Oracle Advanced Services Platform

Oracle® Advanced Services Gateway Installation Guide

E40642-47
February 2026

Oracle Advanced Services Platform Oracle® Advanced Services Gateway Installation Guide,

E40642-47

Contents

Preface

This document details how to build Oracle Advanced Services Gateway (hereafter referred to as Gateway/the Gateway) both in the Cloud (using Oracle Cloud Infrastructure, or OCI) and in an on-premises configuration.

1

Preparing for Installation

This section covers the following topics:

Changes to the Installation Guide Since the Last Release

In this section, we outline changes to *Oracle Advanced Services Gateway Installation Guide* (this guide) since the last release (E40642-46; December 2025):

- New menu items related to regional proxy have been added.
- Outdated system screenshots along with the navigational instructions have been updated in various sections of the document.
- References to Hardware RAID have been removed.
- The latest Advanced Support Gateway release is now 21.20.x.
- Removed references to Windows 7, 8 and 10. Added Windows 11.
- Updated the link for Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware.

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 Gateway on Oracle Cloud Infrastructure

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 8. It can be installed in any environment which supports Oracle Linux 8 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.

Minimum System Requirements

If you would like to order a server from Oracle for the purpose of running the gateway, Oracle recommends the Gateway Server E6-2L. 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 Gateway Server E6-2L, 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:

Advanced Services Gateway Minimum Host System Installation Requirements

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	48 GB	64 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.) The Gateway supports a maximum of 90 agents or up to 900 targets with status whichever is lower.
Storage	1 disk >=1 TB (if using local storage) 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 15 for more information about usable space.	6 disks >= 1 TB each	Multiple disks are recommended to provide fault tolerance using RAID, which is supported by software. All disks must be of equal size. A mixture of differently sized disks in the same system is not supported.
Network	One logical interface. Firewall ports opened.	One logical interface. Firewall ports opened.	Refer to Oracle Advanced Services Gateway Security Guide for details of the specific port and firewall requirements for the gateway to function properly.

Category	On-premises Minimum	On-premises Recommended	Additional Details
Network Bandwidth	10 Mb/s connection to the internet. Optimally, 100 Mb/s is required between the Gateway and the supported systems.	10 Mb/s connection to the internet. Optimally, 100 Mb/s is required between the Gateway and the supported systems.	-

- The Gateway can be installed in **one of the following ways**:
  - Directly onto any server hardware that is supported by Oracle Linux 8.*x* and Unbreakable Enterprise Kernel (UEK) 7 (or later), *or*
  - On Oracle VM, *or*
  - On a VM that supports installation of Oracle Linux 8.*x* and Unbreakable Enterprise Kernel (UEK) 7 or later. For further information, see MOS KB 79373.

To review the Oracle Support position for Oracle products running on virtualized environments, see MOS KB 183395.

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

> **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 contact your Oracle sales representative directly or via Oracle's Contact Us Page.

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.

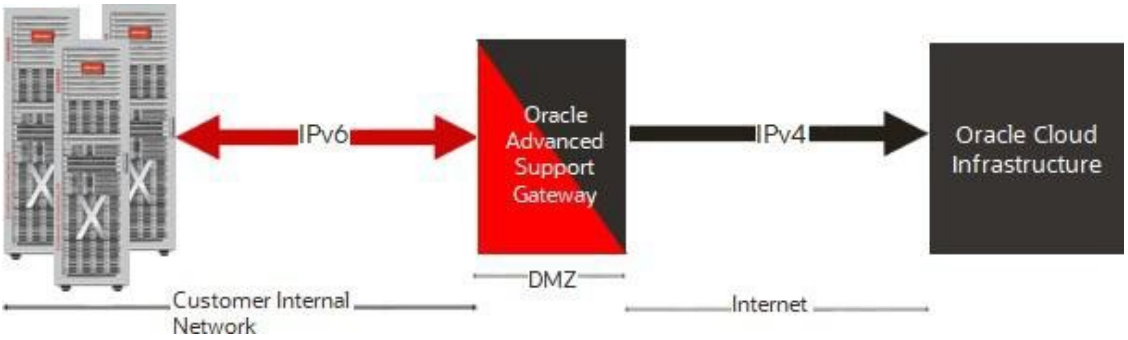
Network Requirements

The Gateway server must have at least one interface configured with an IPv4 address that is used to communicate to the Internet and the Oracle endpoints. You can add more interfaces to the Gateway to support systems that are not accessible from the primary interface. These interfaces can support either IPv4 or IPv6.

> **Note**
>
> When IPv6 addresses are added to the primary interface, *you are not required to add a physically separate cable* to support internal IPv6 networks and IPv4 communication to the Oracle endpoints.

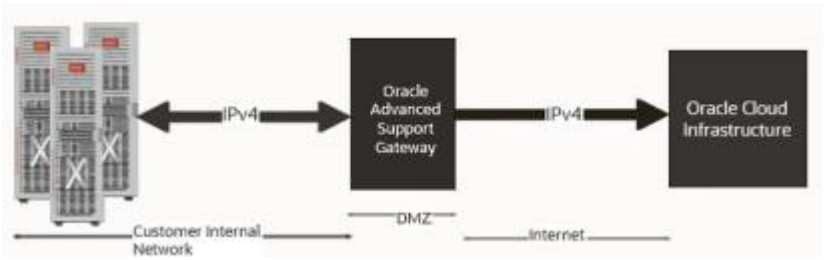
The diagram below depicts an example network configuration featuring an internal customer network and Oracle that incorporates both IPv4 and IPv6.

High Level Network Configuration and IPv4/IPv6 Distribution:



The diagram below depicts an example network configuration featuring an internal customer network and Oracle that uses only IPv4.

High Level Network Configuration and IPv4 Distribution:



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

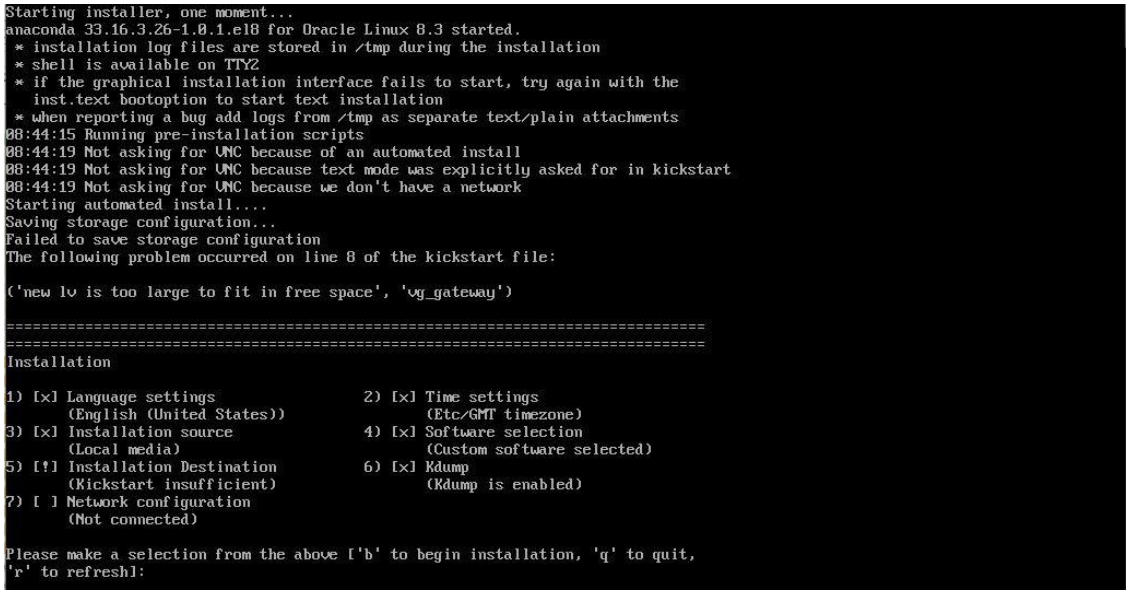
The installation process makes certain assumptions when choosing the appropriate disk drives to use for installation of the operating system. The assumptions are as follows:

- 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 one of the following is excluded because they are assumed to not be a disk drive:
  - /dev/vd
  - /dev/sd

- /dev/xvd
- /dev/mpath
- /dev/cciss
- /dev/nvme

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.

Number of Drives	Minimum Size (Each Drive)	Disk Configuration	Fault Tolerance	Storage Capacity (s = size of each disk)
1	1 TB	All storage on a single disk	None	s
2	1 TB	RAID 1 (mirror)	Can survive a single drive failure.	s

3	1 TB	RAID 1 (mirror or disks 1 and 2) plus disk 3 used for backups	Can survive a single drive failure.	s
4	1 TB	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 of disks 1 or 2 and 3 or 4, but not 1 and 2 or 3 and 4.	2 x s
5	1 TB	RAID 10 (mirror on disks 1 and 2, mirror on disks 3 and 4, striped across the 2 mirrored sets) plus disk 5 used for backups.	Can survive one disk failure in each mirror set and one additional failure.	2 x s
6	1 TB	RAID 10 (mirror on disks 1 and 2, mirror on disks 3 and 4, striped across the 2 mirrored sets) plus RAID 1 (mirror on disk 5 and 6) for backups.	Can survive one disk failure in each mirror set. 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 /var partition is 100 GB.

This value should provide ample space for diagnostic uploads to Oracle Support for SRs.

- The /var/tmp partition is 40 GB.

This value should provide ample space for patch downloads and software upgrades.

- The /var/log partition is 20 GB.

This value should provide ample space for application logging.

- The /var/log/audit partition is 5 GB.

This value should provide ample space for audit specific logs.

- The /home partition is 32 GB.

This value should provide ample space for users' home directories for data collection and analysis within the environment.

- The /boot partition is 2 GB.

This value should provide ample space for future kernel updates.

- The /(root) partition is 50 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 1 TB minimum requirement specified in Supported Local Disk Configurations), 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                     1K-blocks     Used Available Use% Mounted on
/dev/mapper/vg_gateway-lv_root  51290592 16247684  32405084  34% /
```

But the fdisk -l command shows:

```
Disk /dev/mapper/vg_gateway-lv_root: 50 GiB, 53687091200 bytes, 104857600 sectors
```

> **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

The 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)

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. Following installation, access the Gateway using the console to perform network configuration and registration using 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.	

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. Once authenticated, in search window, select ‘Patches and Product Certification Matrix’ or you can use the direct link.
3. Fill in Product = Oracle Advanced Support Gateway
4. For the release, start typing “Advanced Support Gateway” and select the release you want to download from the drop down. Generally, 21.20.x or later should be selected.
5. Click Apply.
6. From the list of displayed releases, click on the “Patch Name” for the specific release you want to download and follow the on-screen download instructions.

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.

If you're using Windows 11, double-click the ISO image file to mount the file as a virtual disc.

To burn an ISO image to a DVD for the Windows platform, use a commercial DVD burning utility such as Roxio or Nero or search for a free utility on the internet.

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.

2

Installing and Activating the Gateway

Follow these procedures to install and activate the Gateway:

- Installing the Operating System Using the ISO Image
- Registering the Gateway With Oracle
- Activating the Gateway
- Replacing an Existing Gateway and Migrating Its Data

Installing 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.

> **Note**
>
> If you are using a proxy to establish the TLS VPN tunnel, the proxy cannot require authentication.

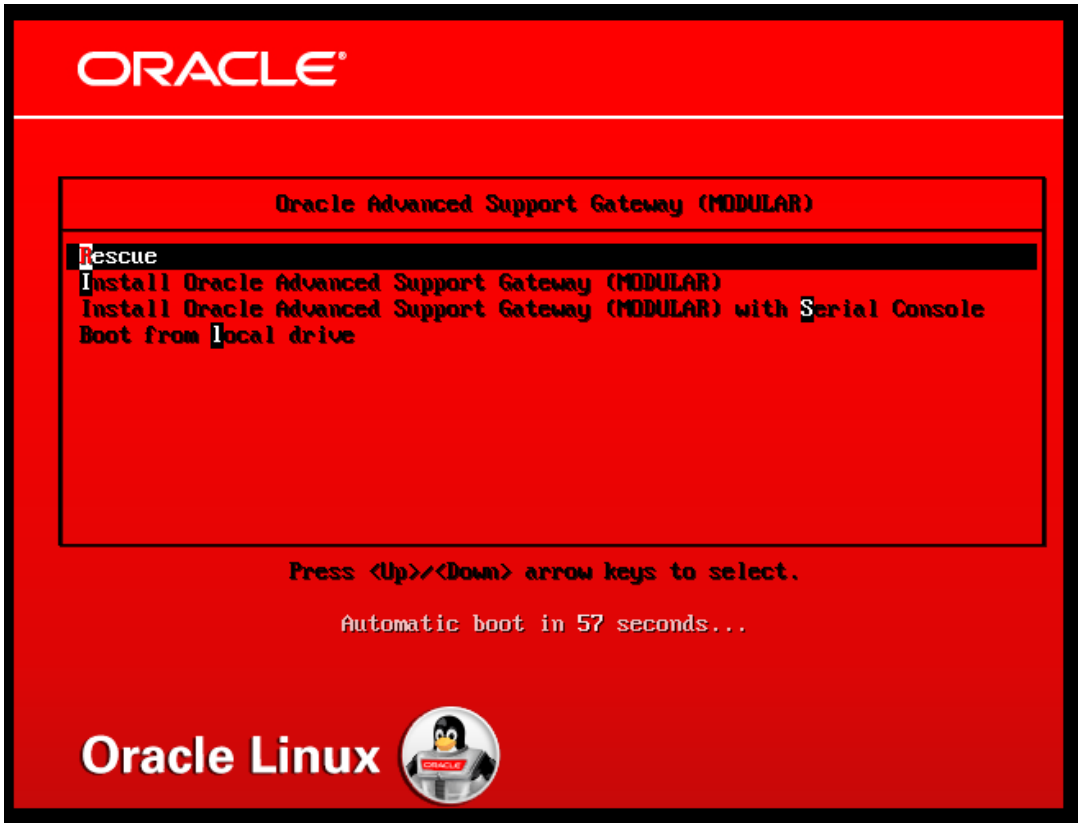
> **Note**
>
> If you are using the alternative IPSec connectivity option, the IPSec tunnel must be established *prior* to the ISO install. Contact your implementation engineer for further information.

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**
>
> By default, *Rescue* option will be selected. To proceed, move the selection down to *Install Oracle Advanced Support Gateway (MODULAR)*.

2. **To start the installation process, choose the default option, Install Oracle Advanced Support Gateway (MODULAR).**
   The initial installation process takes a number of minutes to complete.
3. **Before rebooting the server, eject or unmount the install media so that the server boots the newly installed operating system.**
4. **Press Enter to reboot the server.**
5. **Once the server has rebooted, proceed to the Gateway configuration in the following section.**

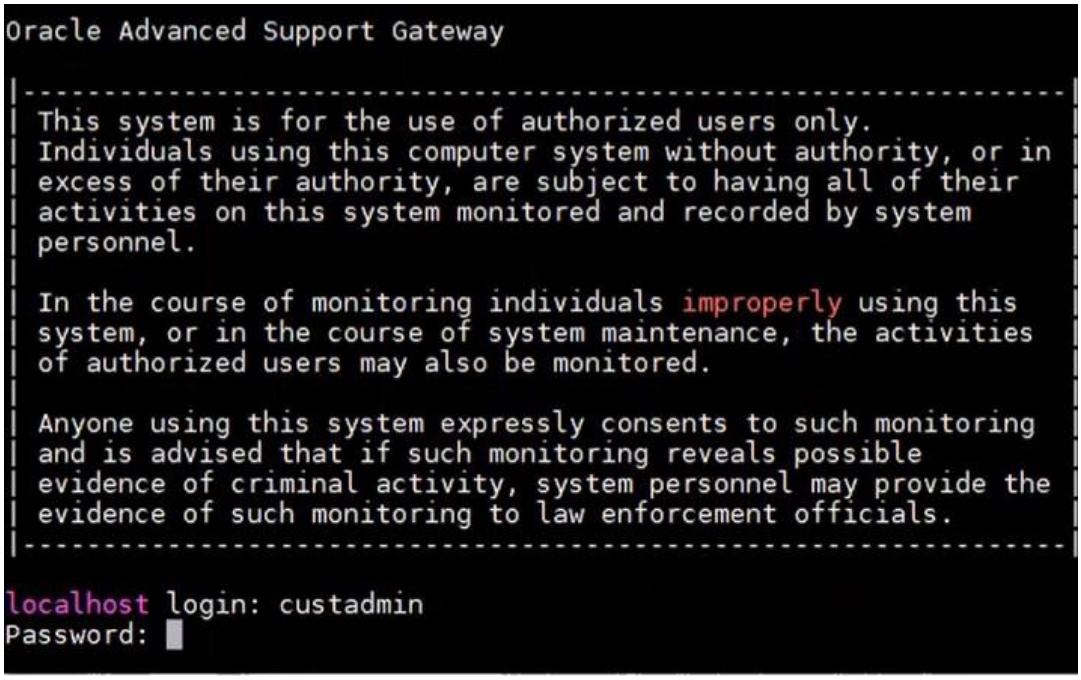
Registering the Gateway With Oracle

During this portion of the installation process, you are guided through a series of menus to collect the necessary information to connect to Oracle and register the Gateway. In addition, you can also configure the network by:

- Adding multiple network interfaces
- Assigning IPv4 or IPv6 addresses
- Adding VLAN tags to interfaces
- Adding bonded interfaces.

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**

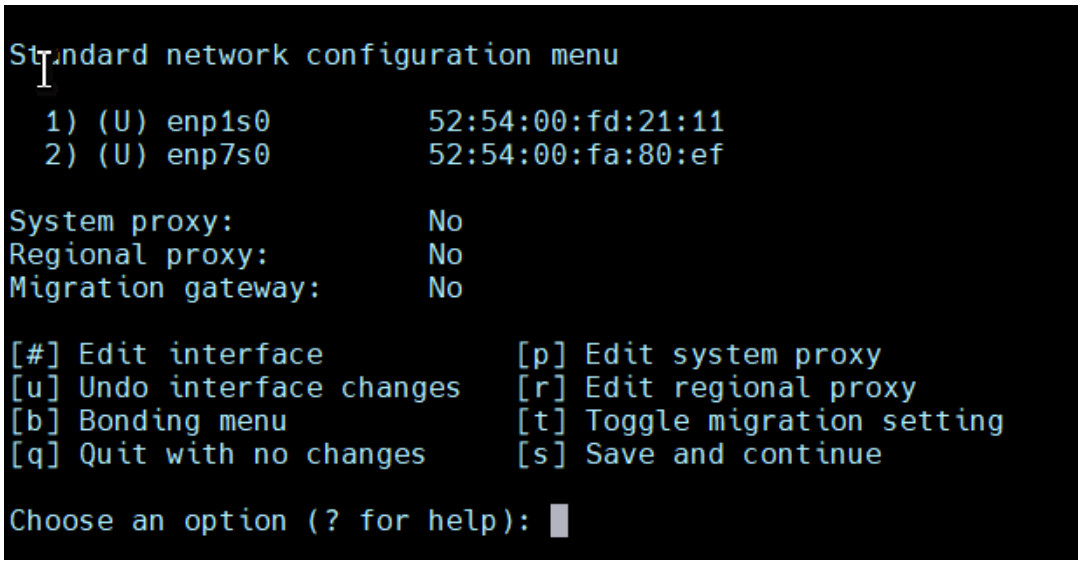
   Upon successful login, a screen displaying a message asking whether you wish to migrate an existing Gateway appears (*OASG* means Oracle Advanced Support Gateway).

3. **Select one of the following options:**

- Enter **y** to use this Gateway to replace an existing Gateway and migrate its data. Refer to Replacing an Existing Gateway and Migrating Its Data
- Enter **n** to set up a new gateway. Continue with the next step.

4. **Select one of the following options:**
   - Enter **b** to switch to the bonding configuration menu. Refer to *Step 7* below.
   - Enter the digit corresponding to the interface you wish to configure.

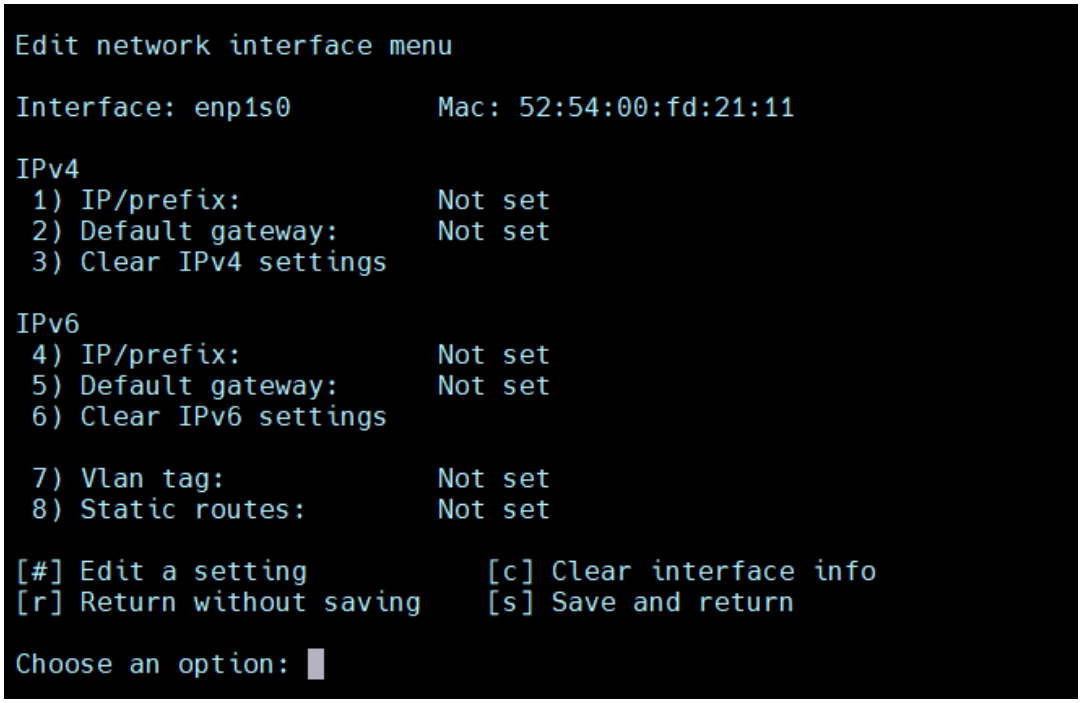
   So, for example, in the screen shot below, the user enters **1** which corresponds to enp1s0.



> **Note**
>
> Enter **?** for a complete list of options and symbols.

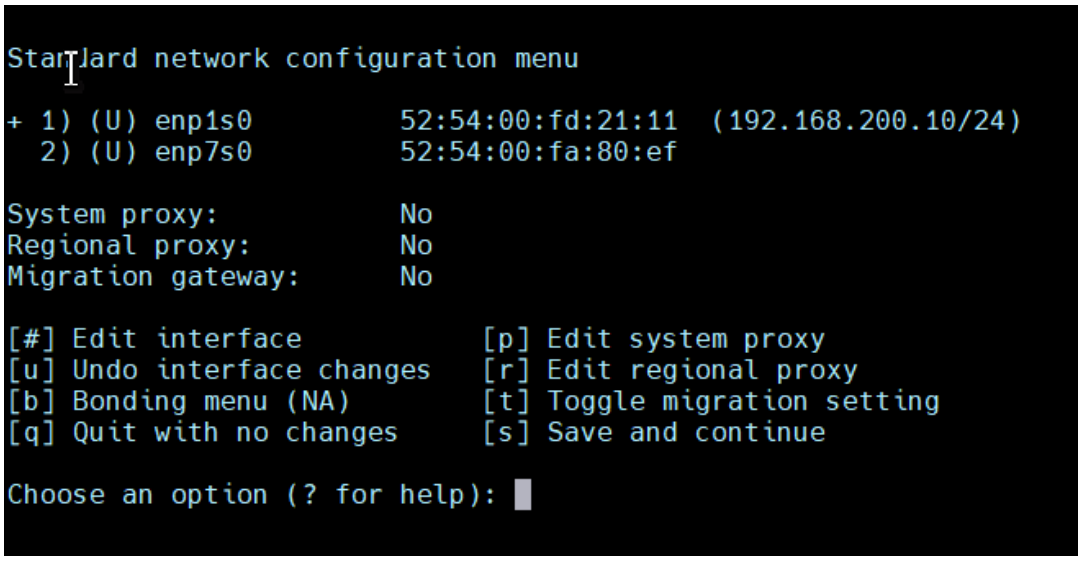
5. **Enter the property number to edit the corresponding property.**
   The configuration information might include:
   - The IP address and CIDR (IPv4 and IPv6 if enabled);
   - The default Gateway of the interface;
   - A VLAN tag;
   - Static routes.

   There can be only *one* IPv4 and *one* IPv6 default Gateway defined per system. There must be *at least one* IPv4 default Gateway defined. The IPv4 and IPv6 default Gateways can be on two different interfaces.

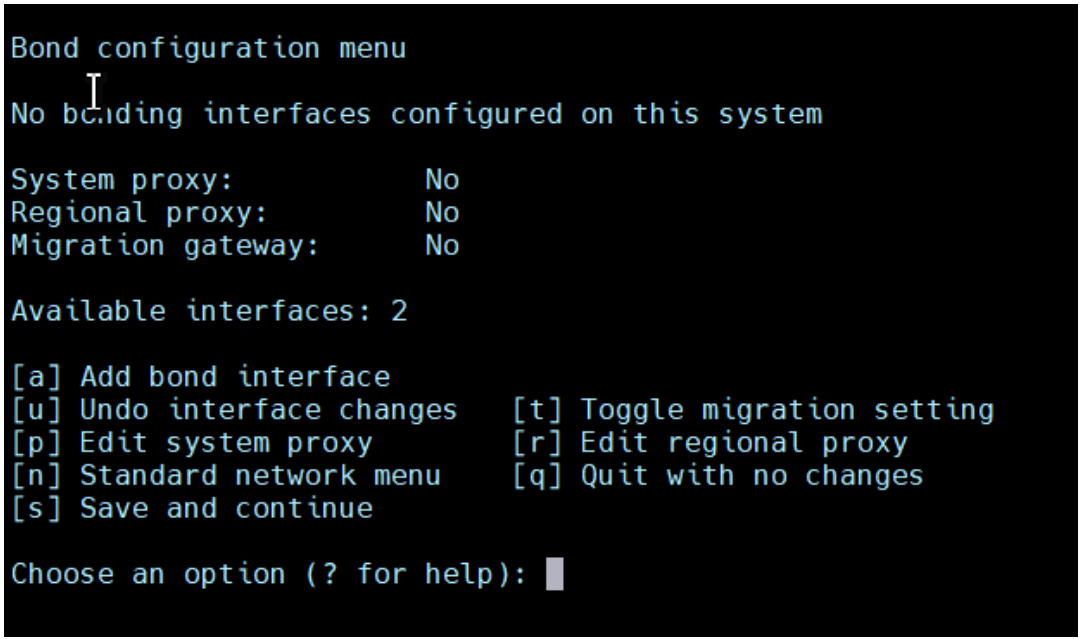


6. **Review the information and enter s to save the configuration.**
If you entered enough information to configure the interface you will notice a plus sign next to the interface, as with enp1s0 in the screen shot below .

> **Note**
>
> An exclamation point indicates there is some information missing.

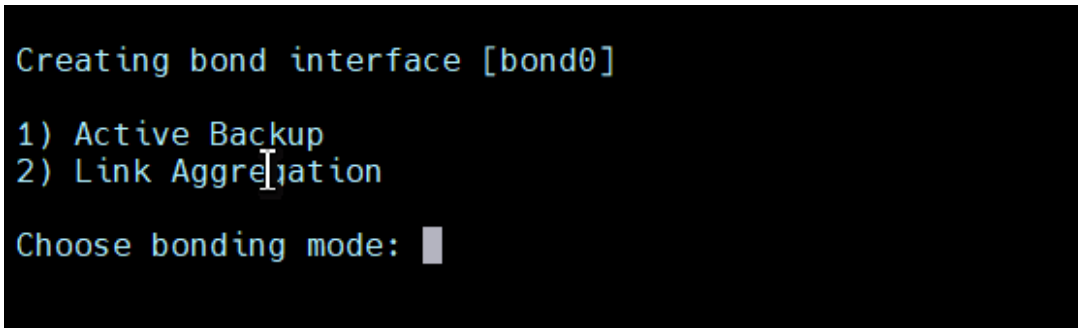


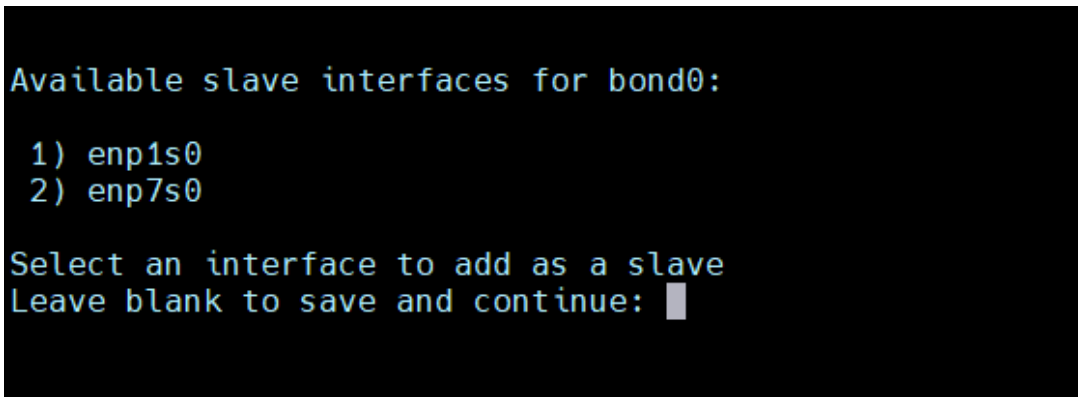
7. **(Optional) To configure a bonding interface, enter b from the standard network configuration menu to display the bonding configuration menu.**



Enter **a** to add a new bonding interface. You will be prompted for: The type of bond:

- The type of bond:
  - Active Backup, *or*
  - Link Aggregation
  - The slaves for the bond (enter the corresponding number of the interface to select or deselect)





After entering the information, the main bond configuration menu appears.

```
Bond configuration menu

! 1) (D) bond0          (enp7s0 enp1s0)

System proxy:            No
Regional proxy:          No
Migration gateway:       No

Available interfaces: 0

[#] Edit bond interface      [a] Add new bond interface
[u] Undo interface changes   [t] Toggle migration setting
[p] Edit system proxy        [r] Edit regional proxy
[n] Standard network menu    [q] Quit with no changes
[s] Save and continue

Choose an option (? for help):
```

> **Note**
>
> In this case, an exclamation point is displayed because the bond is only partially configured at this point.

Select the new bond number, **1**, to edit it.

```
Edit bond interface menu

Interface: bond0

IPv4
 1) IP/prefix:           Not set
 2) Default gateway:     Not set
 3) Clear IPv4 settings

IPv6
 4) IP/prefix:           Not set
 5) Default gateway:     Not set
 6) Clear IPv6 settings

 7) Slaves:              enp7s0 enp1s0
 8) Bond mode:           Active Backup
 9) Vlan tag:            Not set
10) Static routes:       Not set

[#] Edit a setting
[c] Clear all settings       [d] Delete interface
[r] Return without saving    [s] Save and return

Choose an option:
```

The configuration information includes:

- The IP address and CIDR for the bonding interface (IPv4 and IPv6 if enabled);

- The default gateway of the bonding interface;
- Bonding mode (active backup or link aggregation);
- Slave interfaces for the bonds;
- A VLAN tag for the interface;
- Static routes.

Review the information, edit as required, and enter **s** to save the configuration.

The main bond configuration menu containing your saved information is now displayed.

Note - The plus sign next to the bond denotes that it is now correctly configured.

```
Bond configuration menu

+ 1) (D) bond0         (enp7s0 enp1s0)
                       (192.168.100.10/24)

System proxy:           No
Regional proxy:         No
Migration gateway:      No

Available interfaces: 0

[#] Edit bond interface      [a] Add new bond interface
[u] Undo interface changes   [t] Toggle migration setting
[p] Edit system proxy        [r] Edit regional proxy
[n] Standard network menu    [q] Quit with no changes
[s] Save and continue

Choose an option (? for help):
```

8. **When configuring both standard and bonded network interfaces, you have the option to add any number of static routes for each interface.**

```
Static route menu for enp1s0

 No static routes defined

[a] Add a new route
[r] Return without saving    [s] Save and return

Choose an option: a

Would you like to enter an IPv4 or IPv6 route? [4|6]: 4

Enter an IP address and prefix for the route destination (#.#.#.#/#): 10.10.10.10/24

Enter the gateway for 10.10.10.10/24 (#.#.#.#): 10.10.10.1
```

9. **When configuring both standard and bonded network interfaces, you can assign VLAN tags.**
When you edit a non-tagged interface and add a new VLAN tag, the script transfers all the current information for that interface to a new interface with the same name and an extension represented by the VLAN tag you chose. For example, refer to the sample screen shots below:

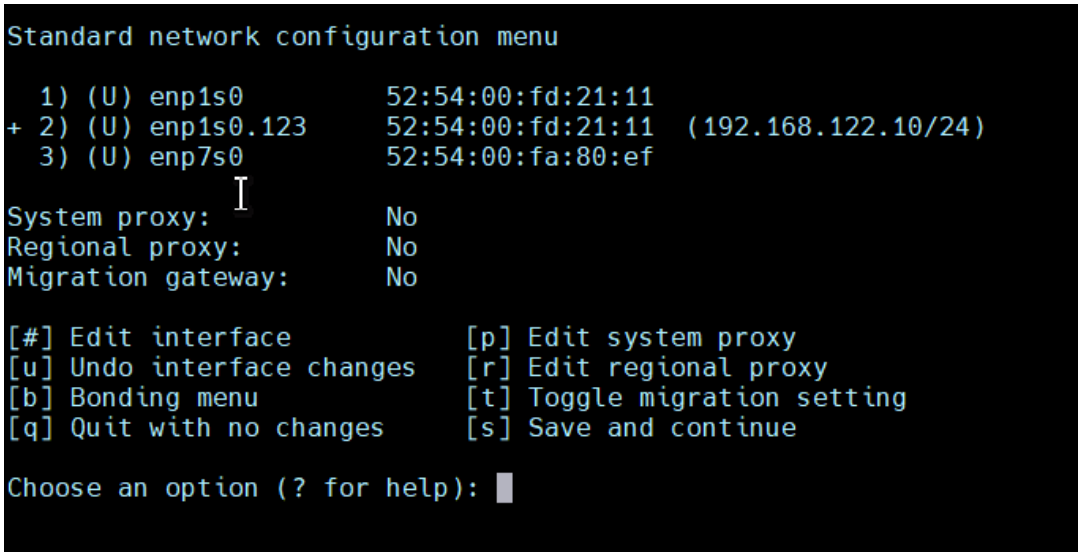
```
Standard network configuration menu

+ 1) (U) enp1s0          52:54:00:fd:21:11  (192.168.122.10/24)
  2) (U) enp7s0          52:54:00:fa:80:ef

System proxy:            No
Regional proxy:          No
Migration gateway:       No

[#] Edit interface           [p] Edit system proxy
[u] Undo interface changes   [r] Edit regional proxy
[b] Bonding menu (NA)        [t] Toggle migration setting
[q] Quit with no changes     [s] Save and continue

Choose an option (? for help):
```

(Optional) Enter **1** to edit *enp1s0* and then add a VLAN tag.

```
Edit network interface menu

Interface: enp1s0          Mac: 52:54:00:fd:21:11

IPv4
 1) IP/prefix:             192.168.122.10/24
 2) Default gateway:       192.168.122.1
 3) Clear IPv4 settings

IPv6
 4) IP/prefix:             Not set
 5) Default gateway:       Not set
 6) Clear IPv6 settings

 7) Vlan tag:              Not set
 8) Static routes:         Not set

[#] Edit a setting           [c] Clear interface info
[r] Return without saving    [s] Save and return

Choose an option: 7

Enter the VLAN tag for enp1s0 (#): 123
```

When you save and return to the standard network menu, you can see that the information from

enp1s0 is now associated to *enp1s0.123*.



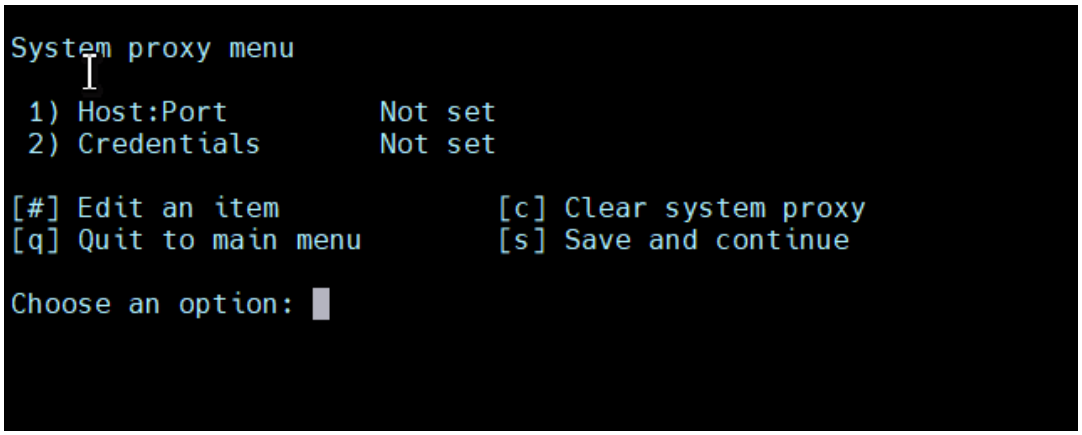
> **Note**
>
> You can assign multiple, different, VLAN tags to the same interface. Each tagged interface has different network address information.

10. **(Required) After the network configuration has been completed, you *must* assign either a system proxy *or* a regional proxy.**
A system proxy is a customer managed intermediary device between the oasg and the internet through which traffic is routed.

    Regional proxies are Oracle managed and reside in OCI. Each regional proxy is in a different geographic location. If a system proxy is not being used, then a regional proxy must be selected. It is generally recommended to choose the region closest to the location of the OASG.

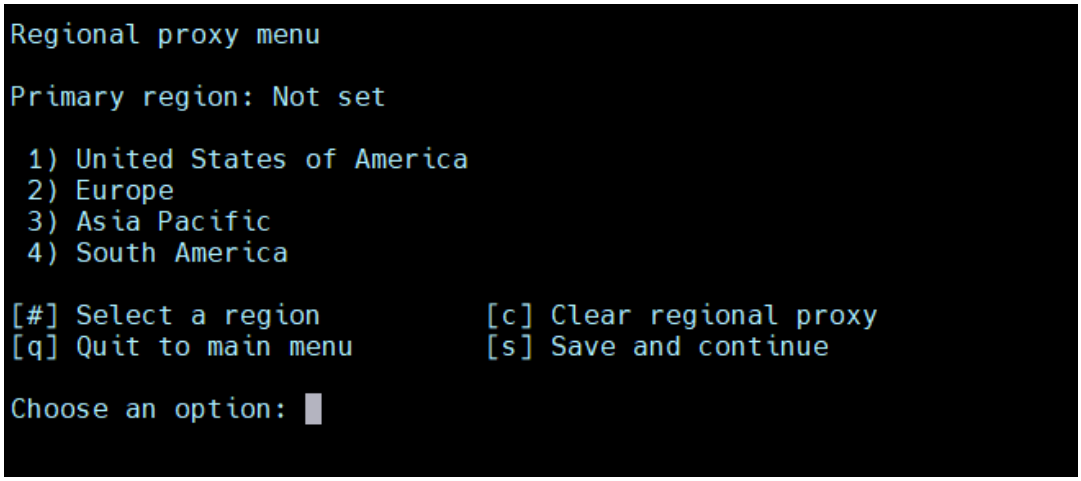
    To add a system proxy, enter **p** from either the standard configuration menu or the bonding configuration menu to display the system proxy configuration menu.

    Enter the proxy IP address and port number. If necessary, enter the proxy username and password and then confirm the password. Refer to the following screenshot.



> **Note**
>
> NTLM authentication is not supported.

To add a regional proxy, enter **r** from either the standard configuration menu or the bonding configuration menu to display the regional proxy configuration menu.



> **Note**
>
> Note - You can only assign a system proxy or a regional proxy, not both. If you enter details for either and need to switch, you must first clear any proxy details that were already entered.

11. **Confirm the network information for all the interfaces you added.**
    Review the network information and select **s** to save the configuration details.

    Any unconfigured interfaces are deleted. All configured interfaces are first deleted (to remove artifacts) and then recreated.

12. **After all 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 a number of minutes. The most recent packages and configuration parameters are downloaded automatically. Do not restart the Gateway during this step.

13. **After the latest packages have been downloaded and applied, you are prompted to select the Gateway type.**
    The Gateway types are outlined as follows:

    - STANDARD: This is the standard Gateway type and the default option. Use this option for all services that include comprehensive monitoring, such as *Oracle Platinum Services*, *Oracle Advanced Monitoring and Resolution* and *Oracle Advanced Management for Hybrid Cloud*.
    - BASIC: This option Installs a limited version of the Gateway for use with services that do not include comprehensive monitoring. Use this option only if you have enrolled in *Oracle Platinum Without Software Monitoring Service*.

    The following screen shot shows sample answers. In this installation, the STANDARD Gateway is selected.

```
2024-03-15 15:43:01 [INFO] Beginning registration and configuration of
2024-03-15 15:43:01 [INFO] the Oracle Advanced Support Gateway (OASG)
2024-03-15 15:43:01 [INFO] Downloading updates
Supported OASG Types: BASIC|STANDARD
Please enter OASG type [STANDARD]:
2024-03-15 15:43:58 [PASS] Downloading updates successful
```

Installation of the updates required takes a number of minutes.

Activating the Gateway

This section provides information about activating the Gateway.

During this activation process, you are guided through a series of prompts to collect the necessary information to activate the Gateway.

1. **You are prompted to register your username and password.**

> **Note**
>
> You require an Oracle Single Sign-on account to register. Enter your username and password. Confirm the password.

```
                    [INFO] Activating and Registering the OASG

An Oracle Single Sign On (OSSO) account is required for data submission.
If you do not have an account or have forgotten your username or
password, visit http://support.oracle.com


Username []:.....@oracle.com
Password:
Password again (to verify):
```

2. **Use the activation code to configure the Gateway.**
   Enter your Gateway activation code to configure 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 guide for Platinum Services on the Gateway documentation page.

   During this activation process, you are guided through a series of prompts to verify the external connections to Oracle.

3. **Test the VPN connection to Oracle.**
   The Gateway generates the VPN password and attempts to establish the VPN connection. Typically, if using SSL/VPN, this process should take a few 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, please contact your Oracle representative. For example, contact your Platinum Implementation Engineer using the Platinum Implementation Service Request.

When prompted to test the VPN connection, enter **r**.

4. **Create a new user password.**
   In this step, you change the *custadmin* password from the default value **install**.
   - In the **New Password** field, enter the password associated with the user.

> **Note**
>
> Ensure the new password is a minimum of 14 characters long. The following screen shot shows the new password prompt:

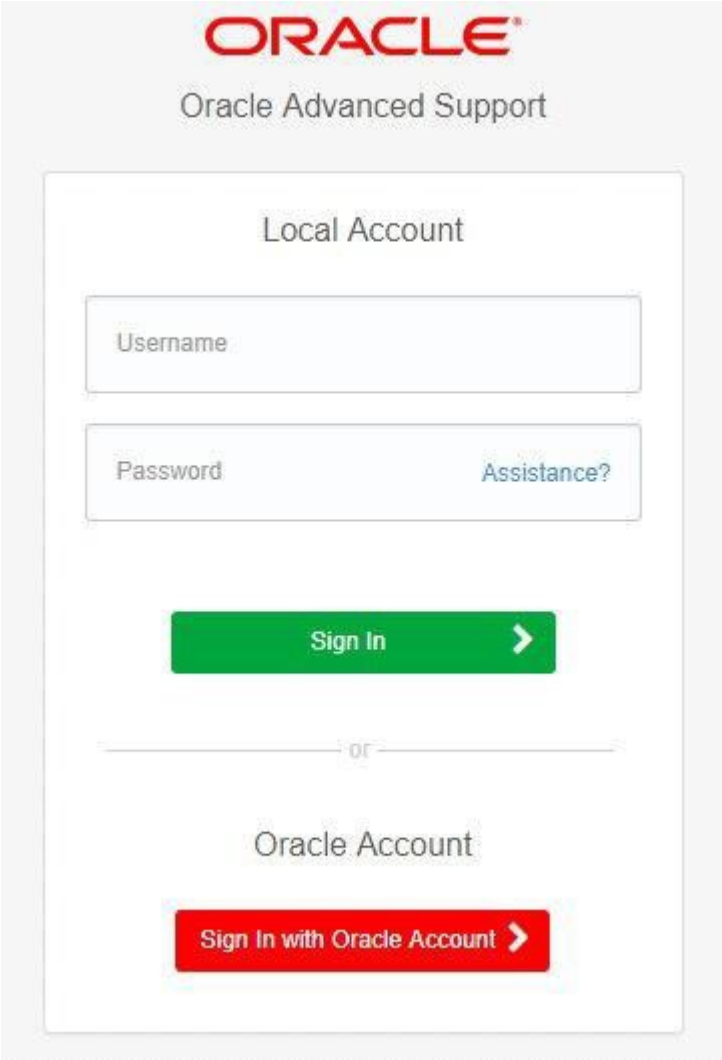
```
You need to set a new password for the OASG user

Changing password for user custadmin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
YYYY-MM-DD HH:MM:SS [PASS] Finalizing configuration successful
YYYY-MM-DD HH:MM:SS [PASS] Setup of the OASG successfully completed

Press enter to exit.
```

The user input for the gateway installation is complete. The final software configuration is executed in the background.

5. **Access the Gateway user interface (UI).**
   Use a browser to 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 communicates internally.

If the software is still being configured, the following screen shot is displayed. Please navigate to the Gateway UI at a later time when configuration is complete.

If the software has been configured, the Gateway login screen appears.



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 into 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:

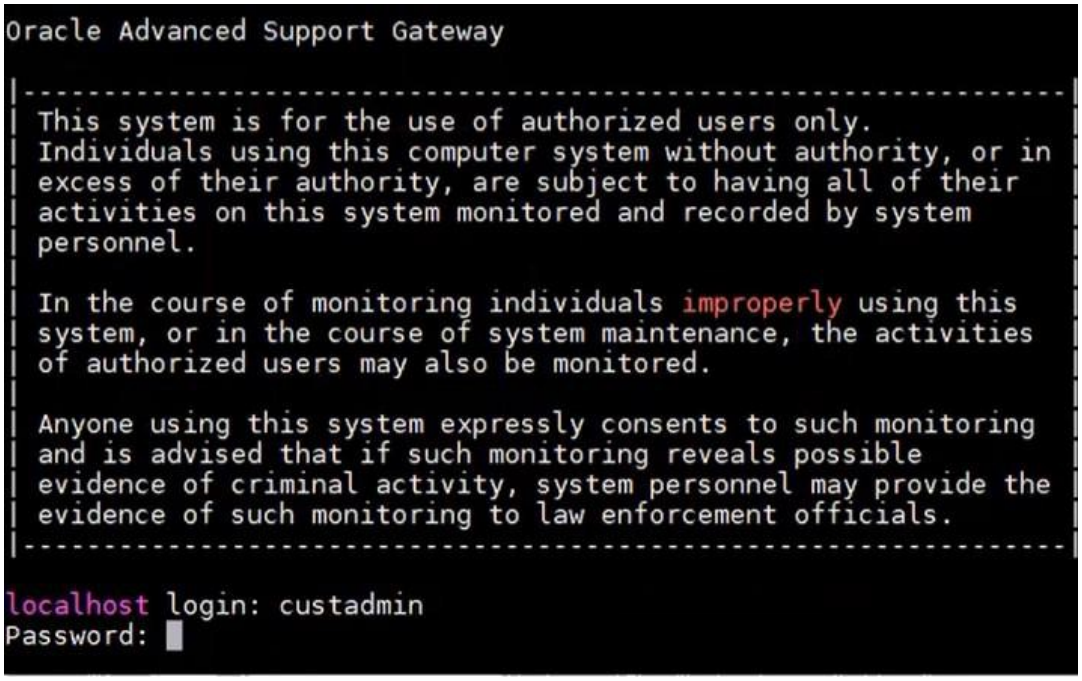
- Navigate to https://*GATEWAY_IP_ADDRESS* where *GATEWAY_IP_ADDRESS* is the IP address assigned to the physical interface of the Gateway. Where two interfaces are used, you need to reference the internal interface. This is the IP address which will communicate internally.
- Log on to the portal. Use the customer administrator account configured at installation time (see the *Gateway user account* in "Collect Registration Information" on page 18) or any other user with the customer administrator role.

The **All Services** page appears.

Replacing an Existing Gateway and Migrating Its Data

During this portion of the installation process, you are guided through a series of questions to collect the necessary information to use this Gateway to replace an existing one and to migrate its data. 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, a screen displaying a message asking whether you wish to migrate an existing Gateway appears (*OASG* means Oracle Advanced Support Gateway).

3. **Select one of the following options:**

   - Enter **y** to use this Gateway to replace an existing Gateway and migrate its data. Continue with the next step.

The script executes a migration script on the system which automates the process. It first uses saved information to restore the Gateway's network configuration, and then completely restores the rest of the Gateway, including the activation phase.

- Enter **n** to set up a new gateway. Refer to Registering the Gateway With Oracle

3

Deploying the Gateway on Oracle Cloud Infrastructure

This section applies to deployment of the Gateway on Oracle Cloud Infrastructure (OCI.) To deploy the Gateway on OCI, review the following multi-step process:

- System Requirements for Cloud Deployment
- Customer Requirements for Deploying the Gateway on Oracle Cloud Infrastructure
- Configuring the Gateway on Oracle Cloud Infrastructure

> **Note**
>
> To review the requirements for installing the Gateway in an on-premises Gateway configuration, see Review Host System Requirements for On-Premises Installation

System Requirements for Cloud Deployment

The server must meet the minimum host system requirements for Oracle Advanced Services 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 Services 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 the 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.

> **Note**
>
> Deployment of the Gateway on Oracle Cloud Infrastructure (OCI) is not supported for Platinum Services.

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

This deployment scenario is defined as follows:

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 Services 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:

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 Services 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:

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 Services 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 the Gateway on Oracle Cloud Infrastructure (OCI). The configuration procedure consists of the following sequential tasks:

- Import the Gateway Custom Image
- Create the OCI Compartment Where the Gateway Will Reside
- Create the VCN
- Create the Subnet
- Create an Internet Gateway to Allow Traffic to the Internet
- Update the Default Route Table for the VCN
- Update the Default Security List for the VCN
- Create a New Compute Instance Using the Gateway Custom Image
- Connect to the Gateway Web Portal

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

> **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 Advanced Services 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 Advanced Services 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 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.

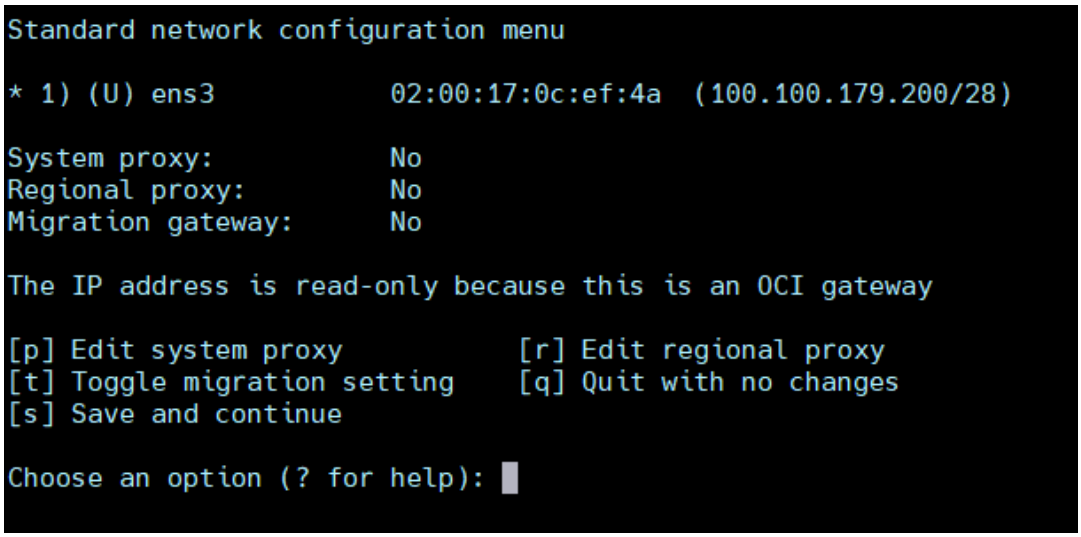
2. **Select your gateway instance.**
   The *custadmin* section of the Gateway installation has already been completed.
3. **Connect to the gateway's IP address via SSH to complete gateway activation and software installation.**
4. **Log in using the default administrator account:**
   - Login: custadmin
   - Password: install

   Upon successful login, a screen displaying a message asking whether you wish to migrate an existing Gateway appears (OASG means Oracle Advanced Support Gateway).

Select one of the following options:

- Enter **y** to use this Gateway to replace an existing Gateway and migrate its data. Refer to Replacing an Existing Gateway and Migrating Its Data
- Enter **n** to set up a new gateway. Continue with the next step.

5. **You will be presented with the following screen showing the Gateway network information.**



> **Note**
>
> The IP/prefix and Default gateway will be read-only since this gateway is in OCI.

6. **You are required to select either a system proxy or a regional proxy.**

Proceed to step 10 of Registering the Gateway With Oracle.