ORACLE

Cloud Infrastructure

Roving Edge Device Setup Guide

March 09, 2026

Contents

Setting Up an Oracle Roving Edge Device

Learn how to set up, configure, and install the Roving Edge software on a Roving Edge Device.

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

Use one of the following task tables based on the Roving Edge model:

- Roving Edge Device Setup Tasks on page 3
- Roving Edge Ultra Setup Tasks on page 3

Roving Edge Device Setup Tasks

> **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**)

Task	Link
1	Receive and Inspect the Shipment on page 4
2	Remove the Ruggedized Case End-Caps on page 6 or Mount the Device in a Rack on page 9
3	Identify Front and Rear Panel Items
4	Cable the Roving Edge Device on page 11
5	Set Up Terminal Emulation on page 13
6	Power On the Device
7	Self-Provision the Device or For Roving Edge Device 1 and any devices that were provisioned at Oracle, see Configure Network Parameters for a Factory Provisioned Device.
8	Unlock the Device on page 14

Roving Edge Ultra Setup Tasks

> **Note:**
>
> These setup instructions apply to Roving Edge Ultras:

Task	Link
1	Receive and Inspect the Shipment on page 4

Task	Link
2	Assemble Roving Edge Ultra
3	Identify Front and Rear Panel Items
4	Cable the Roving Edge Device on page 11
5	Set Up Terminal Emulation on page 13
6	Power On the Device
7	Self-Provision the Device
8	Unlock the Device on page 14

Related Resources

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

What's next?

Receive and Inspect the Shipment on page 4

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 Support Request ticket. See
> .

Confirm Ordering and Shipping Details

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

1. Sign in to your Oracle Cloud Infrastructure (OCI) tenancy.
2. From the console navigation menu, select **Hybrid**, then select **Roving Edge Infrastructure**.
3. Select the compartment for this device.
4. Select **Manage Nodes**.
5. Select 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

> **Note:**
>
> For devices that are self-provisioned, the serial number isn't available in the node until the device has connectivity to your tenancy, as described in Set Up Connectivity to OCI. If you don't see a serial number in the node, skip this step. You're instructed to verify the serial number later during self-provisioning.

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 node in your tenancy. **Note**: Skip this step for self-provisioned devices.

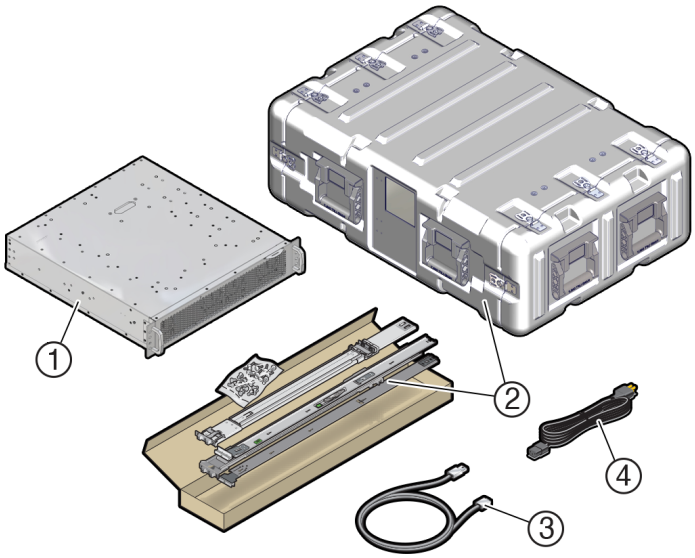
> **Note:**
>
> On Roving Edge 2 devices, the serial number is located on the pullout card on the front of the device. See Roving Edge Device 2 – Front Panel.

3. Unpack and visually inspect the device for any tampering or damage.
4. Ensure that you've received all the shipping kit contents. See one of the following inventory sections:

- Roving Edge Device Shipment Inventory on page 5
- Roving Edge Ultra Shipment Inventory on page 6

Roving Edge Device Shipment Inventory

> **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 Device 1 Node (Deprecated).



No.	Item
1	Roving Edge Device (GPU, Compute, or Storage model)

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

3	USB-to-DB-9 serial cable For devices with ruggedized cases, the cable is in a pouch inside the rear of the case.

No.	Item
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 6.
- If the device isn't in a ruggedized case, install your device in a rack. See Mount the Device in a Rack on page 9.

Roving Edge Ultra Shipment Inventory

Each Roving Edge Ultra includes the following items:

- Roving Edge Ultra
- Battery
- KVMA ruggedized power adapter
- RJ-45 to DB-9 to USB cable
- RJ-45 to CAT5/6 cable
- AC power cord
- Rugged transportation case

What's next?

For Roving Edge Ultra, see Assemble Roving Edge Ultra.

Remove the Ruggedized Case End-Caps

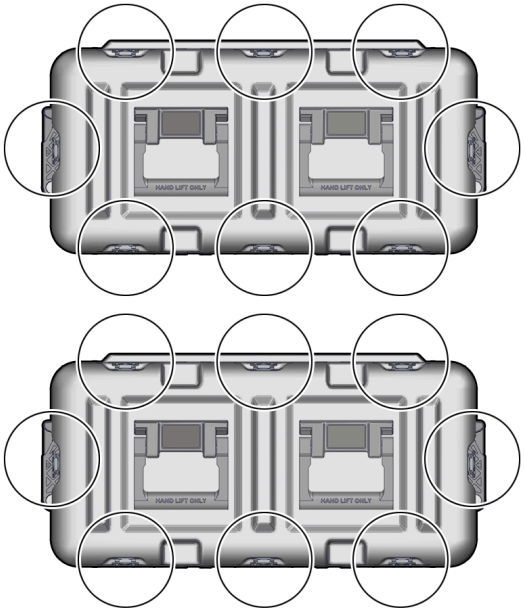
If the Roving Edge Device is in a ruggedized case, you must remove the front and rear end-caps to access the cable connectors. The end-caps remain removed during operation.

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

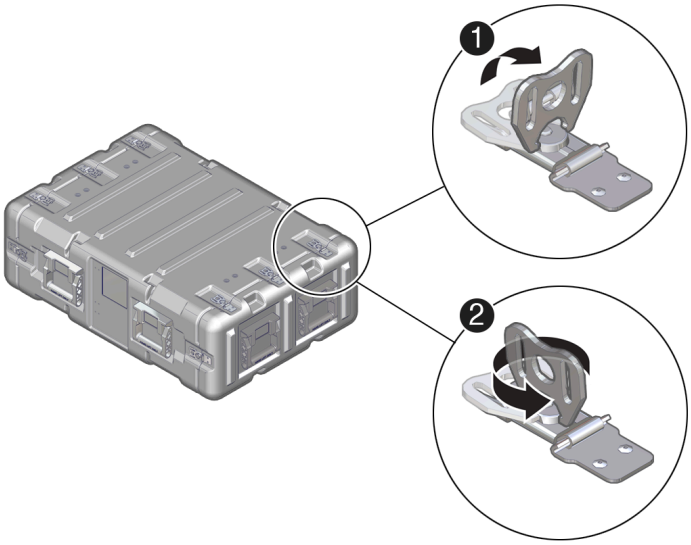
> **Caution:**
>
> Leave the end-caps removed during operation to ensure adequate airflow. Reinstall the end-caps only when the device is powered down.

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

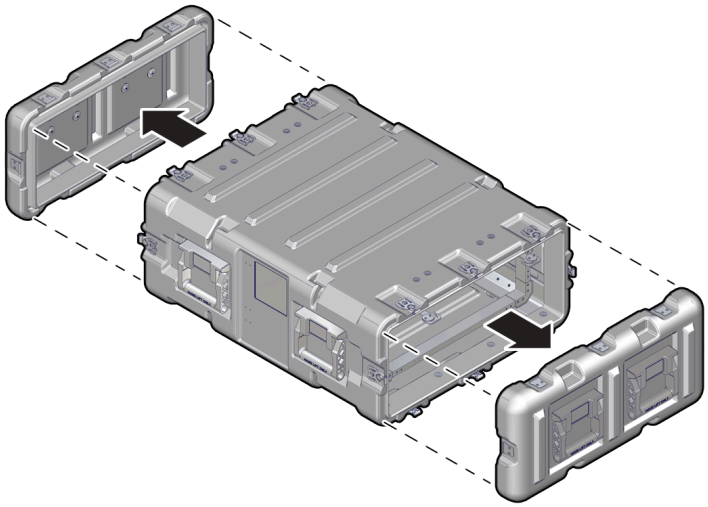
   Note: The rear end-cap has casters.



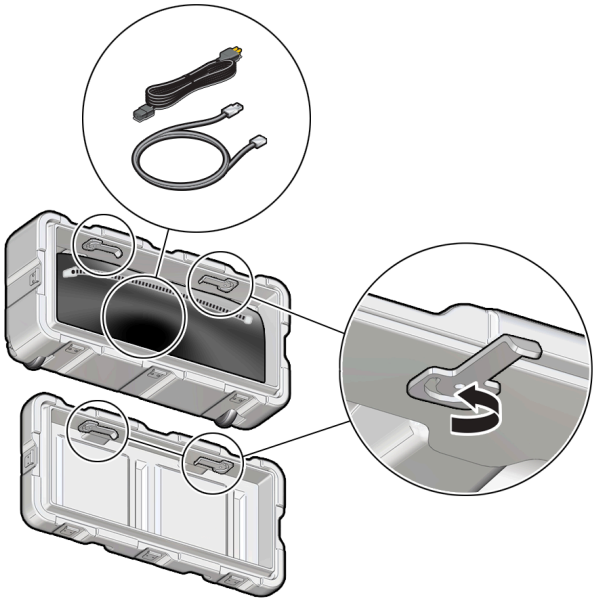
2. Open all 16 wing-turn latches on the front and rear of the case by lifting the latch then turning the latch counterclockwise.



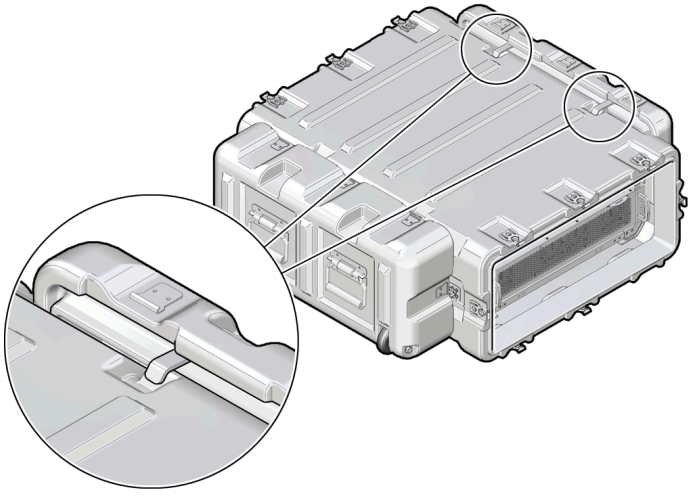
3. Remove the front and rear end-caps.



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?

Identify Front and Rear Panel Items

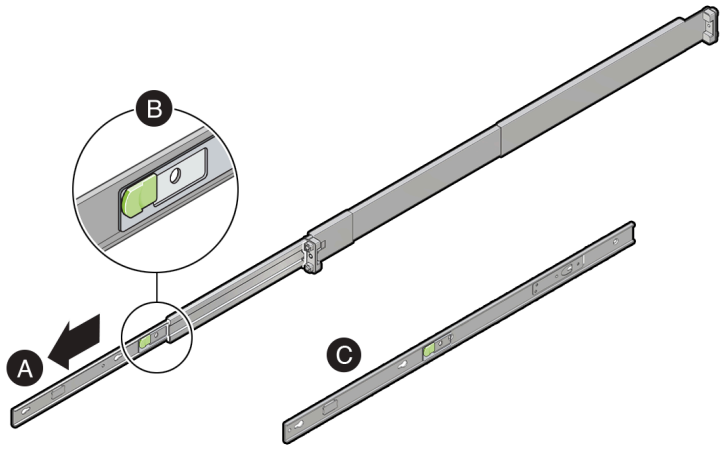
Mount the Device in a Rack

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

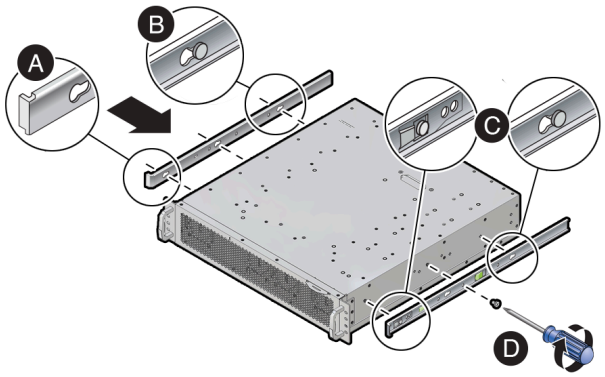
The optional rackmount kit can be used to install the device in a four-post, 19-inch standard rack.

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.

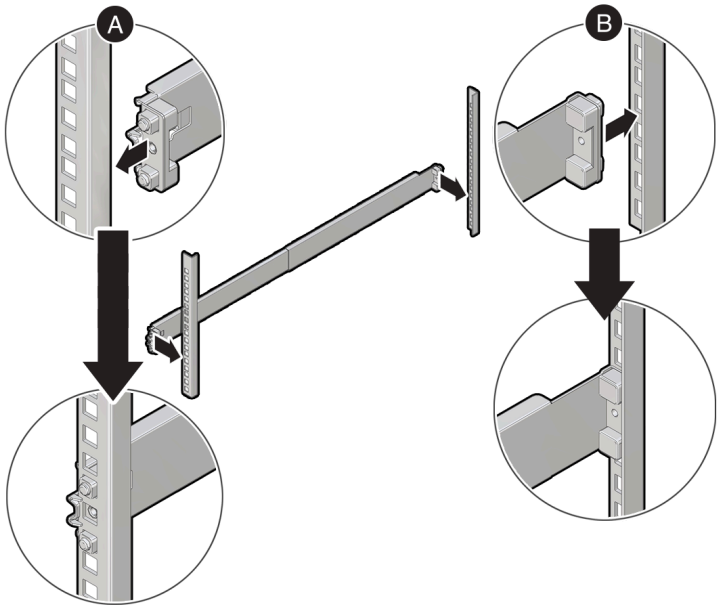


   a. Position the mounting brackets against the device so that the slide-rail stop is at the front of the device.
   b. Line up the keyhole openings on the mounting bracket with the locating pins on the side of the device.
   c. Push the mounting brackets forward until they lock in place with an audible select.
   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.

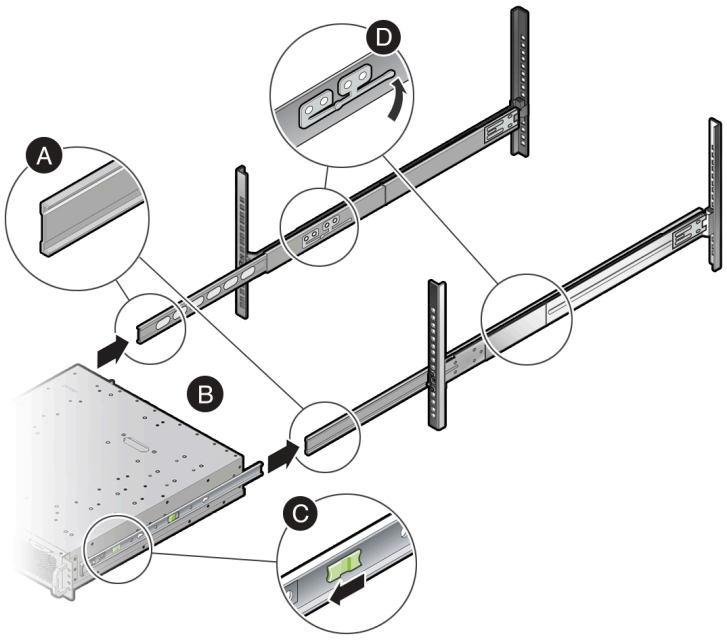
   Roving Edge Device requires two rack units (2U) of vertical space.

> **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.



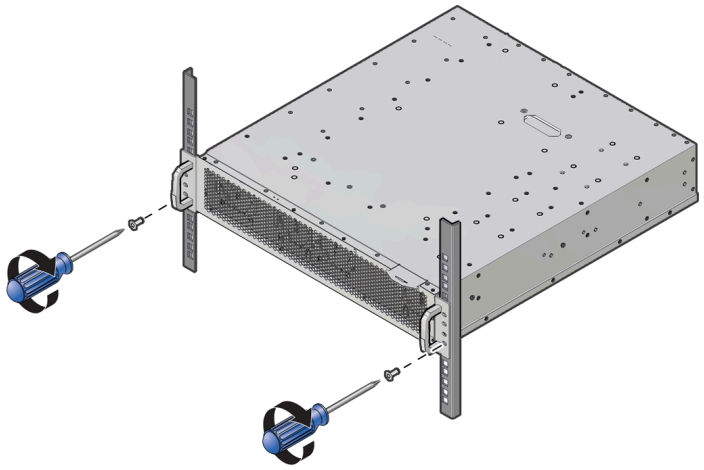
   a. Snap the front slide-rails into the front rack posts.
   b. Adjust the rear slide-rails to reach the rear rack posts, then snap the slide-rails into the rear rack posts.
6. Install the device into the slide-rails.



   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?

Identify Front and Rear Panel Items

Cable the Roving Edge Device

Use the following diagrams to locate connectors on the rear of the Roving Edge Device 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 Identify Front and Rear Panel Items and Managing Ethernet Bonding.

> **Tip:**
>
> Most devices require you to download a large 25 GB software file to self-provision the device. To ensure a smooth installation, we recommend connecting the device to a high-speed network.

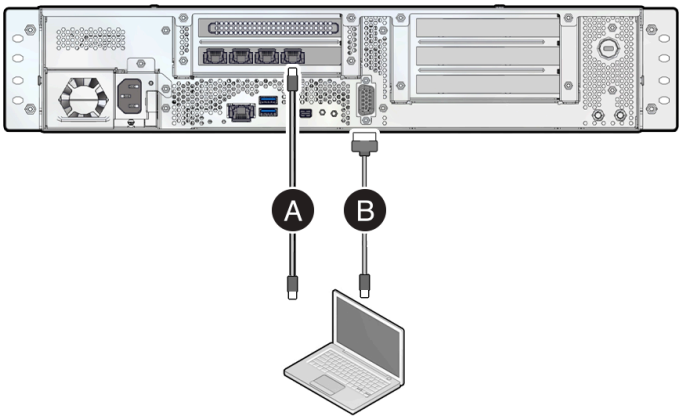
1. Connect cables to the default Ethernet port and to the serial console port as shown in the following diagrams.

> **Note:**
>
> For initial installation and self-provisioning, ensure that the device isn't behind an HTTP proxy server and that the device has internet connectivity. After self-provisioning, you can move the device behind an HTTP proxy server.

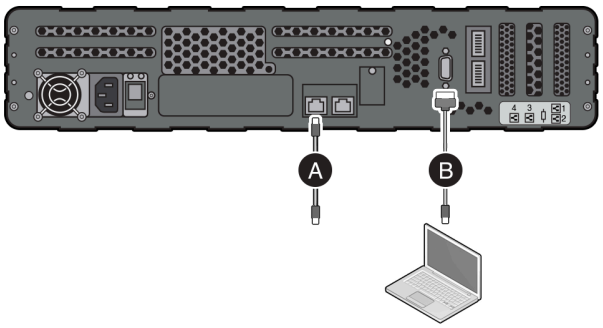
a. Use a 10GBaseT RJ-45 Ethernet cable to connect the device Ethernet port to your Ethernet switch.

b. Connect the provided USB serial cable from the device serial console port to a USB connector on your controlling host, such as a laptop.

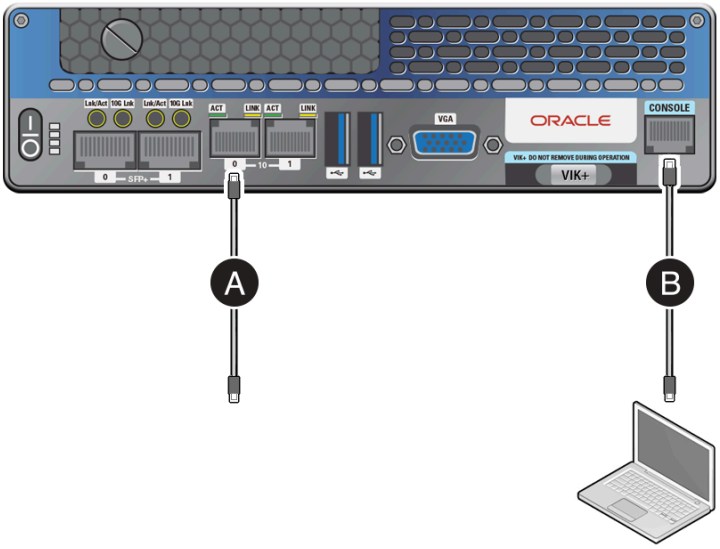
Roving Edge Device 2: Compute, GPU, and Storage Shapes



Roving Edge Device 1



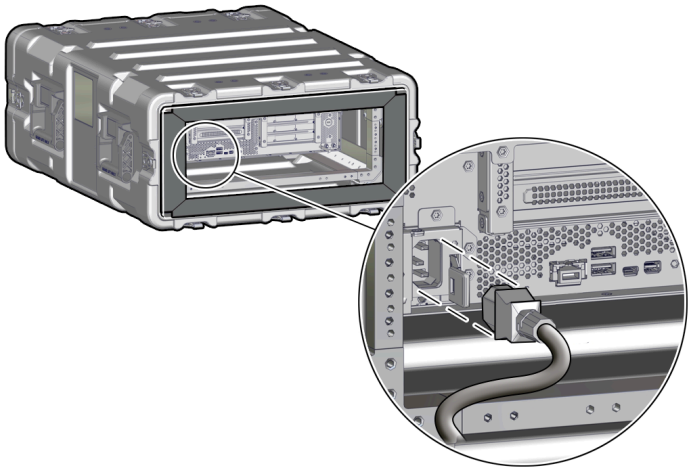
Roving Edge Ultra



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

   For Roving Edge Ultra, connect the power cord to the AC connector on the rear of the device.

   The following illustration shows where to connect the power cable on a Roving Edge Device 2 that's in a ruggedized case.



What's next?

Set Up Terminal Emulation on page 13

Set Up Terminal Emulation

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

1. Based on your host OS and hardware, use the appropriate method to ensure that a USB serial port driver is installed. The driver is required for connectivity to the Roving Edge Device serial port.

   - **Linux**

     The USB serial port driver is preinstalled on Oracle Linux Unbreakable Enterprise Kernel. The following command shows that the USB driver is present (driver version numbers vary):

     ```
     [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
     ```

   - **Microsoft Windows**

     USB serial ports are listed in the **Device Manager** under **Ports (COM & LPT)**. The following example shows the common serial ports:

     ```
     USB-to-Serial Comm Port (COM3)
     USB Serial Port (COM4)
     ```

     If a serial device isn't displayed, you might need to install or update the USB serial port drivers. Go to the Microsoft Windows store to obtain and install the driver.

   - **macOS**

     Example of listing USB serial ports in a terminal window:

     ```
     ls /dev/tty.*
     /dev/tty.usbserial-xxxxx
     ```

If a serial device isn't displayed, you might need to install or update the USB serial port drivers. Go to the Apple store to obtain and install the driver.

2. Install and configure a terminal emulator.

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

   Linux: PuTTY, Minicom, or screen

   Microsoft Windows: PuTTY

   macOS ZOC or screen

   Configure the terminal emulator software settings as follows:

   - Terminal Type: **VT100+**
   - Bits per second: **115200**
   - Data Bits: **8**
   - Stop Bits: **1**
   - Parity: **None**
   - 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.

3. Connect the terminal window to the port:

   - **Linux example:**

     ```
     screen /dev/tty.USBX 115200
     ```

   - **Microsoft Windows:** In PuTTY, under **Connection**, select **Serial**, then enter the following attributes:

     - **Serial line to connect to**: **COM***n* (replace *n* with the appropriate COM number)
     - **Speed (baud)**: **115200**
     - **Data Bits**: **8**
     - **Stop Bits**: **1**
     - **Parity**: **None**
     - **Flow Control**: **None**

     Select **Open**.

   - **macOS example:**

     ```
     screen /dev/tty.usbserialX 115200
     ```

   Serial console output is displayed after the device is powered on.

What's next?

Power On the Device

Unlock the Device

Every time a Roving Edge device is booted, it boots into a locked state. You must unlock the device using an unlock passphrase to use the device.

The passphrase was created in one of the following ways:

- When the device was self-provisioned on-site. See Provision a Device: Set Up Credentials.
- On older Roving Edge Devices and Ultra Devices, the passphrase was created when the node was created in your tenancy. See Creating a Roving Edge Device 1 Node (Deprecated) and Creating a Roving Edge Ultra 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. In the serial console, select **Unlock Device**.
2. Enter the passphrase.

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

What's next?

Establishing the Certificate Authority for Roving Edge Infrastructure Devices

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 Advanced Network Settings.

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 Advanced Network Settings.

What's next?

(Optional) To configure Ethernet bonding, see Managing Ethernet Bonding. Otherwise, go to Unlock the Device on page 14.

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 the 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
- Username
- Password

Ensure The Host Has OpenSSL Installed

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

To decide if OpenSSL is installed on Microsoft Windows, search for openssl. If OpenSSL isn't installed, follow the 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 the computer to find the Device Console IP address regardless of the DNS configuration.

Use one of the following procedures based on the 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 the 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 select **Terminal**.
2. Open the `/etc/hosts` file in a text editor. The following example uses the nano editor:

   ```
   sudo nano /etc/hosts
   ```
3. Enter the 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 the computer OS.

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

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 the home directory.

Microsoft Windows with Firefox

The following steps are for Firefox version 115.

> **Note:**
>
> Browsers evolve over time. If some browser steps don't match what you see in the browser, consult the browser documentation.

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 upper left of the browser address bar.
3. In the Site Information dialog box, select **Connection Secure**, then select **More information**.

   The Firefox Security menu is displayed.
4. Select **View Certificate**.

   The Device Console now displays certificate information.
5. Select the tab called <*hostname*>**-root-CA** .
6. Scroll down to the **Miscellaneous** section.
7. Select 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.

> **Note:**
>
> Browsers evolve over time. If some browser steps don't match what you see in the browser, consult the browser documentation.

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

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

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

Microsoft Windows with Chrome

The following steps are for Google Chrome version 135.0.7049.42.

> **Note:**
>
> Browsers evolve over time. If some browser steps don't match what you see in the browser, consult the browser documentation.

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

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

   The sign-in page reports that the device is unavailable because the connection is insecure until the certificate is imported.
2. Select the **Not secure** icon next to the URL field.
3. Select **Certificate details**.
4. Select the **Details** tab.
5. Under **Certificate Hierarchy**, select the top certificate.
6. Select **Export**.
7. Browse to a convenient download location such as Downloads.
8. Select **Save**.
9. Close the Certificate Viewer.

Task 3 - Import the Root Certificate into The Browser

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

Firefox

> **Note:**
>
> Browsers evolve over time. If some browser steps don't match what you see in the browser, consult the browser documentation.

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

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

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

You're prompted to enter the username and password.

Edge

> **Note:**
>
> Browsers evolve over time. If some browser steps don't match what you see in the browser, consult the browser documentation.

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

   The Certificate manager is displayed.

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

Chrome

> **Note:**
>
> Browsers evolve over time. If some browser steps don't match what you see in the browser, consult the browser documentation.

1. In Chrome, use the navigation menu to open **Settings**.
2. Select **Privacy and security**.
3. Select **Security**.
4. Select **Manage certificates**.
5. Select **Manage imported certificates**.

   The Certificate Manager is displayed.
6. Select the **Trusted Root Certificates** tab.
7. Select **Import**.

   The **Certificate Wizard** is displayed.
8. Select **Next**.
9. Select **Browse**, and browse to the location of the downloaded certificate file, select it, then select **Open**, then select **Next**.
10. Select **Place all certificates in the following store**, then select **Next**.
11. Select **Finish**.
12. Select **OK** to acknowledge the import was successful.
13. Close the **Certificate Wizard**.
14. Refresh the browser tab that's connected to the device.

You're prompted to enter the username and password.

The Roving Edge device is installed and ready for use.

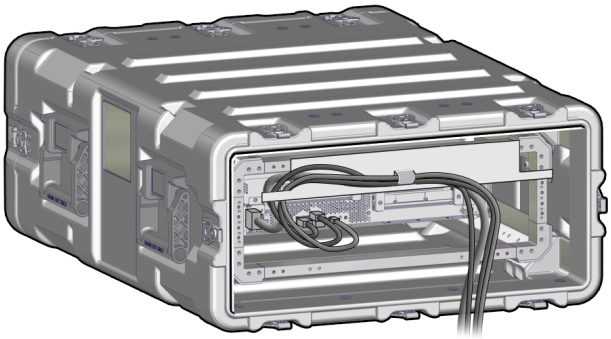
Consider your next action:

- Learn about ways to access the device. See Accessing Roving Edge.
- Start creating Roving Edge Infrastructure resources. See Networking for Roving Edge Infrastructure Devices and Compute Instances.

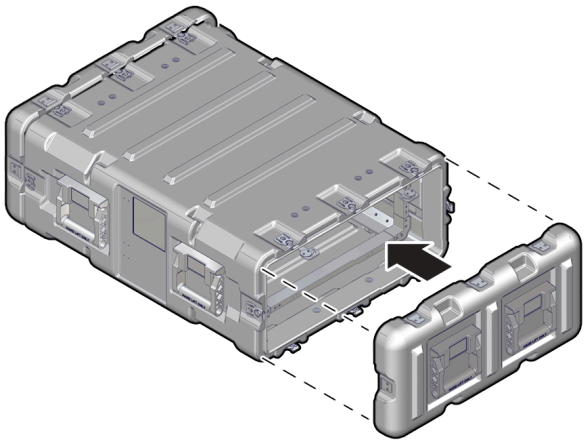
Reinstall the Ruggedized Case End-Cap

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

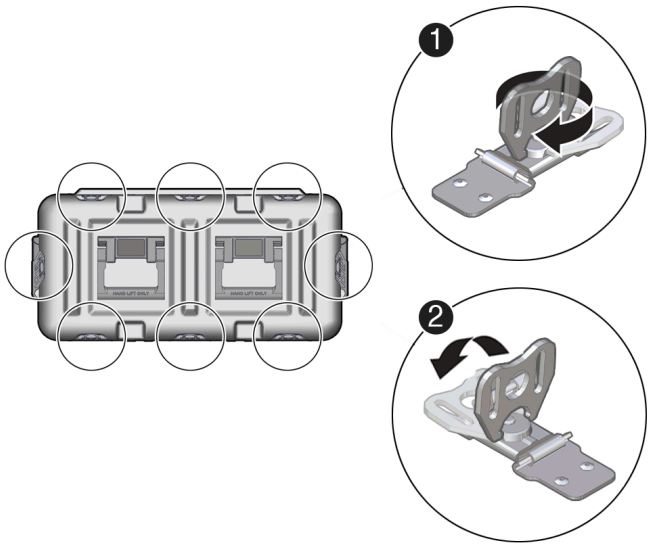
1. Route cable slack through the foam channels.



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