Oracle Advanced Services Platform

Oracle® Advanced Services Gateway for Cloud at Customer Security Guide

E91624-14
February 2026

Oracle Advanced Services Platform Oracle® Advanced Services Gateway for Cloud at Customer Security Guide,

E91624-14

Contents

Preface

1 About Oracle Advanced Services Gateway

General Requirements 1
Changes to the Security Guide Since the Last Release 2
Firewall Port Requirements 2
Downloading the Firewall Rules Document from My Oracle Support 3

2 External Connection

TLS VPN and Oracle Advanced Services Gateway 1
Alternative External Connection Option 2

3 Audit Logging Feature

Enabling and Disabling Logging Messages 2

Preface

This document outlines the requirements for deploying Oracle Advanced Services Gateway for Cloud at Customer infrastructure within the customer environment to support the delivery of certain Oracle cloud services (hereafter referred to as Oracle cloud services.) The Oracle Advanced Services Gateway is an important part of the Oracle delivery platform for Oracle cloud services and its placement has been carefully considered in order for Oracle to deliver Oracle cloud services. This document outlines Oracle recommendations when integrating the Oracle Advanced Services Gateway device within the customer environment. To help explain these options, this document assumes a "simple" customer-side network topology. However, these options can extend to more complex network topologies.

1

About Oracle Advanced Services Gateway

Oracle Advanced Services Gateway is a multi-purpose platform designed to facilitate Oracle Cloud at Customer. The Oracle Advanced Services Gateway enables the simplification of network requirements and a single point of access for the provision and delivery of these services.

The Oracle Advanced Services Gateway platform is based on the Oracle Linux operating system and hosts a full set of Oracle software stacks, including Automated Service Request (ASR), Oracle Enterprise Manager (13*c*), patch management, and a suite of Java applications. Together, these applications aggregate and route telemetry messages from the Cloud at Customer infrastructure to the Oracle Support Services infrastructure. The Oracle Advanced Services Gateway provides remote access for Oracle engineers to access the customer network (with customer permission) and to carry out approved actions on customers' monitored systems.

General Requirements

There are a number of general requirements that are necessary for Oracle to deliver Oracle cloud services:

Changes to the Security Guide Since the Last Release

- An Oracle Advanced Services Gateway must be hosted within the customer environment along with Cloud at Customer Infrastructure.
- Oracle Advanced Services Gateway will be directly connected to the Cloud at Customer infrastructure via the management network.
- Oracle must have access to certain ports and protocols (described below) in order to implement and deliver Oracle cloud services.
- Oracle Advanced Services Gateway must be continuously accessible from the Oracle Support Platform using the secure protocols described below. However, Oracle Advanced Services Gateway must not be directly exposed to the Internet.

In order to expedite the implementation process, the customer will be required to provide high level network topology which should include:

- IP numbering scheme
- Routing policy
- Locations of firewalls
- Locations of Cloud at Customer Infrastructure.
- Proposed location of Oracle Advanced Services Gateway

Having this information enables Oracle to provide a recommendation regarding Oracle Advanced Services Gateway placement.

Changes to the Security Guide Since the Last Release

This section outlines the principal changes made to *Oracle Advanced Services Gateway for Cloud at Customer Security Guide* (this document) since the last release (E91624-12; October 2024):

- We have updated some of the broken links.
- In our last update, all standard firewall port configurations necessary were moved to My Oracle Support (MOS). See Downloading the Firewall Rules Document from My Oracle Support. In this edition the individual placeholder sections that formerly provided firewall rule tables have been removed.

Firewall Port Requirements

The specifics of the Oracle cloud services network requirement depend on the customer network topology relative to the Oracle Services Support centers, Oracle Advanced Services Gateway, and the monitored systems. The customer networks must be configured to permit traffic flow between Oracle Advanced Services Gateway and Oracle Services Support centers. This is referred to as the *external connection*.

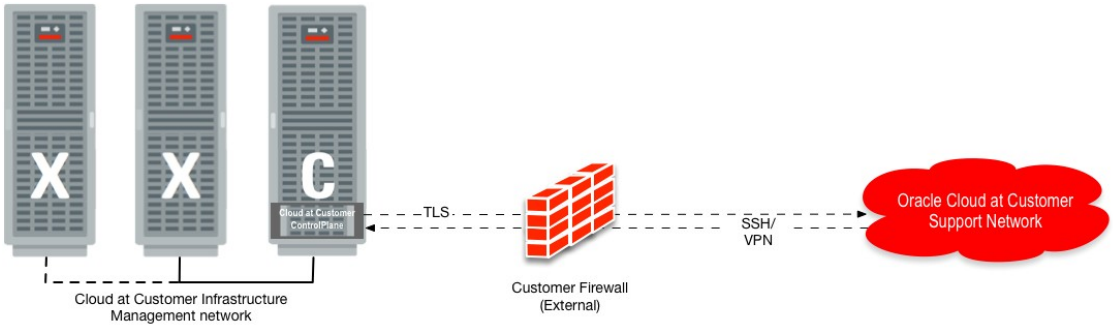
> **Note**
>
> A web proxy can be used to proxy the HTTPS traffic across the external connection. However, Oracle Advanced Services Gateway does not support NTLM or Kerberos proxy authentication. The Transport Layer Security (TLS) VPN traffic cannot be routed through a proxy server.

> **Caution**
>
> To defend against security attacks, you should never connect Oracle Advanced Services Gateway interfaces or the Oracle ILOM Service Processor to a public network, such as the Internet. The Gateway should never be exposed directly to the Internet without the protection of a customer firewall or Access Control List (ACL.)

Oracle Advanced Services Gateway comes with multiple network interfaces. Of these interfaces, two are utilized to support connectivity requirements. The first interface is used primarily for external connectivity while the second interface is connected directly to the Cloud at Customer Infrastructure management network. This provides, in effect, the required isolation between the Cloud at Customer infrastructure and the customer internal network.

The diagram below depicts an example traffic flow between monitored systems and Oracle. (Detailed firewall rules and templates are provided to the customer during the implementation process.)

Figure 1-1 High Level Traffic Flow and Firewall Requirement



Downloading the Firewall Rules Document from My Oracle Support

Information about firewall rules is no longer published in *Oracle Advanced Services Gateway for Cloud at Customer Security Guide* (this document). This information is now available in the form of a knowledge document on My Oracle Support (MOS) instead. To download this document, users are required to log on to MOS using their Oracle Account.

The document contains information on firewall rules:

- For external traffic
- For external traffic through the encrypted VPN tunnel
- For the Oracle Cloud at Customer machine to the customer network
- For the Oracle Exadata Cloud at Customer machine to the customer network
- Between the Gateway and Fusion Applications (SaaS at Customer)

To download the document:

1. Click the following link: Firewall Rules for Oracle Advanced Support Gateway.
2. Enter your Oracle Account details.
3. Download and save the relevant PDF.

Use the firewall rules information to configure traffic flow as outlined in Firewall Port Requirements.

2

External Connection

Oracle utilizes a combination of a VPN solution and TLS to secure communications between Oracle Advanced Services Gateway, located within the customer's environment, and the Oracle Services Support center locations. The VPN is primarily used for tasks such as facilitating patching requirements from Oracle Services Support center locations to Oracle Advanced Services Gateway and TLS is used for transporting the monitoring telemetry from Oracle Advanced Services Gateway to the Oracle Services Support center locations.

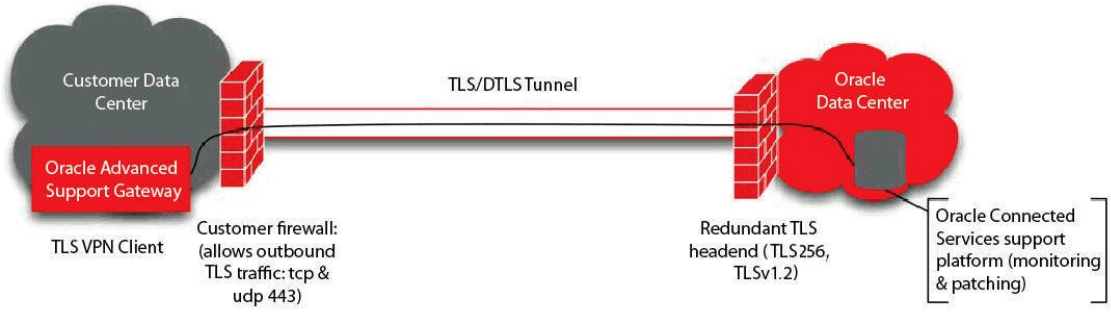
TLS VPN and Oracle Advanced Services Gateway

The Oracle Advanced Services Gateway is configured with a software TLS-based VPN client.

When the Gateway boots up, it opens an outbound connection to one of three Oracle Services Support centers, establishing a TLS VPN tunnel. At that point, this connection is used for inbound connectivity between the Oracle Services Support center and the Gateway. No inbound firewall port openings are required, as the initial connection is outbound. The Gateway is assigned a unique ID and password and connects to one of three Oracle VPN concentrators. The TLS-based VPN has the following features:

- Connection based on TLS 1.2, AES256 symmetric encryption to ensure traffic integrity and confidentiality;
- Continuous VPN connection availability through the use of active/passive VPN cluster servers at the Oracle Services Support centers. Any hardware or software issues on the active VPN server failover all connections to the backup VPN.
- Disaster recovery processes that use multiple clusters around the world. Any connection issue with one of the Oracle Services Support centers failover client connections to the other Oracle Services Support centers.

Figure 2-1 A TLS-Based VPN Client Connection from Oracle Advanced Services Gateway to Oracle



> **Note**
>
> The TLS VPN is the standard method for establishing the connection with Oracle. Alternative connection methods are available on an exception, customer-by-customer basis that is summarized in #unique_19/unique_19_Connect_42_GUID-9E64D6C9-5751-424D-B1BD-88B031C637A7. If you wish to explore these options further, please contact your Oracle Implementation Manager.

Alternative External Connection Option

Oracle offers an alternate method for establishing a connection using IPSec. The connection is terminated on the customer's existing VPN hardware. This option generally requires an extended implementation cycle and is approved on an exception basis. If the customer chooses to use their existing VPN device (for example, firewall or VPN concentrator) as a termination point, the VPN overall requirements described above remain the same. The encryption domain requirements for this connection will create a more complex configuration.

The requirements include, but are not limited to:

- A public IP per Gateway connection supplied by the customer for use inside the VPN encryption domain;
- Access to three /26 subnets and multiple /32 addresses inside the encryption domain;
- Network Address Translation (NAT) between the host and the Oracle resources over the tunnel is not supported (the Gateway must communicate directly to the public IP addresses inside the Oracle VPN.)

3 Audit Logging Feature

The Audit Logging Feature of Oracle Advanced Services Gateway provides audit information for three different categories of system events. The three categories are:

- Outbound Network Connections: The Linux firewall service (iptables) triggers notifications for all outbound network traffic with the exception of traffic to Oracle managed hosts used for monitoring and management (for example, Oracle VPN end points, dts.oracle.com, support.oracle.com).
- Outbound Login Activity: The Linux auditing service (auditd) triggers notifications for all outbound login attempts initiated from Oracle Advanced Services Gateway. This is done by monitoring usage of the ssh and telnet system binaries. Oracle Advanced Services Gateway sends a message that ssh or telnet has been used, by which user, and when. The destination is not provided. auditd logs contain that information. auditd logs are not directly accessible by the customer on Oracle Advanced Services Gateway.
- Inbound Oracle Advanced Services Gateway User Login Activity: The Linux auditing service (auditd) triggers notifications each time any of the system logs used for tracking logins is updated. This includes failed logins and successful login attempts. It also triggers a notification each time a user logs in from a remote system. These activities are monitored using auditd and forwarded to the customer's central logging system.

All audit notifications are delivered using standard syslog protocol. A central logging system must be provided to accept and process these messages.

The format of most of these messages is based on auditd. They can be managed using various auditd and related utilities.

The audit logging feature is disabled by default, and must be explicitly enabled through the Oracle Advanced Services Gateway command line interface (CLI). The details of how to configure this feature are explained in the following section:

Initial Login.

1. Use `ssh` to connect to Oracle Advanced Services Gateway.

   Use the customer administrator account configured at installation time or any other user with the customer administrator role.
2. At the first (CLI or CLISH) prompt, enter the password.
3. At the next prompt enter `configure terminal`.
4. At the next prompt enter `syslog`.

You are now in the syslog-specific section of the Oracle Advanced Services Gateway CLI where you can configure forwarding.

Table 3-1 Available Commands

Command	Description
help	To display a list of available commands.
?	To display a brief explanation of how to enter commands in the CLI.

Table 3-1 (Cont.) Available Commands

Command	Description

stat	To display the current configuration.
	This produces a display similar to the following:
	
	`------------- SyslogBroadcaster Configuration------------`
	`Message Forward Status = enabled`
	`Host IP Address = 1.2.3.4`
	`Host Port Number = 514`
	`Host Time Zone = GMT`
	`firewall Message Forward = enabled`
	`ssh Message Forward = enabled`
	`session Message Forward = enabled`
	`UID/GUID MapICMP Type 0 and 8 = enabled`
	
	`-------------------------------------------------------`

forward enable	To enable syslog forwarding.
forward disable	To disable syslog forwarding.
ip <*ip address*>	To enter the IP address of the remote syslog server (the one receiving the forwarded messages). You must enter a valid IP address, not a host name.
port <*port #*>	To change the port used for forwarding syslog messages.
timezone <*value*>	To set the time zone used in the forwarded syslog messages. Value must be -12 to +12 which is the offset from GMT.
mapping enable mapping disable	To convert the uid and guid contained in each message to the corresponding Unix user and group name.

Enabling and Disabling Logging Messages

The following paragraphs show the commands to enable and disable logging messages, and provide examples of the resulting messages.

In the examples below, user mapping is enabled: uid=#(*username*) and gid=#(*groupname*). In the event that user mapping is disabled, all instances of uid=# and gid=# are replaced with uid=0 and gid=0.

Any combination of the following three categories can be enabled or disabled.

Outbound Network Connectivity.

- To enable or disable this type of message forwarding:

```
firewall enable
firewall disable
```

These messages are generated by iptables and represent all outbound network traffic with the exception of traffic to known addresses used for Oracle monitoring.

The following example shows messages as they are seen on the system that receives the forwarded syslog messages.

Result from an `nslookup` command:

```
Jul 31 15:10:01 Jul-31 15: 10:01 GMT+00:00 0:0:0:0:0:0:0:1 NA:
sample-host kernel: iptables: IN= OUT=eth0 SRC=nn.nn.nn.nn
DST=nn.nn.nn.nn LEN=59 TOS=0x00 PREC=0x00 TTL=64 ID=33101 DF
PROTO=UDP SPT=30849 DPT=53 LEN=39 UID=jsmith GID=admin
```

Result from an `ssh` command:

```
Jul 31 15:13:22 Jul-31 15: 13:22 GMT+00:00 0:0:0:0:0:0:0:1 NA:
sample-host kernel: iptables: IN= OUT=eth0 SRC=nn.nn.nn.nn
DST=nn.nn.nn.nn LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=46937 DF
PROTO=TCP SPT=54842 DPT=22 WINDOW=14600 RES=0x00 SYN URGP=0 UID=jsmith
GID=admin
```

Outbound Login Activity

- To enable or disable this type of message forwarding:

```
ssh enable
ssh disable
```

The following example shows a message as it is seen on the system that receives the forwarded syslog messages.

Result from an `ssh` command:

```
Jul 31 15:22:15 Jul-31 15: 22:14 GMT+00:00 0:0:0:0:0:0:0:1 NA:
sample-host audispd: node=sample-host type=SYSCALL
msg=audit(1437567767.027:17839321): arch=c000003e syscall=59
success=yes exit=0 a0=124e030 a1=123d7f0 a2=1246d90 a3=10
items=2 ppid=22614 pid=25252 auid=54373 uid=jsmith gid=admin euid=54373
suid=54373 fsuid=54373 egid=501 sgid=501 fsgid=501 tty=pts4 ses=90594
comm="ssh" exe="/usr/bin/ssh"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key="gateway_audit"
```

Oracle Advanced Services Gateway User Login Activity.

- To enable or disable this type of message forwarding:

```
session enable
session disable
```

The following examples show messages as they are seen on the system that receives the forwarded Syslog messages.

Example of `ssh` being invoked on Oracle Advanced Services Gateway:

```
Aug 1 21:37:02 Aug-01 17: 37:02 GMT-04:00 0:0:0:0:0:0:0:1
NA: sample-host audispd: node=sample-host type=SYSCALL
msg=audit(1375393022.626:187186): arch=c000003e syscall=59 success=yes
exit=0 a0=7fa860e69380 a1=7fa860e697e0 a2=7fa860e69ca0 a3=0 items=2
ppid=1428 pid=12967 auid=4294967295 uid=jsmith gid=admin euid=0 suid=0
fsuid=0
egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="sshd"
exe="/usr/sbin/sshd" subj=system_u:system_r:sshd_t:s0-s0:c0.c1023
key="SESSION"
```

Result from an `su` command on Oracle Advanced Services Gateway:

```
Aug 1 21:42:49 Aug-01 17: 42:49 GMT-04:00 0:0:0:0:0:0:0:1
NA: sample-host audispd: node=sample-host type=SYSCALL
msg=audit(1437567906.700:17840209): arch=c000003e syscall=2 success=yes
exit=3 a0=7f691418c518 a1=2 a2=7f691418c760a3=fffffffffffffff0 items=1
ppid=22614 pid=25811 auid=54373 uid=54373 gid=501 euid=0 suid=0 fsuid=0
egid=501 sgid=501 fsgid=501 tty=pts4 ses=90594 comm="su" exe="/bin/su"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key="SESSION"
```