Gateway:

▼ Install the Operating System Using the ISO image

Follow this procedure to install the Oracle Linux operating system and all the necessary software to establish connections outbound from the Gateway to Oracle through Data Transport Services (DTS), and inbound from Oracle to the Gateway through Oracle Continuous Connection Network (OCCN) VPN connectivity. The steps are the same for a server or virtual machine, so the term "server" is used to represent both options in the following instructions.

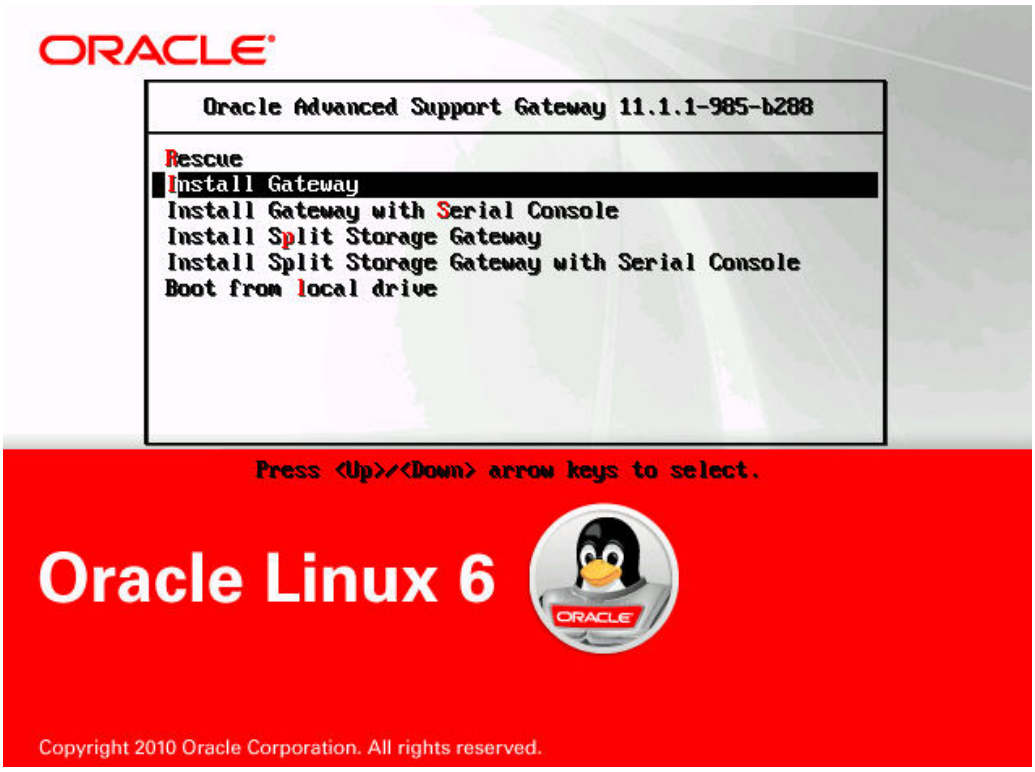
To complete the ISO installation, follow these steps:

Before You Begin Back up your data before re-initializing the disks.

Caution - Possible data loss. Make sure to back up any data currently on the disks before re-initializing the disks.

1. **Boot the server with the ISO image.**

A screen similar to the one shown below appears.

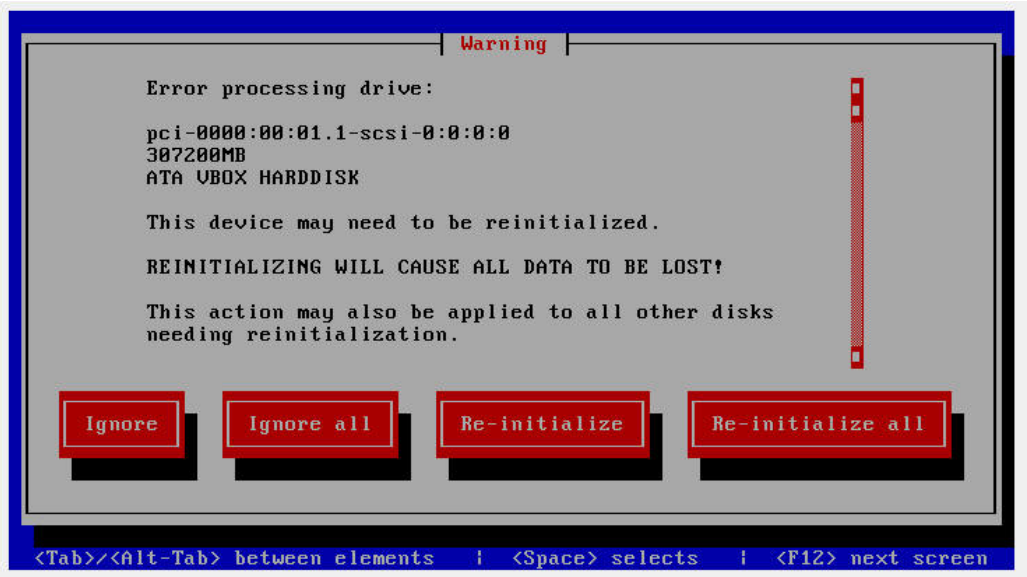


Note - If you require a split storage configuration as outlined above, please refer to your Oracle representative or to Oracle Support to facilitate this arrangement.

2. **To start the installation process, choose the second option, Install Gateway.**

   The installation process takes a few minutes to complete.

If the disk(s) in your system have never been initialized (which is common when using virtualization), you will see a warning message like the one below during the install process.



3. **In this case, choose the Re-initialize all option to proceed with the installation.**

When the installation is complete, a screen similar to the following appears.

4. **Before rebooting the server, eject or unmount the install media so that the server boots the newly installed operating system.**

5. **Press Enter to reboot the server.**

6. **Once the server has rebooted, proceed to the Gateway configuration in the following section.**

▼ Register the Gateway With Oracle

During this portion of the installation process, you are guided through a series of questions to collect the necessary information to connect to Oracle and register the Gateway. You will need console access to complete the following steps.

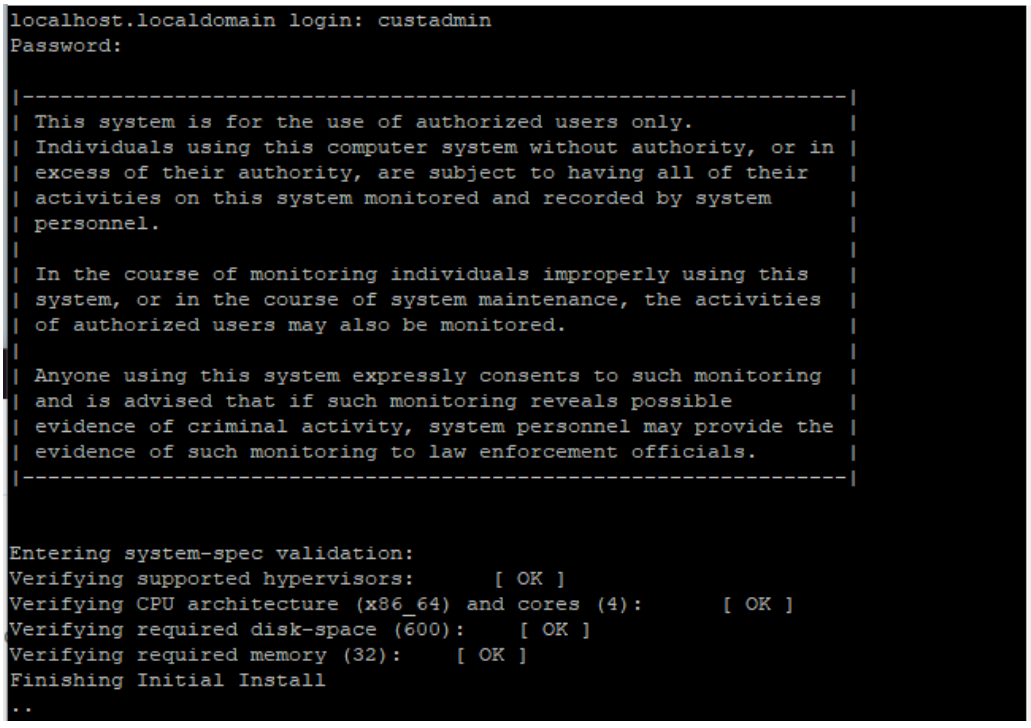
1. **Reboot the server as instructed in the previous section.**

The login screen appears.

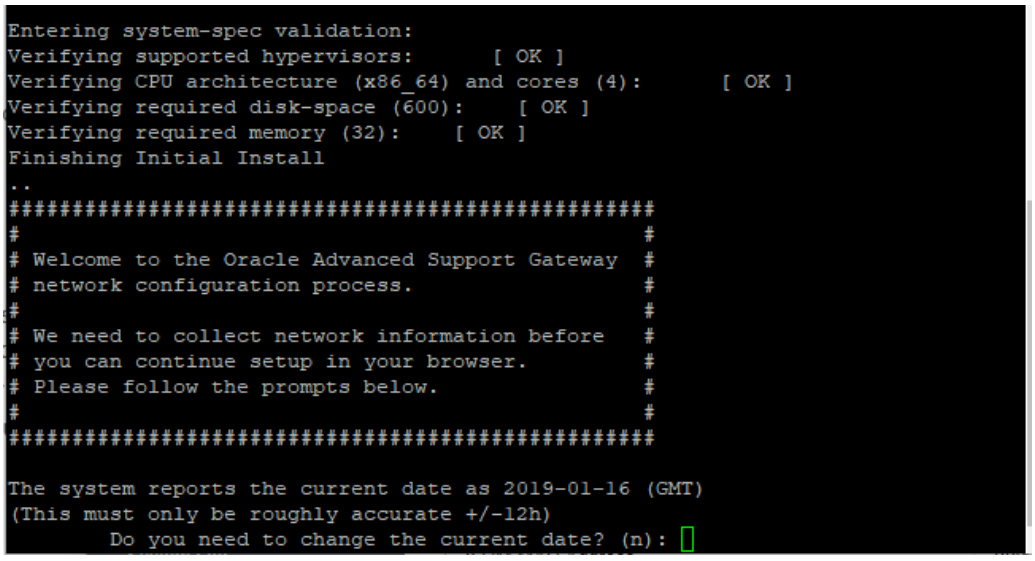
2. **Log in using the default administrator account:**

   - login: **`custadmin`**
   - password: **`install`**

   Upon successful login, you will see the message `Finishing Initial Install`, along with a series of dots to indicate the install progress. This step can take several minutes.

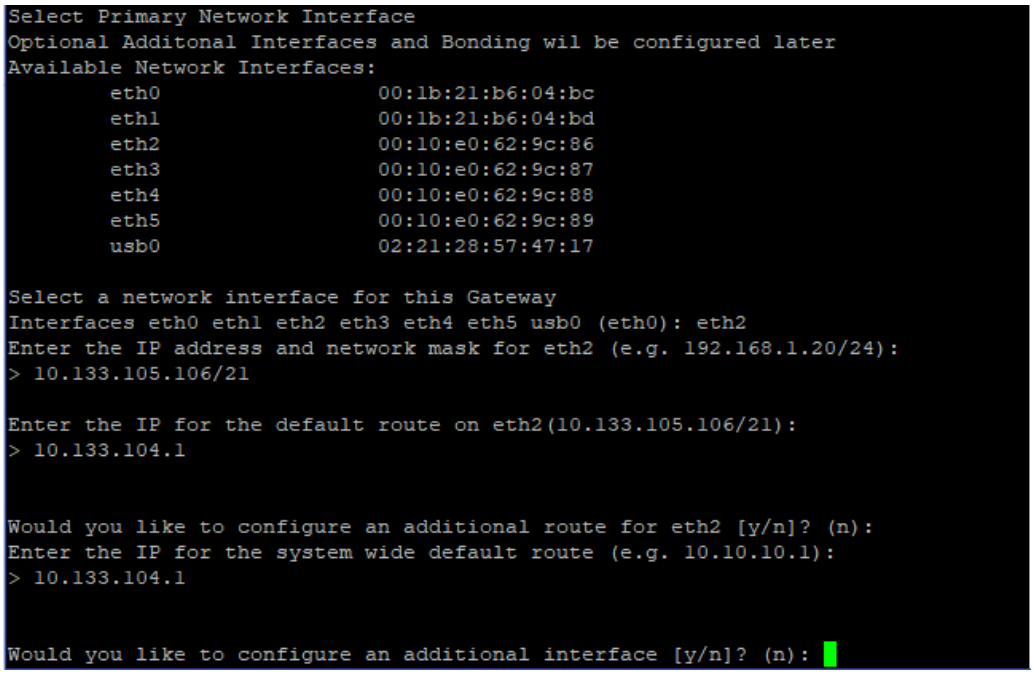


When Step 2 is complete, a screen displaying the following welcome message appears:



3. **Answer the questions with the information collected in the previous sections of this document.**

The following screen shot shows sample answers for each question.



To add a second (or subsequent) interface, enter **y** and continue using the prompts. As the required inputs are equivalent to those for the first interface, repeat for each interface you wish to configure.

Note - In the event of adding an additional interface, *eth0* remains the primary interface for external communication to and from Oracle.

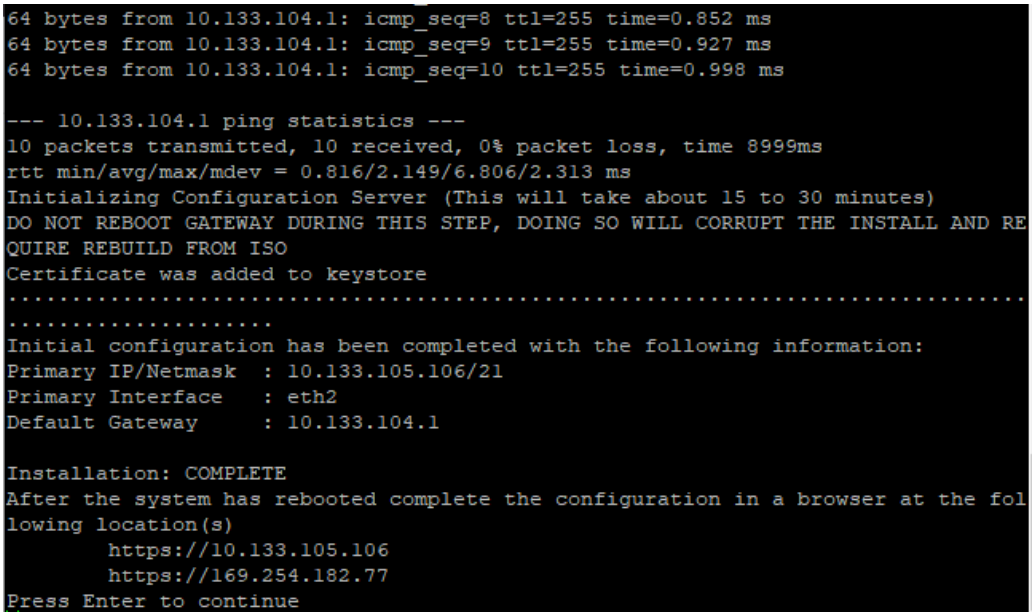
Once you have filled in all the registration information, the installer applies and tests all the configuration information. This will take several minutes. When it is complete, you will see a message indicating configuration was successful.

4. **After all network configuration has been completed, the Gateway performs a test against the default network IP address.**

   Once this test is successful, the Gateway completes the initial configuration. This operation takes between 45-60 minutes. Do not restart the Gateway during this step.

5. **Once the Gateway configuration is complete, a summary of the configuration information is displayed.**

   The following screen shot shows the installation complete message.



   After the installation complete message displays, reboot by pressing **Enter**, and point your web browser at the Gateway IP address (after rebooting.)

Note - If you encounter any installation issues, or the installation procedure fails for any reason, please contact your Installation Engineer. For example, Platinum customers should contact the Platinum Implementation Engineer using the Platinum Implementation Service Request (PISR.)

---

6. **After the Gateway reboots, continue the activation through your web browser.**

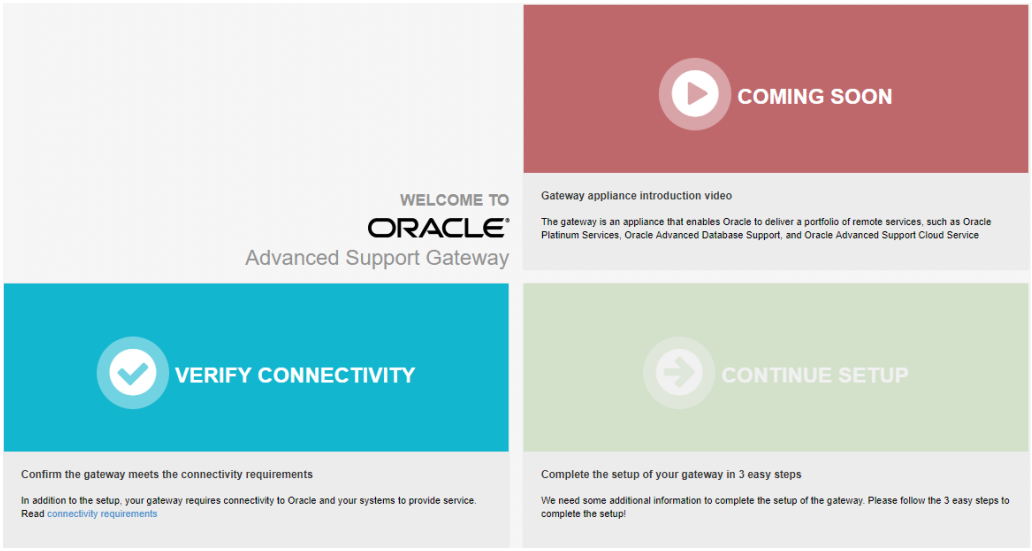
▼ Activate the Gateway

This section provides information about activating the Oracle Advanced Support Gateway. After the Gateway is installed at the customer premises, you can use the Gateway activation code to deploy an activation wizard to configure the Gateway.

During this activation process, you are guided through a series of screens to collect the necessary information to activate the Gateway and create a user account. You will need to access the Gateway portal using your browser to perform the configuration and registration steps.

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

   The welcome screen appears.



   Use the screen to:

   - First verify external connectivity to Oracle.
   - Begin the Oracle Advanced Support Gateway activation process by providing information.

   Note - The Oracle Advanced Support Gateway video feature is not available in this release.

2. **Verify external connectivity to Oracle via the customer firewall.**

   Click **Verify Connectivity** on the Welcome screen.

The following screen appears.

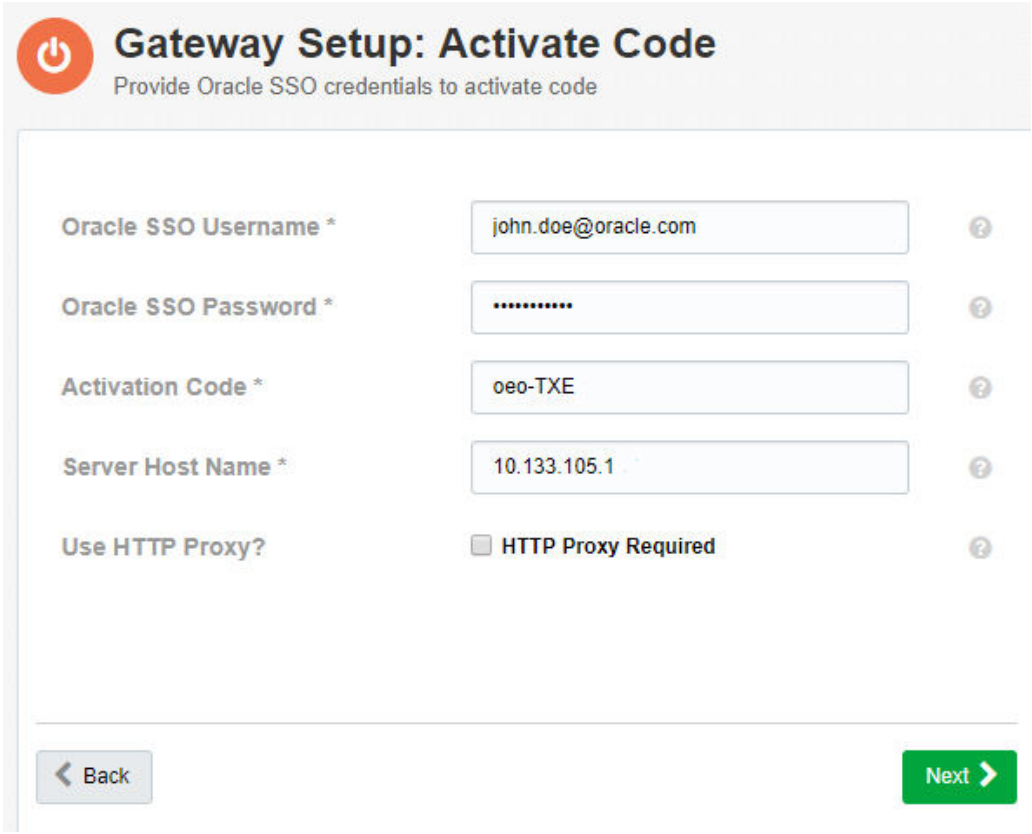
3. **Use the code to activate the Gateway.**

   The Gateway activation code is provided after you complete the Service Implementation Worksheet (SIW), and is sent by email. Activation codes are Gateway-specific and are generated only for new Gateways. Each new Gateway requires a new activation code.

   Tip - For more information about the Service Implementation Worksheet (SIW), refer to the SIW guides for Platinum Services and Advanced Database Support on the Gateway documentation page.

   Select **Continue Setup** to continue with Gateway configuration and registration steps.

The Activate Code screen appears.



Create the customer administration account by providing user credentials to activate the code:

- In the **Oracle SSO Username** field, enter your Oracle user name.
- In the **Oracle SSO Password** field, enter the password associated with your Oracle user name.
- In the **Activation Code** field, enter the code provided when you completed the SIW.
- In the **Server Host Name** field, enter the name of the server host.

Optionally, the user can configure the HTTP proxy settings on this screen.

If you select the **HTTP Proxy Required** checkbox, complete the following fields:

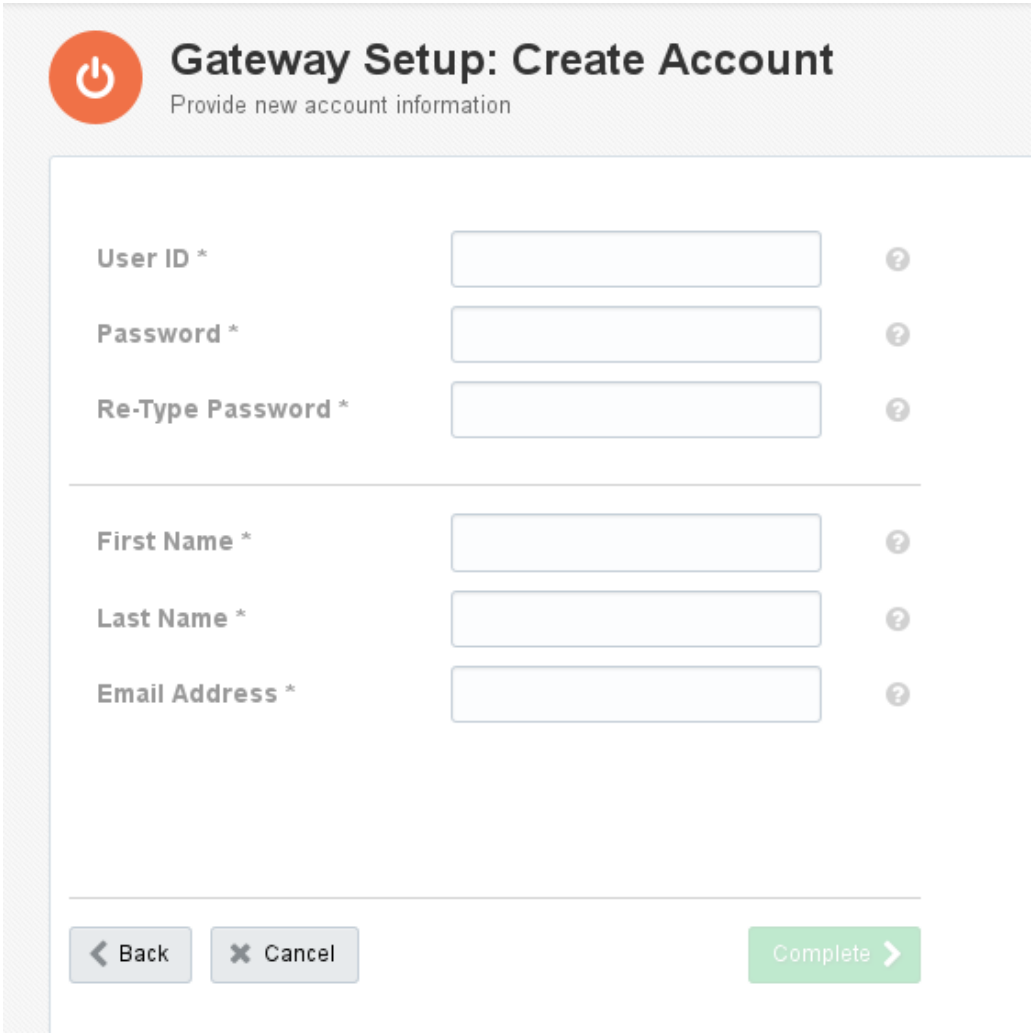
- In the **Server** field, enter your customer IP address. Do not use the hostname or fully-qualified domain name (FQDN) because the Gateway is not yet configured to use Domain Name Service (DNS.)
- In the **Port** field, enter the port associated with the HTTP proxy server.
- In the **Proxy Username** field, enter the name of the HTTP proxy server user.
- In the **Proxy Password** field, enter the password associated with the HTTP proxy server user.

Then, click **Next**.

The activation wizard validates and registers all of the configuration information by connecting to the VPN and installing the required software. After Gateway activation and setup is complete, the Service summary is displayed.

The Create Account screen appears. A new Gateway Administrator account is required for Gateway administration (at which point the *custadmin* account is disabled.)

The user is prompted to supply user ID, initial password, name, and email address (for password maintenance.)



4. Create the user account.

Create the user account by providing user credentials:

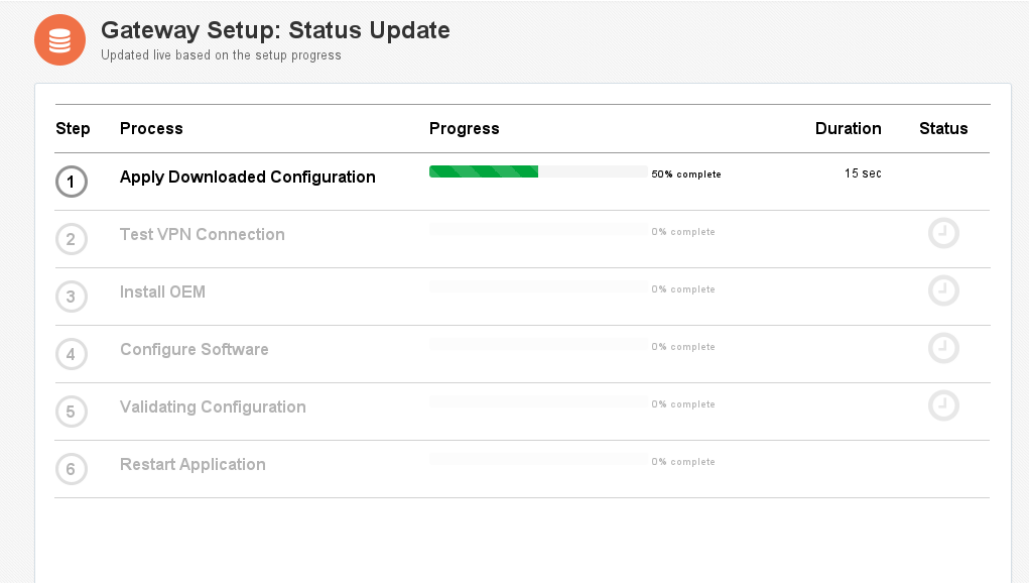
- In the **User ID** field, enter a unique identifier for the user.

- In the **Password** field, enter the password associated with the new user.
- In the **Re-type Password** field, re-enter the password associated with the new user.
- In the **First Name** field, enter the first name of the user.
- In the **Last Name** field, enter the first name of the user.
- In the **Email Address** field, enter the email address of the user. This is used for password reset or recovery.

After the gateway installation is completed, the user has the option of resetting the password or adding more users using the Gateway Portal.

After the installer completes the code activation and new account steps, the Gateway automatically resumes the build and activation process. The Gateway updates the configuration process in a series of steps that are executed serially, and must be completed before the Gateway becomes fully active.

The Status Update screen appears. The Gateway automatically resumes the build and activation process and updates status on the fly.



5. **Apply the downloaded configuration.**

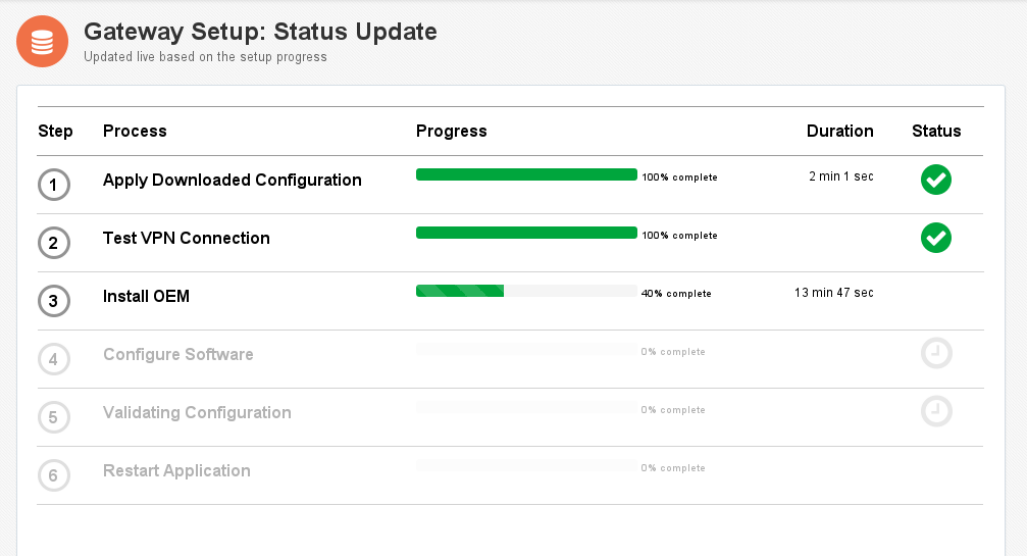
   Network settings are updated and the Gateway is registered with Data Transport Service (DTS.)

6. **Verify the external connection to Oracle.**

The Gateway generates the VPN password and attempts to establish the VPN connection. Typically, this process should take 5-10 minutes. The Gateway tries continuously until the VPN becomes active. If it fails, the user should determine whether the Gateway is able to communicate with Oracle VPN infrastructure, or test network connectivity.

Note - If this is an IPSec configuration, this step will fail. To continue this installation, contact your Oracle representative, for example, your Platinum Implementation Engineer using the Platinum Implementation Service Request.

The Status Update screen appears. The Gateway automatically resumes the installation and configuration of the software.

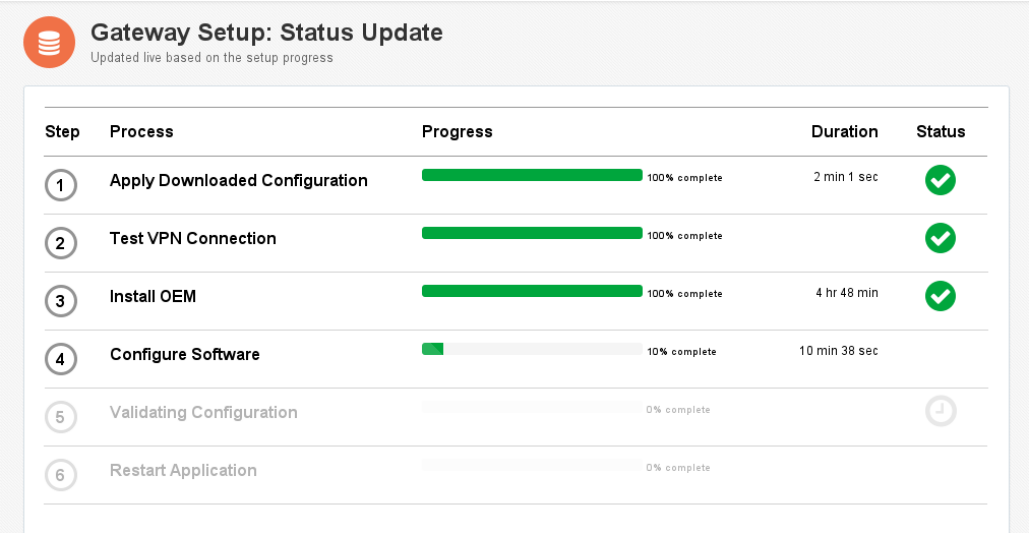


7. Install Oracle Enterprise Manager (OEM.)

Oracle Enterprise Manager (OEM) is downloaded via the internet and installed during the installation of the Gateway. The installation process also ensures that the latest database and OEM patches are applied before the Gateway goes into production. The OEM installation process takes several hours to complete.

Note - Gateways shipped from a factory come with a pre-imaged OS and are pre-loaded with OEM. For Gateways where the customer installs using the ISO from My Oracle Support (MOS), OEM is not present.

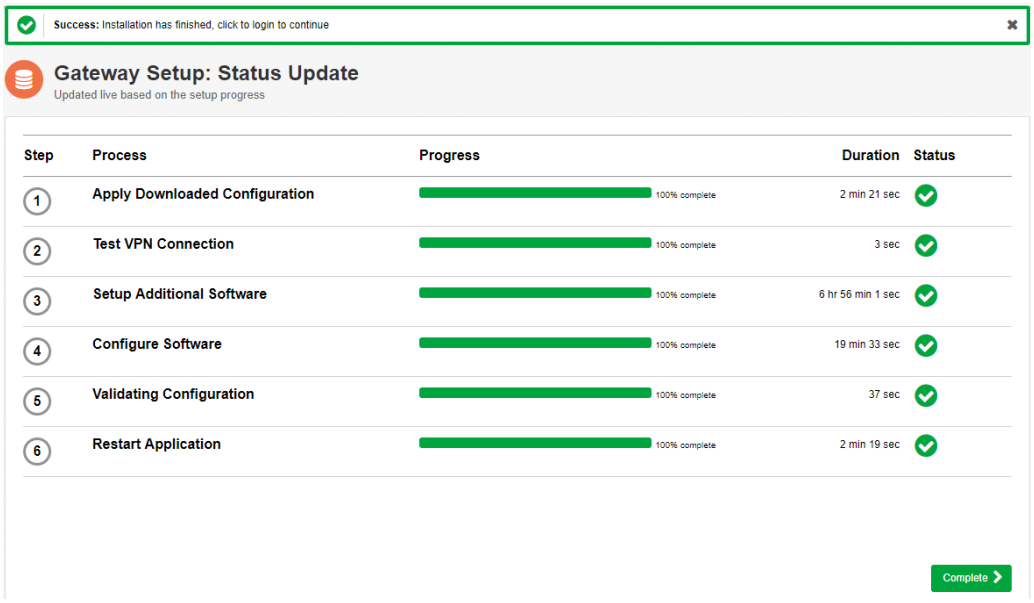
The Status Update screen appears. The software is configured to ensure the Gateway is ready for service.



8. **Configure software.**

The installer configures the Gateway software and ensures that the latest database patches are applied before the Gateway goes into production. This process takes several hours to complete.

The Status Update screen appears. The software configuration is validated to ensure the Gateway is ready for service following a restart.

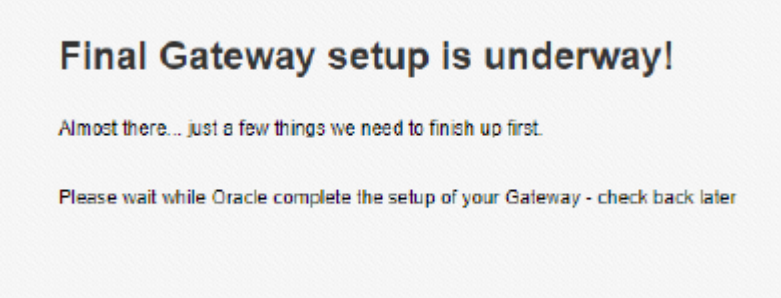


Note - If activation fails, the user can:

- Click **Try Again** to attempt to validate the configuration, *or*
- Contact Oracle Support (or the customer TAM.)

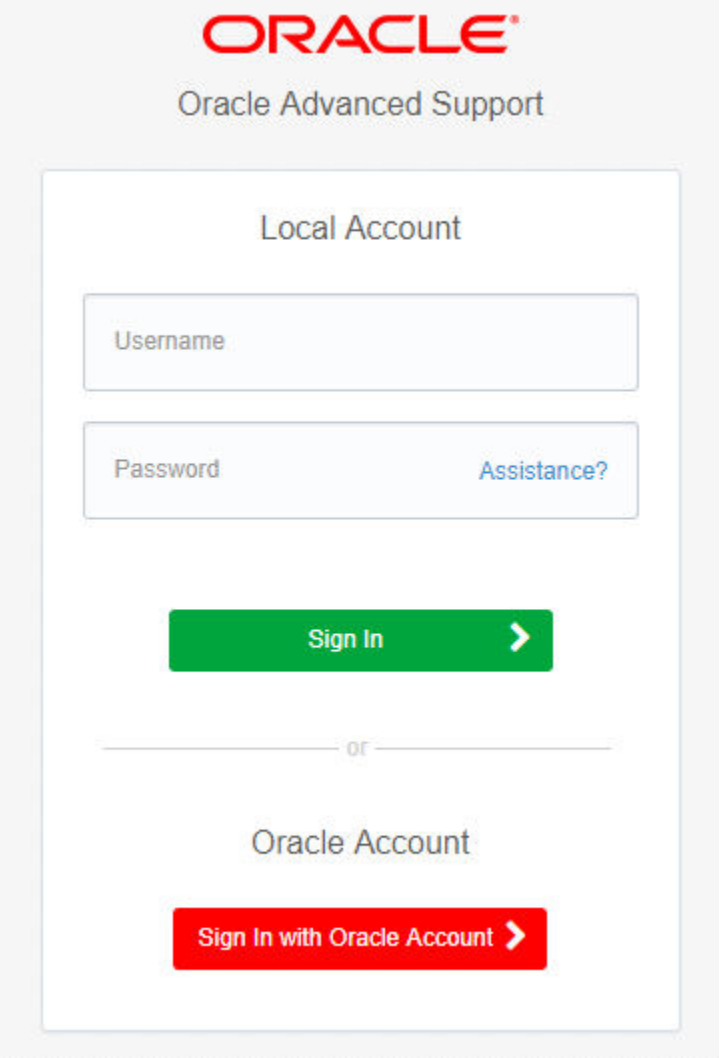
9. **Click Complete.**

A message is displayed confirming that the final steps in the Gateway setup are underway. This may take some time.



After the configuration is validated successfully, the system restarts.

10. **Access the Gateway.**



To access the Gateway using a Web browser, use one of the following methods:

- Enter the username and password for your local account, *or*
- Click **Sign In** to enter your new login credentials provided during installation

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.

Then, perform the following tasks:

- Navigate to https://*GATEWAY_IP_ADDRESS* where *GATEWAY_IP_ADDRESS* is the IP address assigned to the physical interface of the Gateway. Where two interfaces are used, you need to reference the internal interface. This is the IP address which will communicate internally.
- Log on to the portal. Use the customer administrator account configured at installation time (see the *Gateway user account* in "Collect Registration Information" on page 15) or any other user with the customer administrator role.

The All Services page appears.

That completes the installation process.

Deploying the Oracle Advanced Support Gateway on Oracle Cloud Infrastructure

This section applies to deployment of Oracle Advanced Support Gateway on Oracle Cloud Infrastructure (OCI.) To review the requirements for installing the Gateway in an on-premises Gateway configuration, see "Review Host System Requirements for On-Premises Installation" on page 9.

To deploy the Gateway on OCI, review the following multi-step process:

System Requirements for Cloud Deployment

The server must meet the minimum host system requirements for Advanced Support Gateway deployment on Oracle Cloud Infrastructure shown in the following table:

Category	Cloud (Oracle Cloud Infrastructure) Recommended	Additional Details
CPU	4 OCPU	
Memory	60 GB **Note -** This corresponds to *VM.Standard2.4*. For more information on this VM shape, see this document.	The recommended configuration supports up to eight (8) full-rack Oracle Engineered Systems (or equivalent products.) The minimum configuration is acceptable for a small installation that provides service for one (1) or (2) full rack Oracle Engineered Systems (or equivalent products.)
Storage	1 TB minimum, 2 TB recommended.	
Network	1 logical interface. Firewall ports opened.	Refer to Oracle Advanced Support Gateway Security Guide for details of the specific port and firewall requirements for the gateway to function properly.

Customer Requirements for Deploying the Gateway on Oracle Cloud Infrastructure

Before setting up Oracle Advanced Support Gateway to connect to and monitor your assets on Oracle Cloud Infrastructure (OCI), you will need to consider which of the following deployment scenarios best applies to your network configuration. Each customer has a unique network topology, specific security requirements, particular access control policies, and so on. Consequently, Oracle needs to understand prior to deployment what specific information is required from the customer based on their configuration requirements.

Scenario 1: Deploying the Gateway Using Shared Services on a Customer-Managed Network

This deployment scenario is defined as follows:

TABLE 1 Deploying the Gateway Using Shared Services on a Customer-Managed Network

Gateway location:	Customer tenant
Gateway compartment:	Shared services
Network managed by:	Customer
VCN location:	Customer compartment
Customer compartment:	Shared services compartment

▼ Scenario 1 Deployment Requirements

Make sure you meet the following requirements for successfully deploying the gateway in this scenario:

1. **Import the gateway image to the customer tenant using the instructions provided below.**

2. **Allocate a new compartment for Oracle shared services (if this step is not already completed.)**

3. **Create a new subnet in the customer VCN in the shared services compartment where the gateway will reside (/29 will suffice.)**

4. **Configure the customer VCN to allow traffic to the specified addresses by generating a security list based on the firewall requirements listed in Oracle Advanced Support Gateway Security Guide.**

5. **Set up an internet gateway or NAT gateway to allow traffic to the internet on the customer VCN.**

Note - If you opt to use a NAT gateway, Oracle assumes that the customer is responsible for building and activating the gateway up to the point when SSLVPN is connected.

---

6. **Generate a route table incorporating rules pointing the required traffic to the internet on the customer VCN.**

7. **(Optional) Set up a local peering gateway and establish a peering connection if the customer has assets in a separate VCN.**

Scenario 2: Deploying the Gateway Using Shared Services on an Oracle-Managed Network

This deployment scenario is defined as follows:

TABLE 2 Deploying the Gateway Using Shared Services on an Oracle-Managed Network

Gateway location:	Customer tenant
Gateway compartment:	Shared services
Network managed by:	Oracle
VCN location:	Shared services compartment

Gateway subnet location:	Shared services compartment
Location of customer subnet(s):	Customer compartment(s)

Scenario 2 Deployment Requirements

Make sure you meet the following requirements for successfully deploying the gateway in this scenario:

1. **Import the gateway image to the customer tenant using the instructions provided below.**
2. **Allocate a new compartment for Oracle shared services (if this step is not already completed.)**
3. **Create a new subnet in the shared services VCN where the gateway will reside (/29 will suffice.)**
4. **Place customer assets in other subnets on the shared services VCN and/or in the customer 's own VCN.**
5. **Configure the customer VCN to allow traffic to the specified addresses by generating a security list based on the firewall requirements listed in Oracle Advanced Support Gateway Security Guide.**
6. **Set up an internet gateway or NAT gateway to allow traffic to the internet on the customer VCN.**

   Note - If you opt to use a NAT gateway, Oracle assumes that the customer is responsible for building and activating the gateway up to the point when SSLVPN is connected.

7. **Generate a route table incorporating rules pointing the required traffic to the internet on the customer VCN.**
8. **(Optional) Set up a local peering gateway and establish a peering connection if the customer has assets in their own VCN.**

Scenario 3: Deploying the Gateway on a Wholly Customer-Managed Network

This deployment scenario is defined as follows:

TABLE 3 Deploying the Gateway on a Wholly Customer-Managed Network

Gateway location:	Customer tenant
Gateway compartment:	Provided by the customer
Network managed by:	Customer
VCN location:	Customer compartment
Gateway subnet location:	Customer compartment

▼ Scenario 3 Deployment Requirements

Make sure you meet the following requirements for successfully deploying the gateway in this scenario:

1. **Import the gateway image to the customer tenant using the instructions provided below.**
2. **Create a new subnet in the customer compartment where the gateway will reside (/29 will suffice.)**
3. **Configure the customer VCN to allow traffic to the specified addresses by generating a security list based on the firewall requirements listed in Oracle Advanced Support Gateway Security Guide.**
4. **Set up an internet gateway or NAT gateway to allow traffic to the internet on the customer VCN.**

Note - If you opt to use a NAT gateway, Oracle assumes that the customer is responsible for building and activating the gateway up to the point when SSLVPN is connected.

---

5. **Generate a route table incorporating rules pointing the required traffic to the internet on the customer VCN.**

6. **(Optional) Set up a local peering gateway and establish a peering connection if the customer has assets in a separate VCN.**

Configuring the Gateway on Oracle Cloud Infrastructure

This section provides instructions on setting up Oracle Advanced Support Gateway on Oracle Cloud Infrastructure (OCI). The configuration procedure consists of the following sequential tasks:

▼ Import the Gateway Custom Image

Follow this procedure to import the gateway custom image from Oracle using the URL provided. By importing the image in this way, you copy the required *.vmdk* image directly from the Oracle OCI tenant using a secure URL created by Oracle in OCI.

Tip - The URL is in a format look similar to the following: *https://objectstorage.us-phoenix-1.oraclecloud.com/p/gnoqkwdxaVhUTJ1KB5-p6kZD5BHzqtADVZfYFdMOawY/n/oracleacs/b/newoasgbucket/o/GW11.1.1-985-b288.UEFI-UEK4.vmdk.*

To import the custom image using the OCI console, perform the following steps in the OCI web user interface:

1. **Open the navigation menu.**
   Under **Core Infrastructure**, go to **Compute** and click **Custom Images**.

Note - For more information, refer to the relevant OCI documentation here.

---

2. **Click Import Image.**

3. **Select the compartment name you want to import the image to.**
4. **Enter a name for the image.**
5. **Specify the Object Storage URL where the image is stored. You need to specify the pre-authenticated request URL provided.**
6. **Select the image format, .*vmdk*.**
7. **Select EMULATED MODE.**
8. **Ignore the other fields (there is no requirement to add tags.)**
9. **Click Import Image.**

   Once you click **Import Image**, you'll see the imported image in the **Custom Images** list for the compartment, with a status of **IMPORTING**. Once the import completes successfully, the status will change to **AVAILABLE**. If the status does not change, or no entry appears in the **Custom Images** list, the import failed. If the import failed, make sure you have read access to the Object Storage object, and that the object contains a supported image.

▼ Create the OCI Compartment Where the Gateway Will Reside

(Optional) Follow this procedure to create the OCI compartment where the gateway will reside.

Note - This procedure may not be required for certain customers. For example, customers may opt to use an existing compartment rather than create a new instance.

To create the OCI compartment, perform the following steps in the OCI web user interface:

1. **Open the navigation menu.**

   Under **Governance and Administration**, go to **Identity** and click **Compartments**.

Note - For more information, refer to the relevant OCI documentation here.

---

2. **Click Create Compartment.**
3. **Enter the following:**

   Name: Enter a name for the gateway compartment.

Description: Enter a description (required), for example: "Compartment for deploying the gateway".

4. **Click Create Compartment.**

   Your compartment is displayed in the list.

5. **Switch to your new compartment by selecting it from the Compartment list on the left side of the Console.**

▼ Create the VCN

(Optional) Follow this procedure to create the VCN.

Note - This procedure may not be required for certain customers. For example, customers may opt to use an existing VCN rather than create a new instance.

To create the OCI VCN, perform the following steps in the OCI web user interface:

1. **Open the navigation menu.**

   Under **Networking**, go to **Virtual Cloud Networks**.

Note - For more information, refer to the relevant OCI documentation here.

---

2. **Click Create Virtual Cloud Network.**

3. **Enter the following:**

   Name: Enter a name for your cloud network. Avoid entering confidential information.

   Create in Compartment: This field defaults to your current compartment. Select the compartment you want to create the VCN in, if not already selected.

   Select **Create Virtual Cloud Network Only**.

   Specify the CIDR block.

Note - The selected CIDR block must not overlap with any of your customer's networks.

   Leave the remaining options alone.

4. **Select Create Virtual Cloud Network.**

A confirmation page displays the details of the cloud network that you just created.

Create the Subnet

(Optional) Follow this procedure to create the subnet. This procedure follows from “Create the VCN” on page 46.

Note - This procedure may not be required for certain customers. For example, customers may opt to use an existing subnet rather than create a new instance.

To create the OCI subnet, perform the following steps in the OCI web user interface:

1. **While viewing the VCN, click Create Subnet.**

Note - For more information, refer to the relevant OCI documentation here.

2. **Enter the following:**

Name: Enter a name for the gateway VCN subnet. The name doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.

Regional or Availability Domain-Specific: Select **Regional** (recommended), which means the subnet spans all availability domains in the region. Later when you launch an instance, you can create it in any availability domain in the region.

CIDR Block: A single, contiguous CIDR block within the VCN's CIDR block. For example: *172.16.0.0/24*. You cannot change this value later.

Route Table: Select the default route table.

Private or public subnet: Select **Public Subnet**, which means instances in the subnet can optionally have public IP addresses.

Use DNS Hostnames in this Subnet:This option is available only if you provided a DNS label for the VCN during creation. If you want this subnet's instances to have DNS hostnames (which can be used with the built-in DNS capability in the VCN), select the check box for **Use DNS Hostnames in this Subnet**. Then you may specify a DNS label for the subnet, or the Console will generate one for you. The dialog box will automatically display the corresponding DNS Domain Name for the subnet.

DHCP Options: Select the default set of DHCP options.

Security Lists: Make sure the default security list is selected (the default).

Tags: Leave as is. You can add tags later if you want.

3. **Click Create Subnet.**
   Your compartment is then created and displayed on the **Subnets** page.

Create an Internet Gateway to Allow Traffic to the Internet

(Optional) Follow this procedure to create an internet gateway to allow traffic to the internet.

Note - This procedure may not be required for certain customers. Some customers may opt to use a NAT gateway instead (but there can then be no inbound connectivity from the Internet until SSLVPN is connected.)

To create the internet gateway, perform the following steps in the your new compartment:

1. **While viewing the VCN, under Resources, click Internet Gateways.**

Note - For more information, refer to the relevant OCI documentation here.

---

2. **Click Create Internet Gateway.**

3. **Enter the following:**
   Name: Enter a name for the internet gateway. The name doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API). Avoid entering confidential information.
   Create in Compartment: Leave as is.
   Tags: Leave as is. You can add tags later if you want.

4. **Click Create Internet Gateway.**
   Your compartment is then created and displayed on the **Internet Gateways** page. It's already enabled, but you must add a route rule that allows traffic to flow to the gateway.

Update the Default Route Table for the VCN

Follow this procedure to update the default route table for the VCN to direct traffic to:

- Other subnets containing customer assets;
- The internet.

The default route table starts out with no rules. In this procedure you add a rule that routes all traffic destined for addresses outside the VCN to the internet gateway. The existence of this rule also enables inbound connections to come from the internet to the subnet, through the internet gateway. You use security list rules to control the types of traffic that are allowed in and out of the instances in the subnet (see the next task).

No route rule is required in order to route traffic within the VCN itself.

To update the default route table for the VCN, perform the following steps in the your new compartment:

1. **While viewing the VCN, under Resources, click Route Tables.**

Note - For more information, refer to the relevant OCI documentation here.

2. **Click Add Route.**

3. **Enter the following:**

Target Type: Internet Gateway.

Destination CIDR block : *0.0.0.0/0* (which means that all non-intra-VCN traffic that is not already covered by other rules in the route table goes to the target specified in this rule.)

Compartment: The compartment where the internet gateway is located.

Target: The internet gateway you created.

4. **Click Add Route Rule.**

The default route table now has a rule for the internet gateway. Because the subnet was set up to use the default route table, the resources in the subnet can now use the internet gateway. The next step is to specify the types of traffic you want to allow in and out of the instances you later create in the subnet.

▼ Update the Default Security List for the VCN

Follow this procedure to update the default security list for the VCN to allow necessary traffic.

Earlier you set up the subnet to use the VCN's default security list. Now you add security list rules that allow the types of connections that the instances in the VCN will need.

Note - Some customers may wish to explicitly allow only the protocols/ports listed in Oracle Advanced Support Gateway Security Guide.

To update the default security list for the VCN, perform the following steps in the your new compartment:

1. **While viewing the VCN, under Resources, click Security Lists.**

Note - For more information, refer to the relevant OCI documentation here.

2. **Click the default security list to view its details. By default, you land on the Ingress Rules page.**
3. **Click Add Ingress Rule.**
4. **To enable inbound connections for HTTPS (TCP port 443), enter the following:**

   Stateless: Unselected (this is a stateful rule.)

   Source Type: *CIDR*.

   Source CIDR: 0.0.0.0/0

   IP Protocol: TCP

   Source Port Range: All

   Destination Port Range: 443
5. **Click Add Ingress Rule.**
6. **Use the above steps to add a stateful ingress rule for any subnets with customer assets for the protocols/ports listed in Oracle Advanced Support Gateway Security Guide.**
7. **Add a stateful ingress rule for Oracle's Jumpgate Host for TCP Ports 22 and 443.**

▼ Create a New Compute Instance Using the Gateway Custom Image

Follow this procedure to create a new compute instance using the Gateway custom image.

To create a new compute instance using the Gateway custom image, perform the following steps in the OCI web user interface:

1. **Open the navigation menu.**

   Under **Core Infrastructure**, go to **Compute** and click **Instances**. Choose the Compartment you require for the gateway and then click **Create Instance**.

Note - For more information, refer to the relevant OCI documentation here.

---

2. **Specify the resources.**

   In the **Create Compute Instance** dialog box, you specify the resources to use for your instance. By default, your instance launches in the current compartment, and the resources you choose also come from the current compartment.

   In the **Create Compute Instance** dialog box, specify the following:

   - **Name your instance**: The name for the instance. You can add or change the name later. The name doesn't need to be unique; an Oracle Cloud Identifier (OCID) uniquely identifies the instance.
   - **Select an availability domain for your instance**: Select an Availability Domain based on current AD usage in your tenancy.
   - **Choose an operating system or image source**: The source of the image to use for booting the instance. When you click Change Image Source, the Browse All Images dialog box opens with the operating system or image source options.

     Choose **Custom Images**, then **Select your image**, and choose the image from the saved location.
   - **Choose instance type**: Select **Virtual Machine**.
   - **Choose instance shape**: Choose the instance shape based on the standard gateway requirements (VM.Standard2.4.)

     See “Minimum System Requirements” on page 10 for more information about the gateway requirements.
   - **Configure boot volume**: Select the default.
   - **Add SSH key**: Do not choose an SSH key.
   - **Configure networking**: The network details for the instance. In this section, you configure the following:
     - **Virtual Cloud Network Compartment**: The compartment containing the network in which to create the instance.
     - **Virtual Cloud Network**: The VCN created for the gateway.
     - **Subnet Compartment**: The subnet compartment created for the gateway.

- **Subnet**: The subnet created for the gateway.
- **Show Advanced Options**: Advanced networking and management options.
  - On the **Networking** tab, select **Private IP Address**.

    Choose a private IP address for the gateway from the subnet (this will be the static IP of the Gateway used for monitoring.)
  - On the **Networking** tab, select **Assign public IP address:**.

3. **Click Create.**

   After the instance is provisioned, details about it appear in the instance list. To view additional details, including public and private IP addresses, click the instance name.

Connect to the Gateway Web Portal

Once the Gateway instance is up and running, you can see its public and private IP addresses in the OCI web console as outlined in the previous section.

Follow this procedure to obtain the IP address of the gateway and connect to the gateway web portal. The IP address you use (public/private) depends on whether you are connecting from the internet or somewhere within the customer's OCI tenant.

To connect to the gateway web portal:

1. **Open the navigation menu.**

   Under **Core Infrastructure**, go to **Compute** and click **Instances**.

   Note - For more information, refer to the relevant OCI documentation here.

2. **Select your gateway instance.**

   The *custadmin* section of the Gateway installation has already been completed.

3. **Navigate to the IP address of the gateway (in the format https://<IP address>) to complete the Gateway activation and software installation.**

   See “Installing and Activating the Oracle Advanced Support Gateway” on page 19.