ORACLE

Cloud Infrastructure

Roving Edge Device Setup Guide

December 12, 2024

Contents

Setting Up Oracle Roving Edge Device

Set up the Roving Edge Device at your location, and configure the device to connect to your Oracle Cloud Infrastructure tenancy so that it serves as an extension of your tenancy.

> **Note:**
>
> These setup instructions apply to the following device models:
>
> - Roving Edge Device Compute (shape name: **RED.2.56**)
> - Roving Edge Device GPU (shape name: **RED2.56.GPU**)
> - Roving Edge Device Storage (shape name: **RED.2.56.STG**)
> - Roving Edge Device 1 (shape name: **RED.GPU.1.RX1.40**)

To display a PDF of this *Roving Edge Device Setup Guide* that you can save to your local computer, click: Roving Edge Device Setup Guide PDF

Perform the following tasks to set up the Roving Edge Device:

Task	Link
1	Receive and Inspect the Shipment on page 3
2	Remove the Ruggedized Case End-Caps on page 5 or Mount the Device in a Rack on page 7
3	Cable the Roving Edge Device on page 10
4	Set Up Terminal Emulation on page 12
5	Power On the Device
6	Configure Network Parameters on page 13
7	Unlock the Device on page 13
8	Download the Root CA Certificate on page 15

Related Resources

- Roving Edge Infrastructure Device Specifications
- Safety and Compliance Resources:
  -
  -

What's next?

Receive and Inspect the Shipment on page 3

Receive and Inspect the Shipment

Carefully inspect the Roving Edge Device shipment before you unpack the shipment.

> **Important:**
>
> Report any damage or concerns to Oracle using a Service Request ticket. See Getting Help and Contacting Support and My Oracle Support.

Obtain Shipment Details

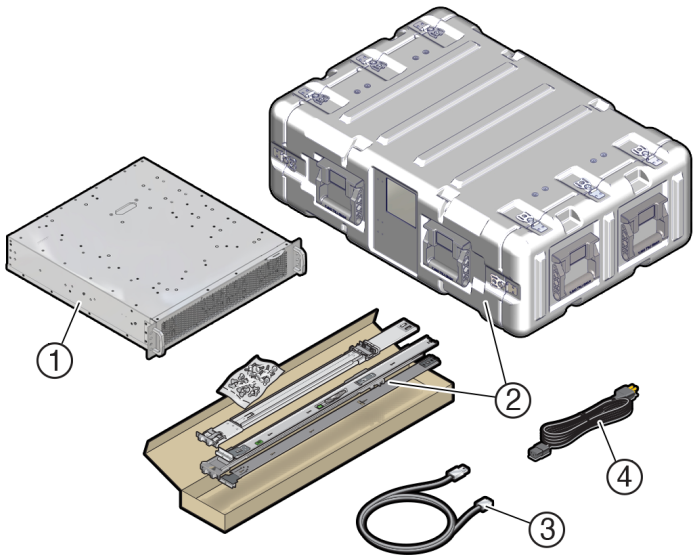
Perform these steps to gather information you can use to inspect the shipment and ensure a tamper free device.

1. Sign in to your Oracle Cloud Infrastructure (OCI) tenancy.
2. From the console navigation menu, click **Hybrid**, then click **Roving Edge Infrastructure**.
3. Select the compartment for this device.
4. Click **Manage Nodes**.
5. Click the node name to display the details page, and make note of these details:
   - Device request is updated to a *Delivered* status
   - The date and time it was received
   - The serial number

Inspect the Shipment

1. Visually inspect the device shipping container for any damage, tampering, or missing ties before opening it.
2. Compare the serial number that appears on all the security ties with the serial number listed for the device in your tenancy.
3. Unpack and visually inspect the device for any tampering or damage.
4. Ensure that you've received all the shipping kit contents, as shown in the following illustration.

> **Note:**
>
> The device ships with either a ruggedized case or a rackmounting kit based on what was specified when the device node was created. See Creating a Roving Edge Infrastructure Device Node.



No.	Item
1	Roving Edge Device

2	One of the following:
	• Ruggedized case
	• Rack mounting kit with the following items:
	  • Two mounting brackets inside two slide-rails
	  • 4 M4 screws

No.	Item
3	USB-to-DB-9 serial cable For devices with ruggedized cases, the cable is in a pouch inside the rear of the case.
4	AC power cord For devices with ruggedized cases, the power cord is in a pouch inside the rear of the case.

What's next?

- If your device is inside a ruggedized case, see Remove the Ruggedized Case End-Caps on page 5.
- If the device isn't in a ruggedized case, install your device in a rack. See Mount the Device in a Rack on page 7.

Remove the Ruggedized Case End-Caps

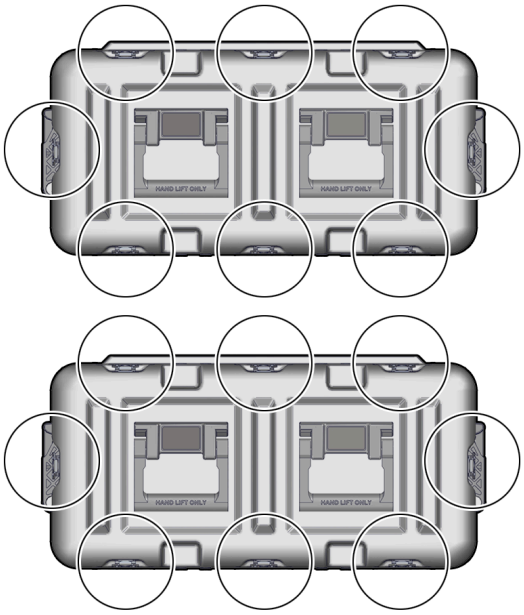
If the Roving Edge Device is in a ruggedized case, you must remove the front and rear end-caps to access the cable connectors. The end-caps remain removed during operation.

> **Caution:**
>
> Don't remove the Roving Edge Device from the case. Doing so can damage the device.

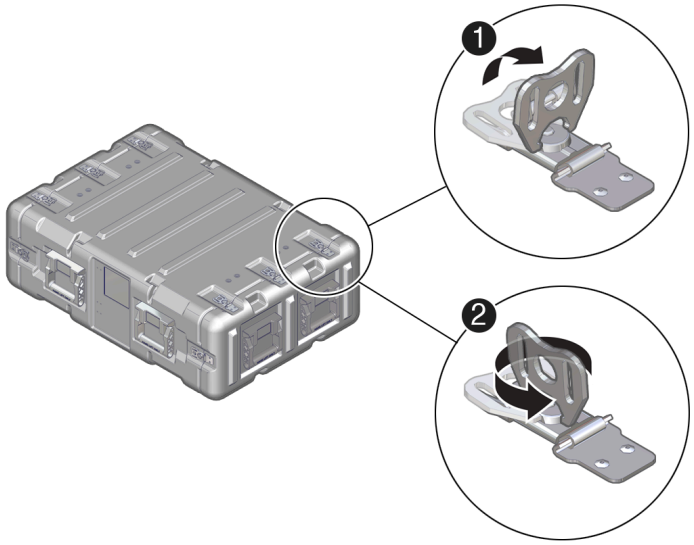
> **Caution:**
>
> Leave the end-caps removed during operation to ensure adequate airflow. Reinstall the end-caps only when the device is powered down.

1. On the front and rear of the ruggedized case, find the 16 wing-turn latches.

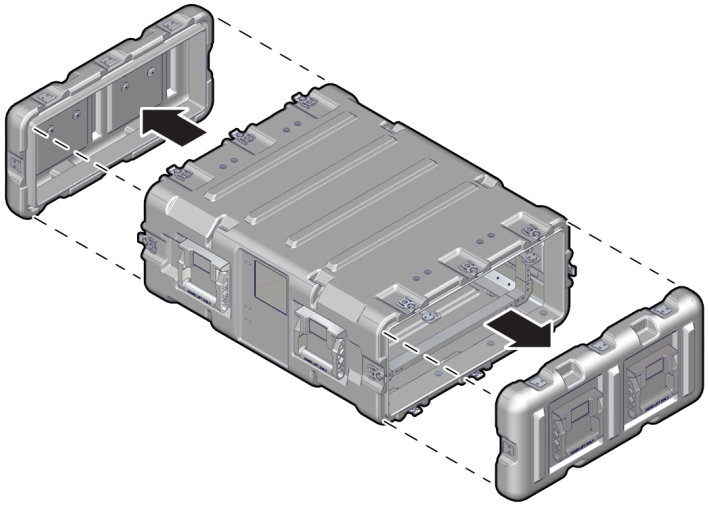
   Note: The rear end-cap has casters.



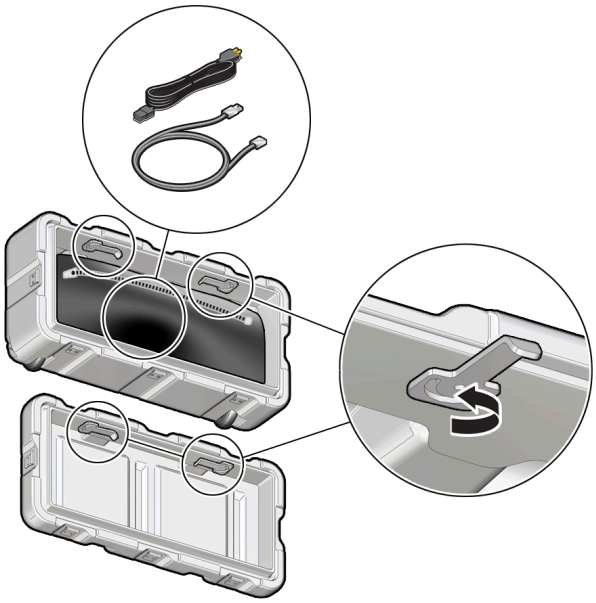
2. Open all 16 wing-turn latches on the front and rear of the case by lifting the latch then turning the latch counterclockwise.



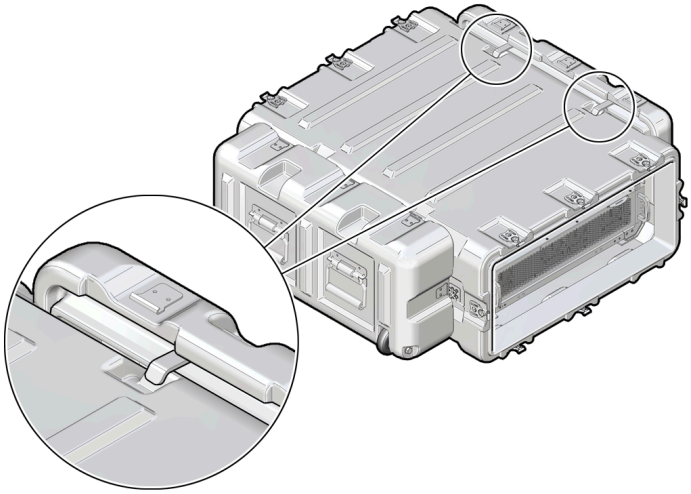
3. Remove the front and rear end-caps.



4. Remove the cable pouch, and extend the end-cap hooks.



5. Hang the end-caps on the sides of the ruggedized case.



What's next?

Rear Panel Identification

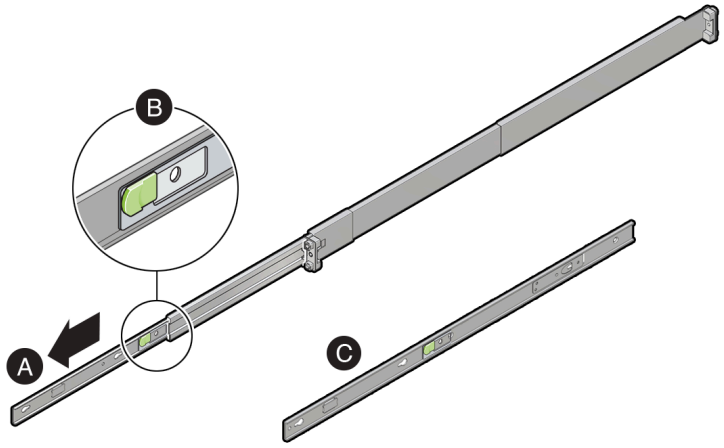
Mount the Device in a Rack

Use these instructions if you plan to mount your Roving Edge Device in a standard rack.

The optional rackmount kit can be used to install the device in a four-post, 19-inch standard rack.

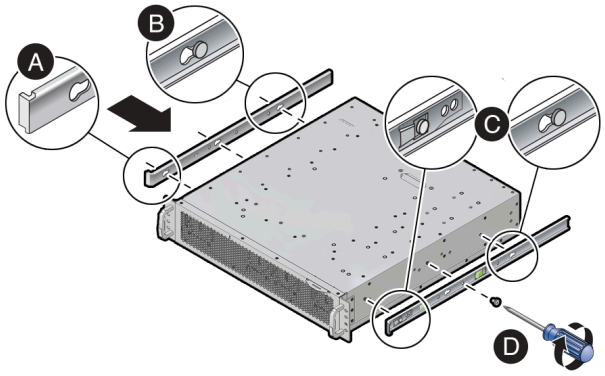
Rackmounting the Device

1. Separate the device mounting brackets from the slide-rails.



   a. Pull the mounting brackets out of the slide-rail brackets.
   b. Press the release lever to release the locking mechanism.
   c. Remove the mounting brackets from side-rails.

2. Attach the mounting brackets to the device.



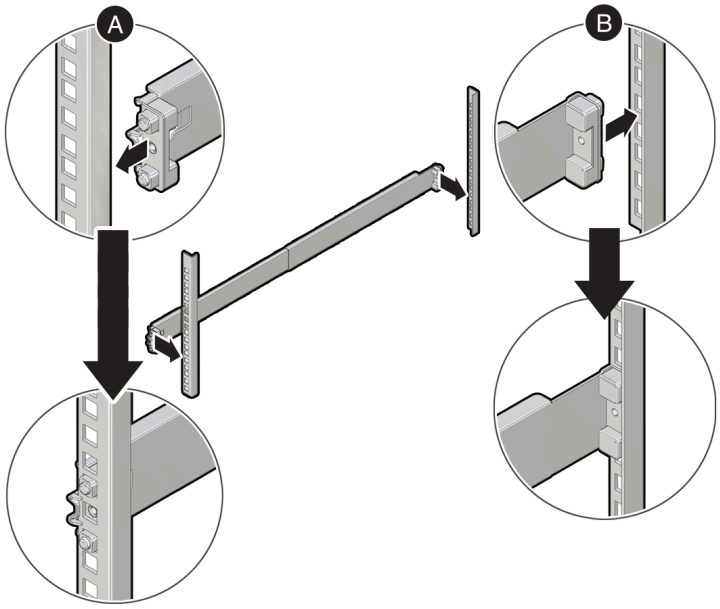
   a. Position the mounting brackets against the device so that the slide-rail stop is at the front of the device.
   b. Line up the keyhole openings on the mounting bracket with the locating pins on the side of the device.
   c. Push the mounting brackets forward until they lock in place with an audible click.
   d. Secure the mounting brackets by installing one M4 screw to each side of the device.

3. Identify the location in the rack where you want to place the device.

   Roving Edge Device requires two rack units (2U) of vertical space.

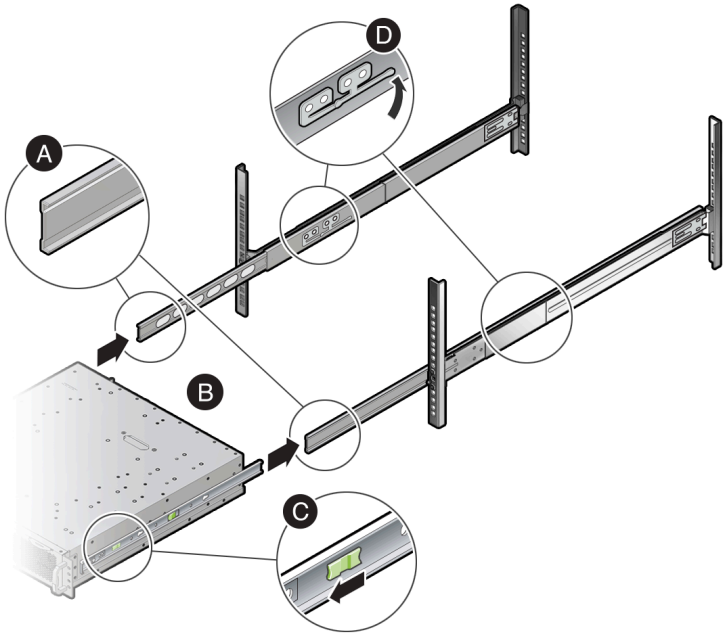
   > **Caution:**
   >
   > To reduce the risk of personal injury, stabilize the rack cabinet, and if available, extend the anti-tilt bar before you install the server.

4. If your rack posts aren't labeled, mark the mounting holes on the front and rear posts to ensure a level installation.
5. Attach the two slide-rails to the rack.



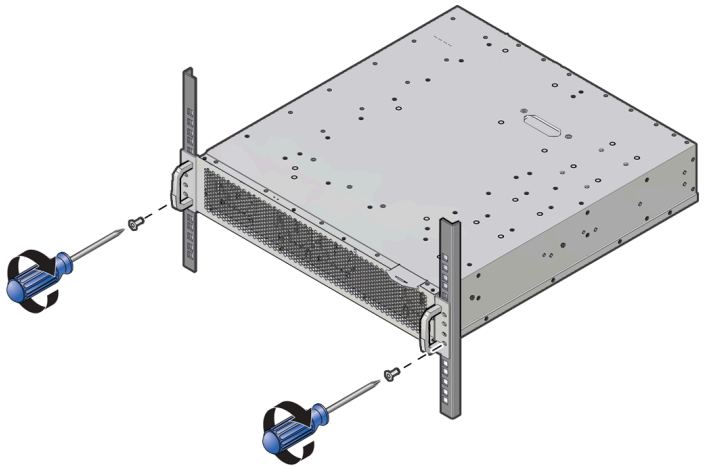
a. Snap the front slide-rails into the front rack posts.
b. Adjust the rear slide-rails to reach the rear rack posts, then snap the slide-rails into the rear rack posts.

6. Install the device into the slide-rails.



a. Extend the inner-front slide-rails.
b. Slide the mounting brackets into the extended slide-rails until the device is securely supported by the slide-rails, but is extended from the rack.
c. Pull the green lever forward to enable the mounting brackets to slide fully into the slide-rails.
d. Lift the slide-rail stop lever and push the device completely into the rack.

7. Install two M4 screws to the front of the device.



What's next?

Rear Panel Identification

Cable the Roving Edge Device

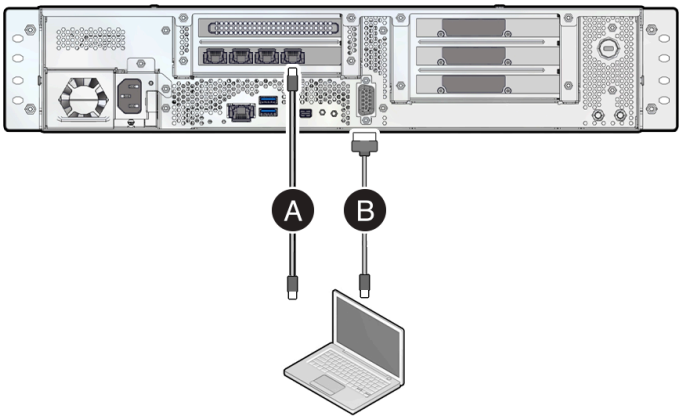
Use the following diagram to locate connectors on the rear of the Roving Edge Device 2 as you connect cables in this procedure.

> **Note:**
>
> To meet MIL-STD-461 Rev G RE102 requirements, all Ethernet network cables attached to the Roving Edge Device must be CAT8 rated. Otherwise, the minimum requirement for Ethernet cables is CAT6.

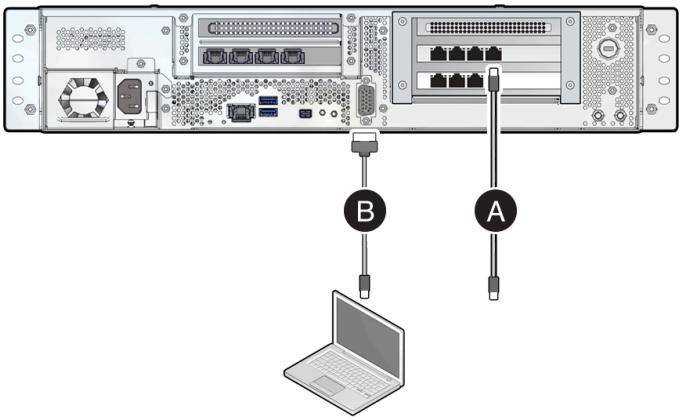
> **Note:**
>
> The Ethernet connections described in this section are the minimum Ethernet connections you need to make to set up the device. You can use the other NIC ports and configure Ethernet bonding. See Rear Panel Identification and Managing Ethernet Bonding.

1. Connect cables to the default Ethernet port and to the serial console port as shown in the following diagrams.
   a. Use a 10GBaseT RJ-45 Ethernet cable to connect the device Ethernet port to your Ethernet switch.
   b. Connect the provided USB-to-DB-9 Ethernet cable from the device DB-9 serial console port to a USB connector on your controlling host, such as a laptop.

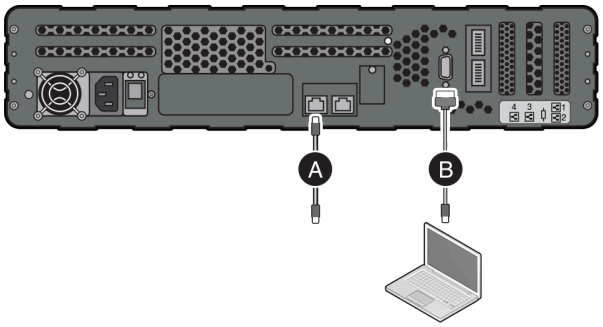
Roving Edge Device 2, GPU and Storage Shape



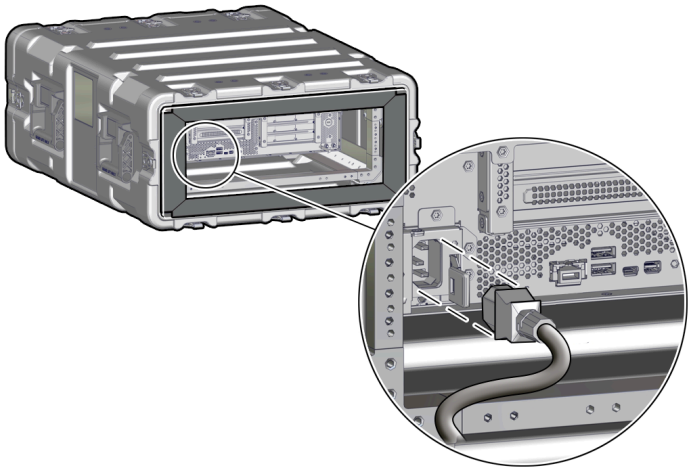
Roving Edge Device 2, Compute Shape



Roving Edge Device 1



2. Connect the provided power cord to the device power receptacle and to your power source, but don't power on the device yet.



What's next?

Set Up Terminal Emulation on page 12

Set Up Terminal Emulation

Your initial communication with the Roving Edge Device is made through the serial console that's connected to a controlling host computer, such a laptop. The controlling host must have terminal emulation software that's configured as described in this section.

We recommend the following terminal emulation software based on your host operating system:

Microsoft Windows: **PuTTY**

Mac OS X: **ZOC** or **screen** (for example: screen /dev/ttyusbserialX 115200)

Linux: **PuTTY**, **Minicom**, **screen** (for example: screen /dev/ttyUSBX 115200)

1. Based on your host OS, use the appropriate method to ensure that the `pl2303` USB driver is installed. This USB driver is required for connectivity to the Roving Edge Device DB-9 serial port.

   The USB driver is preinstalled on Oracle Unbreakable Enterprise Kernel. The following command shows that the USB driver is present:

   ```
   [root@localhost ~]# modprobe pl2303
   [root@localhost ~]# lsmod | grep -i pl2303
   pl2303                 24576  0
   [root@localhost ~]# modinfo -d pl2303
   Prolific PL2303 USB to serial adaptor driver
   ```

   If the driver isn't installed, use the appropriate method to install the driver. For example, go to the Microsoft Windows or Apple store to obtain and install the driver.
2. Configure the terminal emulator software settings as follows:
   - Terminal Type: **VT100+**
   - Bits per second: **115200**
   - Data Bits: **8**
   - Parity: **None**
   - Stop Bits: **1**
   - Flow Control: **None**

> **Note:**
>
> With PuTTY, you can't configure all these settings individually. However, you can configure the PuTTY default settings by selecting the Serial connection type and specifying 115200 for the Serial Line baud speed. This configuration is sufficient to use PuTTY as a terminal emulator for the device.

What's next?

Power On the Device

Unlock the Device

Roving Edge Device arrives in a locked state. You must unlock the device using an unlock passphrase when you power on the device.

The passphrase was created when you created the device node, as described in Creating a Roving Edge Infrastructure Device Node.

> **Note:**
>
> Anytime you reboot the device, it reverts to a locked state. Receiving a `Device is locked` message after trying to connect to an API endpoint is indicative that the device is in a locked state. Unlock the device to proceed.

> **Note:**
>
> If your device is unexpectedly in a locked state, it might have accidentally rebooted. Check that your power connection is steady and not inadvertently causing device reboots.

1. From the serial console **Configure Networking** screen, select **Go Back** to return to the main serial console menu.
2. Select **Unlock Device**.

   In the terminal emulator, you're prompted for the passphrase.
3. Enter the unlock passphrase to unlock the device.

   The device is unlocked, and the serial console menu is displayed.

What's next?

Download the Root CA Certificate on page 15

Configure Network Parameters

Configure the Roving Edge Device network settings through your controlling host that's connected to the serial port.

> **Note:**
>
> For a list of serial console commands, see Operating the Serial Console

The following procedure describes how to configure the minimum network parameters that are required during the initial device setup. For more network configuration information, see Managing the Network.

The minimum network parameters that you need to configure are as follows:

- Device IP address, subnet, and gateway.
- DNS
- NTP

1. From the controlling host terminal window, select the **Configure the Network** menu option. The following options are displayed:
   - **Set Node IP Settings (Current Node Only)**: Set the node IP address, subnet mask, and default gateway.
   - **Display Settings**: Show the current network settings.
   - **Set Public IP Pool Range for Compute Instances**: Set the external IP address pool for compute instances.

     IP addresses are allocated from this pool when an instance is created with public IP address assigned to it.

     Important – This operation removes the current external IP address pool, and replaces it with the ranges from the new input.

     The best practice is to use a contiguous range of IPs. An ideal range is a CIDR range such as 10.10.0.0 - 10.10.0.15, which corresponds to 10.10.0.0/28, which is what is stored internally.

     If you're updating your public IP pool range, none of the IPs in the existing range can be allocated to a compute instance during the operation. The best practice is to ensure all public IPs are dissociated with all compute instances before updating your public IP pool range.
   - **Display Public IP Pool Status**: Show the current public IP pool range.
   - **Control Network Ports**: Enable or disable network ports.
   - **Configure DNS**: Configure the DNS servers for the current node control plane. Reboot the device for the DNS configurations to take effect, if the device is already unlocked.
   - **Configure Subnet Gateway**: Configure the gateway for a given subnet. The destination can be the default IGW or a private IP Address. You can perform the following tasks:
     - **Show Configuration**: Show the current subnet gateway configuration. The output shows whether the destination is IGW or a private IP address for each subnet.
     - **Update Configuration**: Update the current subnet gateway configuration. For example:

```
-------------------------------------------------------------------------------
Idx  Subnet CIDR      DNS Label     Gateway
-------------------------------------------------------------------------------
1    10.0.1.0/24      Subnet-1      10.0.2.2
2    10.0.2.0/24      Subnet-2      IGW
3    10.0.3.0/24      Subnet-3      IGW

Enter Subnet Index: 1
Enter the gateway (IGW or private IP address) for this subnet:
```

   - **Configure NTP**: Perform the following NTP configuration tasks:
     - **Display NTP Configuration**: Configure external NTP servers. For example:

```
Local Time and RTC
Local time: Fri 2022-05-13 04:26:41 UTC
Universal time: Fri 2022-05-13 04:26:41 UTC
RTC time: Fri 2022-05-13 04:26:43
Time zone: UTC (UTC, +0000)
NTP enabled: n/a
NTP synchronized: no
RTC in local TZ: no
DST active: n/a
```

     - **Update NTP configuration**: Identify the primary and secondary servers that set up the NTP configuration for the device.
   - **Reset Network**: Reset the network by erasing all the network configurations such as Node IP, Public pool, DNS, NTP, and Gateway.
   - **Help**: Display online help for the **Network Configuration** menu options.
   - **Go Back**: Return to the main serial console menu.
2. Use the menu options to configure the device network parameters according to your network environment. At minimum, configure these parameters:

- Network settings
- DNS
- NTP

3. If you need to configure other network parameters like network bonding, see Managing the Network.

What's next?

(Optional) To configure Ethernet bonding, see Managing Ethernet Bonding. Otherwise, go to Unlock the Device on page 13.

Download the Root CA Certificate

To access the Device Console, the computer (host) that you use to access the Device Console must have the root CA certificate from the Roving Edge Device. The root CA certificate is the top most certificate in the certificate chain of trust and is used by your computer to verify the authenticity of the Device Console.

Perform the tasks in this section to download the root CA certificate and sign in to the device UI for the first time.

Prerequisites

To perform the tasks in this section, you need the following Roving Edge device items:

- IP address
- hostname
- User name
- Password

Oracle provides these items to your organization when Oracle provisions your device request.

Ensure Your Host Has OpenSSL Installed

Most Linux and MacOS computers have OpenSSL installed. For Microsoft Windows, you might need to install OpenSSL.

To determine if OpenSSL is installed on Microsoft Windows, search for openssl. If OpenSSL isn't installed, follow your organization's best practices for installing OpenSSL.

The following links take you to popular OpenSSL sites from which OpenSSL can be obtained:

-
-
-

Task 1 - Configure the hosts File

Adding the device IP address and hostname to the hosts file enables your computer to find the Device Console IP address regardless of the DNS configuration.

Use one of the following procedures based on your OS.

Linux

1. In a text editor, open the `/etc/hosts` file. The following example uses the `vim` editor:

```
sudo vim /etc/hosts
```

2. Enter your administrator password.
3. Open a new line and enter the device IP address and hostname. Example:

```
198.168.0.1    my-1234567  my-device-hostname
```

4. Save the `/etc/hosts` file.

MacOS

1. Open a terminal:

   Navigate to **Finder** > **Utilities**, then click **Terminal**.
2. Open the `/etc/hosts` file in a text editor. The following example uses the nano editor:

   ```
   sudo nano /etc/hosts
   ```
3. Enter your administrator password.
4. Create a new line and enter the device IP address and hostname. Example:

   ```
   198.168.0.1    my-1234567  my-device-hostname
   ```
5. Save the `/etc/hosts` file.

Microsoft Windows

1. Open Notepad as the administrator.
2. In Notepad, open the following file:

   ```
   C:\Windows\System32\drivers\etc\hosts
   ```
3. Open a new line and enter the device IP address and hostname. Example:

   ```
   198.168.0.1    my-1234567  my-device-hostname
   ```
4. Save the `hosts` file.

Task 2 - Download the Root Certificate File from the Device

Use one of the following procedures based on your computer OS.

If your computer runs Microsoft Windows, also select the procedure based on your browser type.

Note - Browsers evolve over time. If some browser steps don't match what you see in your browser, consult your browser documentation.

Linux and MacOS

1. In a terminal window, use the following command to download the certificate from the Roving Edge device:

   ```
   echo -n | openssl s_client -showcerts -
   connect <device_ip_address>:8015 | sed -ne '/-BEGIN CERTIFICATE-/,/-
   END CERTIFICATE-/p' > $HOME/redroot.pem
   ```

   The root certificate `redroot.pem` is downloaded to your home directory.

Microsoft Windows with Firefox

The following steps are for Firefox version 115.

1. In the browser address field, enter the device address and port number:

   ```
   https://<device_hostname>:8015
   ```

   If a security risk warning is displayed, accept the risk, and ignore the warning: `Roving Edge Device is currently unavailable`.
2. Click the padlock symbol that's to the left of the browser address bar.
3. In the Site Information dialog box, click **Connection Secure**, then click **More information**.

   The Firefox Security menu is displayed.

4. Click **View Certificate**.

   The Device Console now displays certificate information.
5. Click the tab called <*hostname*>**-root-CA** .
6. Scroll down to the **Miscellaneous** section.
7. Click the **PEM (Cert)** link, and save the file somewhere convenient such as the Downloads folder.

Microsoft Windows with Edge

The following steps are for Microsoft Edge version 128.0.2739.67.

1. In the browser address field, enter the device address and port number:

   ```
   https://<device_hostname>:8015
   ```
2. Click the secure icon next to the URL.
3. Click **Certificate** or **Manage Certificate**.
4. Click **Details**.
5. Click **Export**.
6. Browse to a convenient download location such as Downloads.
7. Click **Save**.

   The root certificate file is saved with a `.crt` extension.

Microsoft Windows with Chrome

The following steps are for Google Chrome version 128.0.6613.120.

1. In the browser address field, enter the device address and port number:

   ```
   https://<device_hostname>:8015
   ```
2. Click the secure icon next to the URL.
3. Click the **Certificate is not valid** icon.
4. Click the **Details** tab.
5. Click **Export**.
6. Browse to a convenient download location such as Downloads.
7. Click **Save**.

   The root certificate file is saved with a `.crt` extension.

Task 3 - Import the Root Certificate into Your Browser

Import the downloaded root certificate into your browser using one of the following tasks based on your browser type.

Note - Browsers evolve over time. If some browser steps don't match what you see in your browser, consult your browser documentation.

Firefox

1. In Firefox, use the navigation menu to open **Settings**.
2. In the **Find in Settings** field, enter `certificates`.
3. Click **View Certificates**.

   The Certificate manager is displayed.
4. With the **Authorities tab** selected, click **Import**.

   Browse to the location of the downloaded certificate file, select it, then click **Open**.
5. In the Certificate Manager, click **Trust this CA to identify websites**, then click **OK**.
6. In the Certificate Manager, click **OK**.
7. Refresh the browser tab that's connected to the device.

You're prompted to enter your user name and password.

Edge

1. In Edge, use the navigation menu to open **Settings**.
2. In the **Find in Settings** field, enter `certificates`.
3. Click **Manage certificates**.

   The Certificate manager is displayed.

   a. In the **Certificates** dialog box, click **Import**.
   b. In the **Import Wizard**, click **Next**.
   c. Click **Browse**, and navigate to the location of the downloaded certificate file.
   d. In the **file type** drop-down menu, select **All Files**.
   e. Select your downloaded certificate file, and click **Open**.
   f. Click **Next**.
   g. Select **Automatically select the certificate store based on the type of certificate**.
   h. Click **Next**.
   i. Click **Finish**.
   j. Click **OK**.
   k. In the **Certificate manager**, click **Close**.

   Now you can sign in to the Device Console.
4. Refresh the browser tab that's connected to the device.

   You're prompted to enter your user name and password.

Chrome

1. In Chrome, use the navigation menu to open **Settings**.
2. In the **Search settings** field, enter `certificates`.
3. Click **Security**.
4. Click **Manage certificates**.

   The **Certificate manager** is displayed.
5. Select the **Trusted Root Certificates** tab.
6. Click **Import**.

   The **Certificate Wizard** is displayed.
7. Click **Next**.
8. Click **Browse**, and browse to the location of the downloaded certificate file, select it, then click **Open**.
9. Select **Automatically select the certificate store based on the type of certificate**, then click **Next**.
10. Click **Finish**.
11. Click **OK** to acknowledge the import was successful.
12. Close the **Certificate Wizard** by clicking **Cancel**.
13. In the **Certificates** dialog box, click **Close**.
14. Refresh the browser tab that's connected to the device.

    You're prompted to enter your user name and password.

What's next?

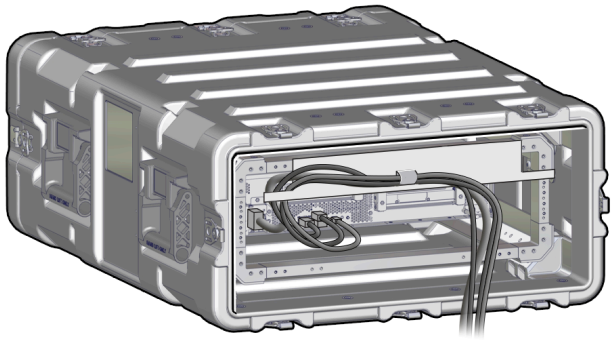
Go to the online Roving Edge Infrastructure documentation.

Learn about ways to access the device. See Accessing a Roving Edge Infrastructure Device.

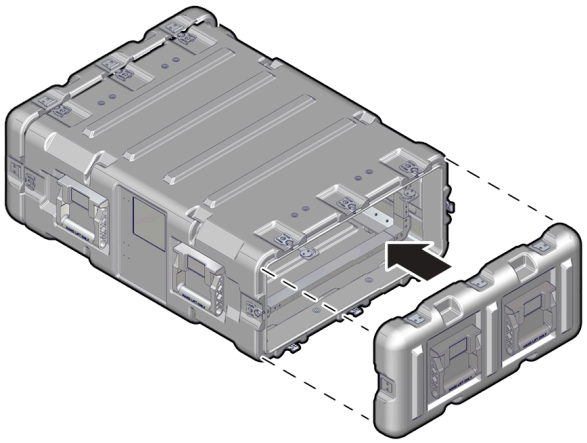
Reinstall the Ruggedized Case End-Cap

If you removed the ruggedized case end-cap, use these instructions to reinstall it.

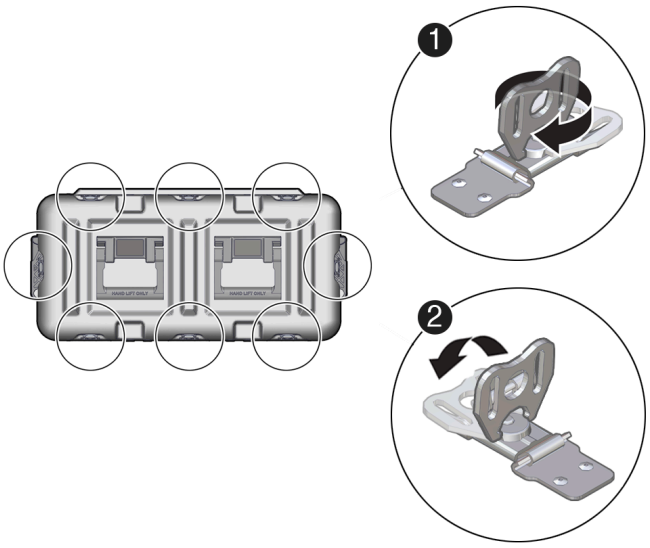
1. Route cable slack through the foam channels.



2. Replace the end-cap.



3. Secure the end-cap by latching eight wing-turn latches (turn clockwise, then close).



What's Next

- Roving Edge Infrastructure documentation home page
- Getting Started with Roving Edge Infrastructure