Oracle Machine Learning Secure Access via OCI Bastion Service

This guide shows how to configure network access and SSH port forwarding for a local browser to reach Oracle Machine Learning Notebooks behind a private endpoint on Autonomous AI Database Serverless through Oracle Cloud Infrastructure (OCI) Bastion.

Contents

Introduction

This guide walks you through accessing OML Notebooks on an Autonomous AI Database configured with private endpoint access. Since the database is not exposed to the public internet, you will establish an SSH tunnel through OCI Bastion to forward local traffic to the private endpoint on the standard HTTPS port 443. These steps assume your Autonomous AI Database and private endpoint are already configured. For details on configuring private endpoints, refer to the Autonomous AI Database Serverless documentation.

What is OCI Bastion?

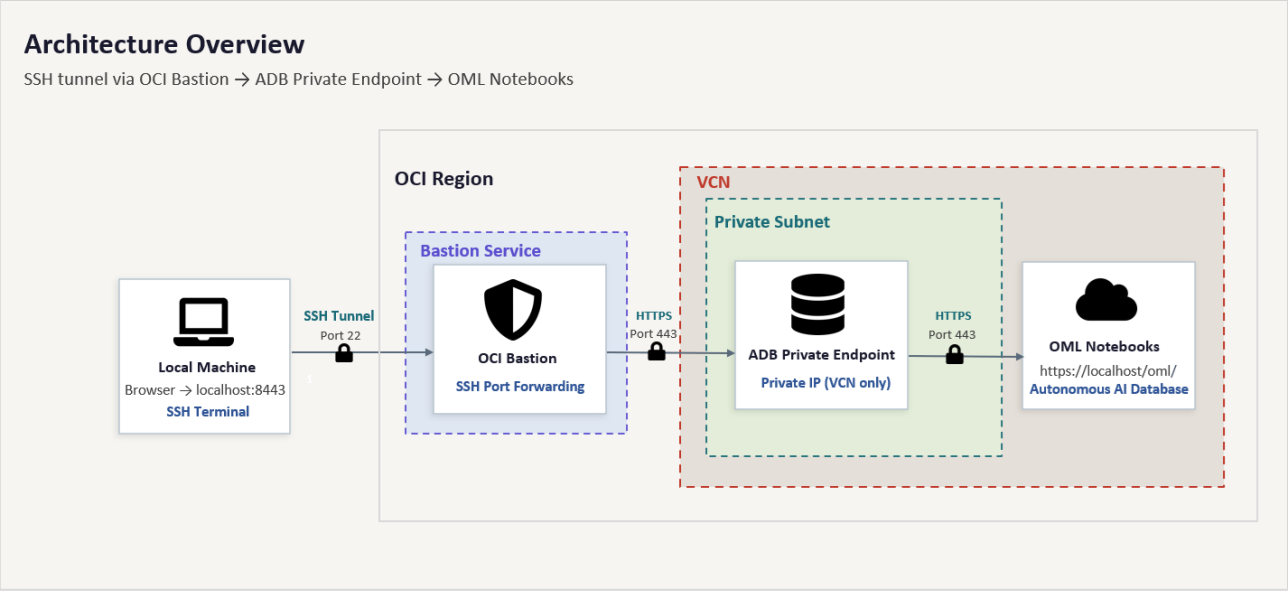
OCI Bastion is a fully managed jump host service that provides SSH access to private OCI resources without requiring a public IP address or a separately managed bastion virtual machine. A jump host is an "in-between" computer that you connect to first, and then from there you connect to the private server you actually want.

You would typically use Bastion when:

- Your target resource (such as an Autonomous AI Database private endpoint) lives entirely inside a VCN and has no public IP address.
- You need a controlled, audited ingress path without permanently modifying security lists or NSG rules.
- You want time-limited sessions. Bastion sessions expire automatically, limiting the duration of access compared with persistent jump hosts.
- You want to avoid the operational overhead of provisioning and patching a jump host VM.

For more information, see the OCI Bastion documentation and the Bastion service overview.

Architecture Overview



Your local machine connects to an OCI Bastion session, which forwards traffic inside the VCN to the Autonomous AI Database private endpoint. Your browser sends requests to a local port, which are relayed over the tunnel to the OML HTTPS endpoint.

- Your local machine opens an SSH tunnel through OCI Bastion, an OCI-managed jump host that allows access to private endpoints without exposing them to the public internet.
- Traffic is forwarded to the Autonomous AI Database private endpoint over port 443.
- OML Notebooks are accessed through the local forwarded port.

Understanding the ports

Port 443 on the destination side is required. It is the standard HTTPS port that the Autonomous AI Database private endpoint listens on and cannot be changed. Port 22 is the standard SSH port that OCI Bastion expects for incoming connections. The local port, chosen as 8443 in this document, is the one value you can adjust. Other unprivileged ports will work, but 8443 is used because it is above 1024, the threshold below which most operating systems require elevated privileges to bind a port.

Prerequisites

- A private Autonomous AI Database provisioned in OCI
- OCI Bastion Service configured for the same VCN
- An SSH key pair for Bastion authentication
- An OCI compute instance deployed in the same VCN, accessible via the Bastion service, to serve as the SSH tunnel target.
- Permissions to view and manage networking, Bastion sessions, and Autonomous AI Database
- A terminal on Mac, Linux, or Windows with Windows Subsystem for Linux (WSL)/Git Bash

Section 1: Network Security Configuration

Locate the ADB private endpoint network path

1. Go to cloud.oracle.com and sign into the OCI console
2. Select the region where your Autonomous AI Database resides
3. In the Search bar, enter “Autonomous AI Database”
4. Select your compartment and database and scroll to the Network section
5. Note the private endpoint IP address, URL, VCN, and subnet, and any attached NSG

Add an ingress rule for HTTPS

The Autonomous AI Database private endpoint must allow HTTPS traffic from the Bastion path. If your private endpoint uses a Network Security Group (NSG), add the rule there. If not, update the relevant subnet security list. The source can be the Bastion subnet Classless Inter-Domain Routing (CIDR) or the Bastion private endpoint IP in /32 format, which restricts access to that IP only.

Field	Value
Direction	Ingress
Source Type	CIDR
Source	Bastion subnet CIDR or Bastion private endpoint IP/32
IP Protocol	TCP
Destination Port	443
Stateless	No

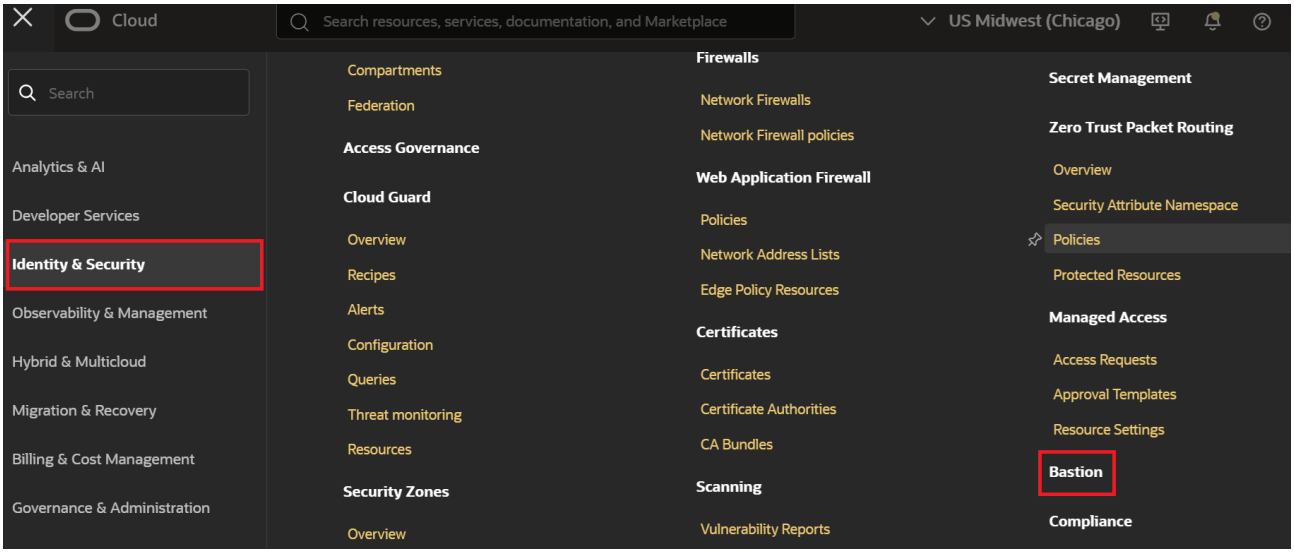
Understand CIDR notation

A value such as <BASTION-PRIVATE-IP>/32 means a single IP address. In OCI security rules, the source field is entered in CIDR format, so /32 is how you specify one exact host. If you allow the whole Bastion subnet instead, use a placeholder such as <BASTION-SUBNET-CIDR>.

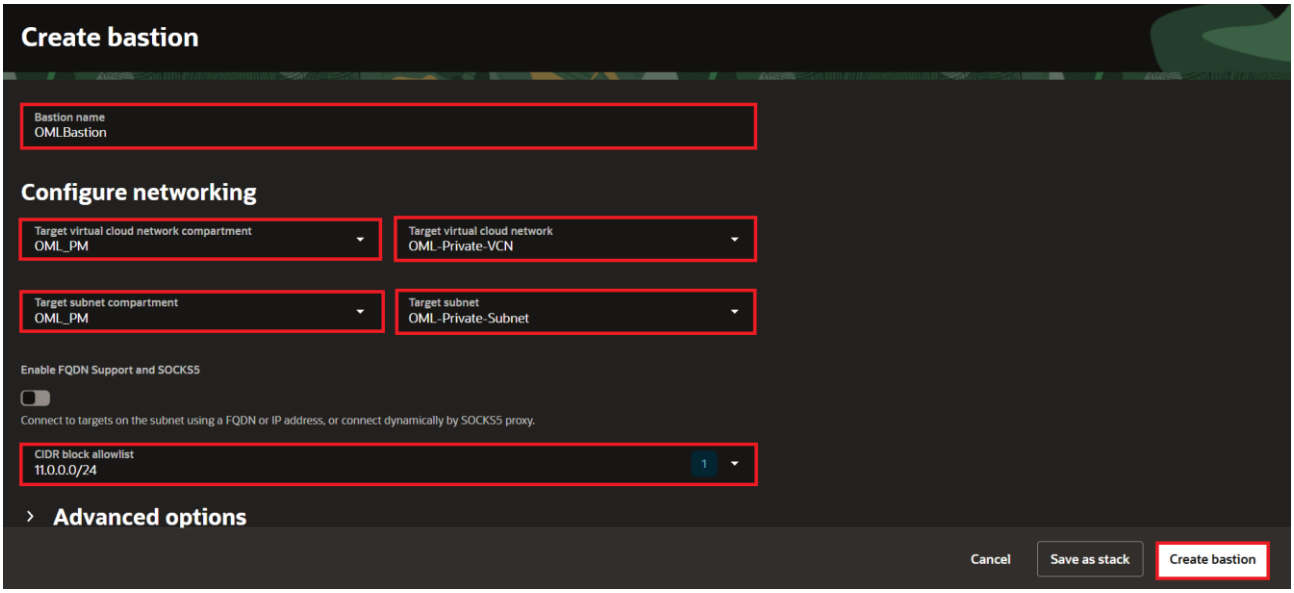
Section 2: Create the Bastion SSH Port Forwarding Session

Create the Bastion service

1. Log into cloud.oracle.com
2. From the three-line menu in the upper-left corner of the screen, navigate to Identity & Security, then Bastion. Alternatively, search for Bastion in the search menu.

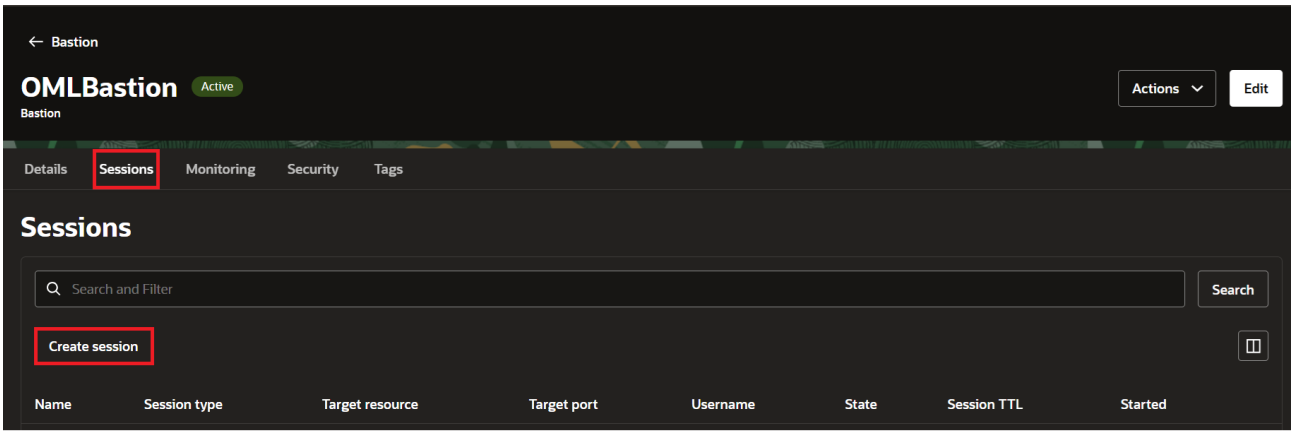


3. Click **Create Bastion** and enter a Bastion name
4. Under **Configure Networking**, select the target VCN compartment, VCN, subnet compartment, and subnet where your Autonomous AI Database private endpoint resides
5. Add a CIDR block allowlist to restrict which IPs can use this Bastion service
6. Click **Create Bastion** and wait for the service to become active

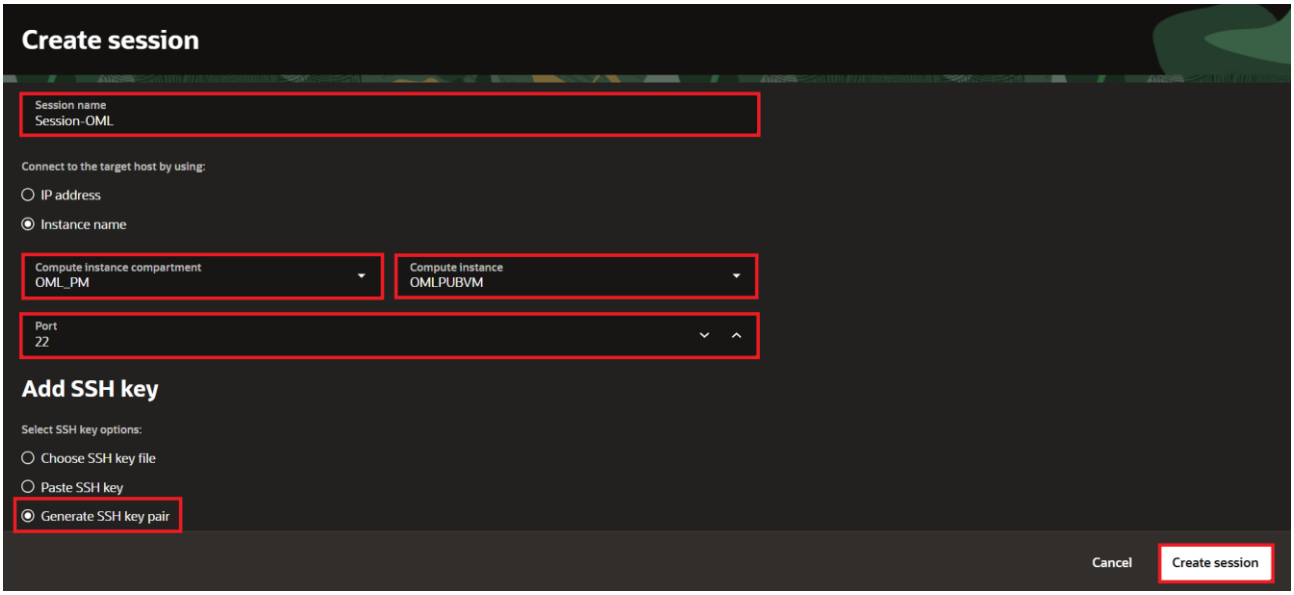


Create the Bastion session

1. From the Bastion service, click **Sessions**, then **Create session**

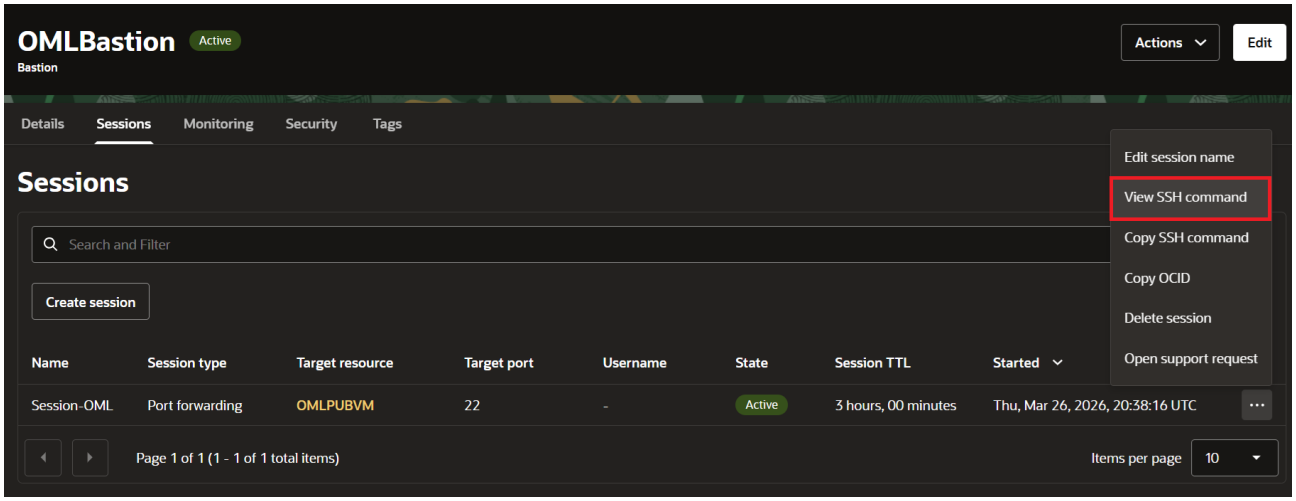


2. Select **Instance name** as the target connection type, then choose the compartment and OCI compute instance that resides in the same VCN as your Autonomous AI Database private endpoint
3. Set the SSH port to 22
4. Choose the option to generate an SSH key pair if you do not have one
5. Add your SSH public key and select **Create session**



Retrieve the generated SSH command

1. Wait until the session state is Active
2. Open the session menu and select View SSH command
3. Copy the generated command and use it as the starting point



Note, the generated command uses local port 443. In the next step you will optionally change this to 8443 to avoid requiring elevated privileges on your local machine.

Section 3: Establish the SSH Tunnel from Your Local Machine

Use a non-privileged local port first

For initial testing, optionally use a local port such as 8443 instead of 443. This avoids requiring elevated privileges on your local machine and makes troubleshooting easier. Once the tunnel works, you can decide whether you need a different port mapping.

Using port 8443 locally does not affect security. The SSH tunnel is encrypted regardless of which local port you choose, and traffic from Bastion to the Autonomous AI Database private endpoint still travels over HTTPS on port 443.

Build the SSH command

The SSH command template is:

```
ssh -i <path to private key> -N -L <local port>:<ADBS-private-endpoint-IP>:443 -p 22
<bastion-session-ocid>@host.bastion.<region>.oci.oraclecloud.com
```

Example SSH command

Replace the template values with your specific values. For example:

```
ssh -i /home/opc/myprivatekey.pem -N -L 8443:10.0.0.157:443 -p 22
ocid1.bastionsession.oc1.iad.amaaaaaaqztqlnaafosanmsy7cs7o7hgeodzfnappxbamybd9x3bod62noka
@host.bastion.us-ashburn-1.oci.oraclecloud.com
```

Expected terminal behavior

After authentication succeeds, the terminal will appear idle. Do not close it. The SSH tunnel is active and running in this session. Closing the terminal or interrupting the process will immediately drop the tunnel and disconnect your browser from OML Notebooks.

Section 4: Access OML Notebooks in Your Browser

Open the OML URL

```
https://localhost:8443/oml/
```

Because the service certificate belongs to the Autonomous AI Database hostname rather than localhost, your browser may display a certificate warning. That warning is expected in this local-forwarding scenario.

Sign into OML Notebooks

When signing into OML Notebooks, you will be prompted to enter the following information: the full tenancy OCID, database name, and database username and password.

Troubleshooting

Tunnel does not connect

- Confirm the Bastion session is Active.
- Verify you used the correct SSH private key.
- Confirm the target IP in the session and the SSH command matches the Autonomous AI Database private endpoint IP.
- Run the SSH command with -v to see connection details.

Browser times out

- Verify that the ingress rule allows TCP 443 from the Bastion path to the ADB private endpoint.
- Test the tunnel in a second terminal with curl -vk https://localhost:8443/oml/.
- Confirm that the route tables and security rules allow VCN connectivity between Bastion and the database private endpoint.

Permission denied on local port

If you try to bind local port 443, your operating system may require elevated privileges. Use 8443 during setup and troubleshooting so you can focus on network validation rather than local privilege issues.

HTTP 404 error

Use the full OML path with the trailing slash: https://localhost:8443/oml/. Testing https://localhost:8443/ords can also help confirm that the tunnel is working even before you sign in to OML.